INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

DIGITAL SOVEREIGNTY VS OPEN INTERNET: COMPARATIVE HUMAN RIGHTS IMPLICATIONS

AUTHORED BY - SNEHA SHARMA[1] AND ANMOL KUMAR[2]

ABSTRACT

The contemporary digital landscape is characterized by a fundamental tension between digital sovereignty and open internet principles, each carrying profound implications for human rights protection and realization. Digital sovereignty represents the assertion of state control over digital infrastructure, data governance, and internet regulation within national borders, while open internet principles emphasize global interconnectedness, unrestricted information flow, and universal access to digital resources. Digital sovereignty manifests through data localization mandates, content restrictions, and national internet controls as states seek to protect citizen privacy, maintain cultural identity, and secure national interests. The European Union's comprehensive data protection framework and various national cybersecurity laws exemplify sophisticated attempts to exercise digital control while claiming to safeguard citizen rights. However, these measures often result in internet fragmentation, creating isolated digital ecosystems that undermine the global nature of internet infrastructure and limit cross-border collaboration. Conversely, open internet principles prioritize universality, accessibility, freedom of expression, and network neutrality. This paradigm supports innovation, unrestricted information access, and maintenance of a globally interoperable network that facilitates economic development and human rights realization. Yet, unregulated digital environments can expose users to privacy violations, surveillance capitalism, and exploitation by dominant platforms. The human rights implications are complex and multifaceted. Digital sovereignty measures may protect privacy and data rights but frequently restrict freedom of expression, limit information access, and create barriers to democratic participation. Internet shutdowns and content blocking isolate populations from global discourse. Alternatively, completely open internet environments enable surveillance and algorithmic manipulation that can erode privacy rights and user autonomy. Neither absolute digital sovereignty nor unrestricted internet openness adequately safeguards human rights. Sustainable digital governance requires nuanced regulatory frameworks balancing state interests with individual rights, international

[1] Sneha Sharma, 2nd Year student of BA LLB at Lovely Professional University, Phagwara, Punjab.
[2] Anmol Kumar, 4th Year student of BBA LLB at Lovely Professional University, Phagwara, Punjab.

ISSN: 2582-6433

cooperation, and adaptive legal structures. As internet fragmentation accelerates and digital nationalism intensifies, developing global standards respecting both sovereignty and human rights becomes increasingly critical for ensuring digital governance enhances rather than diminishes human dignity and freedom.

Keywords: Sovereignty, Cyber, Human Rights, International, Internet.

1. INTRODUCTION

The rapid expansion of digital technologies has reshaped global governance paradigms, giving rise to a fundamental tension between digital sovereignty, the assertion of state control over national digital infrastructures and data and the open internet model, which prioritizes universal connectivity and unrestricted information flows. While digital sovereignty has gained traction as governments seek to safeguard national security, cultural integrity, and economic autonomy, the open internet ethos underscores the importance of freedom of expression, network neutrality, and multistakeholder governance to realize fundamental human rights. Originally conceived as a borderless network facilitating academic collaboration, the internet evolved into a global public resource underpinned by principles of interoperability and permissionless innovation. The open internet framework, enshrined in instruments such as the Charter of Human Rights and Principles for the Internet, emphasizes that access to information, freedom of expression, and equal participation in digital spaces are essential components of human dignity and democratic governance. This paradigm has driven unprecedented economic growth and social empowerment by enabling cross-border communication, digital entrepreneurship, and civic engagement.[3]

Conversely, the concept of digital sovereignty has evolved from a peripheral policy concern into a central pillar of statecraft. Initially dismissed as antithetical to the internet's decentralized architecture, digital sovereignty reemerged as states confronted the growing influence of multinational technology platforms and the risks posed by transnational cyber threats. Countries such as China and Russia prosecute stringent data localization rules and content controls to assert territorial jurisdiction over digital activities, while democratic states in Europe and India advocate "technological sovereignty" to protect citizen data and reduce dependence

[3] *Internet Rights & Principles Coalition*, Internet Governance Forum United Nations, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf (last visited Oct 6, 2025).

ISSN: 2582-6433

on foreign platforms. However, these measures frequently produce internet fragmentation splintered networks that erode global interoperability and impede cross-border data flows.[4] The human rights implications of both paradigms are complex. Digital sovereignty initiatives, often enacted through internet shutdowns and censorship, disrupt essential services and curtail freedom of expression, disproportionately affecting vulnerable communities reliant on digital connectivity for education, health, and livelihoods. Meanwhile, unregulated open internet environments enable pervasive surveillance capitalism and algorithmic discrimination by dominant platforms, undermining privacy rights and democratic discourse. The rise of quasi-sovereign corporate actors controlling critical digital infrastructure further complicates the landscape, revealing gaps in existing governance regimes.[5]

Research Objectives

- To analyze the evolving concepts of digital sovereignty and open internet and their impact on internet governance frameworks.
- To compare regulatory approaches in key jurisdictions such as the EU, US, China, and India concerning digital sovereignty and open internet principles.
- To assess how digital sovereignty measures affect fundamental human rights including freedom of expression, privacy, and access to information.
- To evaluate the role of multistakeholder governance and international cooperation in balancing sovereignty claims with open internet values.
- To propose policy recommendations for adaptive governance models that reconcile state sovereignty with the protection of digital human rights.

Literature Review

The literature on internet governance reveals a historical trajectory characterized by the tension between an open, decentralized network architecture and emerging state-centric sovereignty claims. Early scholarship traces the internet's origins to the ARPANET project (1969) and TCP/IP protocol standardization (1983), emphasizing how these foundational technologies created a borderless infrastructure designed to maximize interoperability and innovation. The governance model during this formative period was informal and collaborative, with technical

[4] Julia Pohle and Thorsten Thiel, *Digital Sovereignty*, 9(4) Concepts of digital society 3 (2020).
[5] *Joint Statement on Protecting Human Rights Online and Preventing Internet Shutdowns in Times of Armed Conflict*, Freedom Online Coalition, *https://freedomonlinecoalition.com/joint-statement-on-protecting-human-rights-online-and-preventing-internet-shutdowns-in-times-of-armed-conflict/* (last visited Oct 6, 2025).

ISSN: 2582-6433

coordination managed through multistakeholder bodies such as the Internet Engineering Task Force and the Internet Assigned Numbers Authority, ensuring that no single entity could monopolize control over internet standards or content.

The open internet paradigm gained further legitimacy with the establishment of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998, which embodied principles of global participation and non-state control over critical resources such as domain names and IP addressing. Leiner et al. document how this era's normative consensus held that unfettered cross-border data flows and minimal content restrictions would maximize social and economic benefits, positioning freedom of expression and access to information as foundational human rights in digital spaces. The Charter of Human Rights and Principles for the Internet, developed by the Internet Rights & Principles Coalition, further codifies these values, emphasizing universality, accessibility, and equal participation as essential components of human dignity and democratic governance.

However, the digital sovereignty concept has evolved from a peripheral policy concern into a central pillar of contemporary statecraft. Pohle and Thiel trace this evolution, noting how initial dismissals of sovereignty as incompatible with the internet's decentralized architecture gave way to renewed state assertions following cybersecurity threats and mass surveillance revelations, particularly the 2013 Snowden disclosures. Countries such as China and Russia have implemented stringent data localization rules and content controls exemplified by the Great Firewall and sovereign internet legislation to assert territorial jurisdiction over digital activities and protect national security and cultural values. Democratic states have also embraced digital sovereignty, with the European Union developing "technological autonomy" through the General Data Protection Regulation (GDPR), which balances individual data rights with regulated cross-border transfers.

Critical scholarship examines how sovereignty measures contribute to internet fragmentation or the "splinternet," where divergent regulatory regimes create isolated digital ecosystems. Nocetti's analysis of China, Russia, India, and the European Union demonstrates how data localization mandates, national firewalls, and content controls undermine global interoperability, increase operational costs for cross-border services, and exacerbate the digital divide particularly in developing regions lacking sovereign infrastructure. This fragmentation disproportionately harms vulnerable populations by restricting access to essential services,

ISSN: 2582-6433

economic opportunities, and democratic participation platforms, as documented in Human Rights Watch's examination of India's extensive internet shutdowns.

Conversely, scholars critique unfettered open internet environments for enabling surveillance capitalism and algorithmic discrimination in the absence of comprehensive regulatory safeguards. Research on platform governance highlights how dominant technology corporations concentrate power and exploit user data without adequate accountability mechanisms, undermining privacy rights and democratic discourse. The landmark *Shreya Singhal v. Union of India* case illustrates judicial recognition of the need to balance digital expression rights with reasonable content restrictions, while India's *K.S. Puttaswamy* decision establishes privacy as a fundamental constitutional right that must inform both sovereignty and openness paradigms.

Emerging literature advocates hybrid governance frameworks that reconcile legitimate sovereignty aims security, cultural preservation, economic autonomy with open internet values of universal access, freedom of expression, and multistakeholder participation. Barber and Canales propose rights-based approaches to platform regulation that embed human rights impact assessments in policy design, while the European Union's Digital Services Act attempts to balance democratic participation with platform accountability through transparency requirements and content moderation standards. These hybrid models emphasize international cooperation, adaptive regulation responsive to emerging technologies, and equitable representation of civil society and marginalized communities in policymaking processes to sustain the internet's role as a global public good while protecting human dignity in the digital age.

Hypothesis

- Digital sovereignty measures designed to enhance state control over data and infrastructure paradoxically undermine fundamental human rights particularly freedom of expression, privacy, and access to information more significantly than open internet governance models.
- Democratic jurisdictions that implement digital sovereignty frameworks with robust rights safeguards (e.g., the EU’s GDPR) maintain higher levels of human rights protection compared to authoritarian regimes whose sovereignty claims serve primarily to consolidate state power (e.g., China’s Cybersecurity Law).

ISSN: 2582-6433

- Internet fragmentation resulting from digital sovereignty initiatives disproportionately harms vulnerable and marginalized populations by restricting access to essential services, economic opportunities, and democratic participation platforms.
- Governance frameworks incorporating genuine multistakeholder participation and international cooperation mechanisms provide more effective protection of digital human rights than either exclusively state-centric sovereignty models or wholly market-driven open internet approaches.
- Hybrid regulatory models that combine rights-based standards with adaptive, technology-neutral approaches yield superior human rights outcomes compared to rigid sovereignty or unregulated openness paradigms, particularly in addressing emerging challenges posed by AI and platform algorithms.

Research Questions

1. How do different conceptualizations of digital sovereignty and open internet influence internet governance policies worldwide?
2. What are the comparative impacts of digital sovereignty and open internet regulatory approaches on fundamental human rights such as freedom of expression, privacy, and access to information?
3. To what extent do digital sovereignty measures contribute to internet fragmentation, and how does this fragmentation affect global connectivity and human rights?
4. How do multistakeholder governance models and international cooperation mechanisms address the tensions between state sovereignty and open internet principles?
5. What policy frameworks can reconcile state interests in digital sovereignty with the protection of universal digital rights and open internet values?

Research Methodology

The research will employ a qualitative comparative analysis methodology to explore the tensions between digital sovereignty and open internet governance, focusing on their human rights implications. First, a doctrinal analysis of regulatory frameworks in key jurisdictions such as the European Union's GDPR and Digital Markets Act, the United States' sectoral privacy laws, China's Cybersecurity Law, and India's intermediary guidelines will be conducted to identify how legal provisions shape data control, content regulation, and platform

ISSN: 2582-6433

governance. Second, thematic content analysis of secondary sources, including reports from human rights organizations, policy think tanks, and academic literature, will assess real-world impacts of these regulations on freedom of expression, privacy, access to information, and democratic participation.

The study will further analyze internet fragmentation phenomena through documented cases of internet shutdowns, content filtering, and data localization, examining their effects on marginalized communities. Multistakeholder governance models and international cooperation mechanisms will be scrutinized to understand their potential in mitigating conflicts between state sovereignty and internet openness. This research will draw on a mixed methodological framework combining legal analysis, policy review, and empirical evidence synthesis to develop comprehensive insights. The approach allows for nuanced understanding of regulatory efficacy and human rights outcomes across diverse political contexts. Data triangulation from multiple sources ensures reliability and depth in findings. Ultimately, the methodology supports formulating policy recommendations that safeguard human rights while respecting legitimate sovereignty concerns in the digital era.

Research Gap

Despite growing scholarly and policy interest in digital sovereignty and open internet governance, significant research gaps remain in understanding their comparative human rights implications. Much of the existing literature tends to focus on technological or legal aspects in isolation, without fully integrating the multidimensional impacts on fundamental rights such as freedom of expression, privacy, and access to information. There is a lack of comprehensive comparative studies that systematically analyze how diverse regulatory frameworks across different political and cultural contexts reconcile or fail to reconcile state sovereignty claims with the principles of an open, rights-respecting internet.

Moreover, empirical data on the real-world social and economic consequences of internet fragmentation, including its disproportionate effects on vulnerable populations, remains limited and fragmented across disciplines. Multistakeholder governance mechanisms and international cooperative efforts to bridge these tensions are often discussed normatively rather than evaluated through rigorous, evidence-based assessments. Additionally, emerging challenges posed by new technologies like artificial intelligence, blockchain, and platform algorithms complicate governance dynamics but have yet to be adequately explored in relation to

ISSN: 2582-6433

sovereignty and human rights.

This research aims to address these gaps by providing an integrated, comparative human rights analysis of digital sovereignty and open internet paradigms. It seeks to highlight areas where existing frameworks fall short in protecting digital rights, identify inconsistencies between policy objectives and outcomes, and offer targeted recommendations for adaptive governance that balances sovereign interests with universal human rights protections in the rapidly evolving digital landscape.

Historical Evolution of Internet Governance

The origins of internet governance are rooted in the design principles of the ARPANET project (1969) and the subsequent adoption of the TCP/IP protocol (1983), which together established a borderless, decentralized network architecture prioritizing interoperability and permissionless innovation. During this formative period, governance was informal and collaborative: technical coordination occurred through bodies like the Internet Engineering Task Force (IETF) and the Internet Assigned Numbers Authority (IANA), reflecting a multistakeholder model in which universities, private companies, and government agencies jointly shaped standards and policies.[6]

In the 1990s, the emergence of the World Wide Web propelled exponential growth in user numbers and applications, reinforcing the open internet paradigm. Governance expanded to include the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998, which embodied principles of global participation and non-state control over critical resources such as domain names and IP addressing. This era's normative consensus held that unfettered cross-border data flows and minimal content restrictions would maximize social and economic benefits, underpinning freedom of expression and access to information as foundational human rights.[7]

By the early 2000s, growing concerns over cybercrime, terrorism, and large-scale surveillance crystallized by the 2013 Snowden revelations prompted states to reassert territorial jurisdiction

[6] *History of the Internet*, WIKIPEDIA, https://en.wikipedia.org/wiki/History_of_the_Internet (last visited Oct 6, 2025).
[7] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, *A Brief History of the Internet*, *https://www.internetsociety.org/internet/history-internet/brief-history-internet/* (last visited Oct 6, 2025).

ISSN: 2582-6433

in cyberspace. The concept of digital sovereignty, once peripheral, gained traction as governments sought to protect national security, cultural identity, and economic autonomy. European initiatives such as the General Data Protection Regulation (GDPR) (2016) introduced comprehensive data protection rules, asserting citizens' rights over personal data while preserving cross-border flows under strict safeguards. Simultaneously, nations like China implemented the Great Firewall and Russia passed "sovereign internet" legislation to localize data and regulate content, marking a shift toward internet fragmentation.[8]

In the 2020s, this duality between an open, rights-based internet and state-centric digital sovereignty has crystallized into competing governance paradigms. Open-internet advocates emphasize universality, network neutrality, and multistakeholder stewardship to uphold freedom of expression and inclusive access. Conversely, digital-sovereignty proponents prioritize jurisdictional control, data localization, and content regulation to safeguard security and cultural values. The resulting landscape is marked by splintered networks and divergent legal frameworks, posing complex challenges for the protection of digital human rights in a global, yet increasingly segmented, internet ecosystem.

Conceptual Framework: Digital Sovereignty vs. Open Internet

Digital sovereignty and the open internet represent two divergent governance paradigms that shape how states, corporations, and individuals interact within cyberspace. Digital sovereignty asserts that nation-states hold ultimate authority over digital infrastructure and data generated within their borders. This principle encompasses jurisdictional control, whereby governments enact data localization requirements and content regulations to enforce domestic laws on collection, storage, and processing. By prioritizing security and stability, states aim to shield critical infrastructure from external threats and preserve cultural values through mechanisms such as national firewalls and sovereign clouds. Economic autonomy further motivates sovereignty measures, as countries incentivize local digital industries and reduce reliance on foreign technology providers by mandating the use of domestic data centers and cloud services.[9]

In contrast, the open internet paradigm champions a borderless network underpinned by standardized protocols that ensure interoperability and universal access. Core values include

[8] Supra, at 2.
[9] Id. at 6.

ISSN: 2582-6433

freedom of expression minimizing content restrictions to foster journalism, civic discourse, and creative innovation and network neutrality, which guarantees that data packets are treated equally without discrimination. Governance under this model follows a multistakeholder approach, distributing authority among governments, the private sector, civil society, and technical experts to collaboratively manage critical resources and policy development.[10]

These paradigms intersect along legal, technical, and normative dimensions. Legally, digital sovereignty concentrates regulatory power within state institutions, whereas open internet governance disperses authority across a diverse array of stakeholders. Architecturally, sovereignty initiatives often fragment networks into isolated ecosystems, while open models favor global connectivity and seamless data flows. Ethically, sovereignty emphasizes collective security and cultural preservation, sometimes at the expense of individual freedoms; conversely, open internet ethics foreground individual rights but may under-emphasize state interests in security and economic resilience.[11]

By mapping these dimensions, this framework provides a basis for analyzing how varying governance choices influence human rights outcomes particularly privacy, freedom of expression, and equitable access to information across different political and legal contexts.

Comparative Regulatory Landscapes

- **European Union**

  The European Union epitomizes a rights-based approach that balances digital sovereignty with open internet principles. The General Data Protection Regulation empowers individuals with control over personal data through rights of access, rectification, and erasure while permitting cross-border data transfers under rigorous safeguards. The Digital Markets Act and Digital Services Act constrain dominant platform practices, promoting fair competition and transparency without erecting national firewalls. Meanwhile, the AI Act establishes a risk-based framework for algorithmic governance, embedding human rights safeguards into emerging technologies. Together, these measures reflect “technological sovereignty” asserting

[10] Supra, at 1.
[11] Julien NOCETTI, A Splintered Internet? Internet Fragmentation and the Strategies of China, Russia, India and the European Union, IFRI (Feb 27, 2024), https://www.ifri.org/en/studies/splintered-internet-internet-fragmentation-and-strategies-china-russia-india-and-european

ISSN: 2582-6433

regulatory authority to protect citizens and markets while maintaining interoperability and preserving users' fundamental freedoms.[12]

- **United States**

  In the United States, internet governance is driven by market-oriented policies and sector-specific regulations. The First Amendment robustly protects freedom of expression online, and Section 230 of the Communications Decency Act shields platforms from liability for third-party content, fostering innovation and speech. However, limited federal privacy legislation means enforcement relies on sectoral statutes such as HIPAA and the Children's Online Privacy Protection Act (COPPA). State initiatives like the California Consumer Privacy Act have begun to fill regulatory gaps, but the absence of a unified data protection framework exposes users to inconsistent rights and uneven enforcement. The U.S. model privileges an open, commercially driven internet, sometimes at the expense of comprehensive privacy and antitrust protections.[13]

- **China**

  China's approach prioritizes state-centric digital sovereignty. The Cybersecurity Law and Personal Information Protection Law mandate stringent data localization, requiring both domestic and foreign entities to store sensitive data within national borders. The Great Firewall enforces extensive content controls, filtering information deemed harmful to social stability or political unity. Surveillance technologies and real-name registration systems enhance state oversight of online activities. While these measures bolster national security and cultural cohesion, they significantly restrict freedom of expression, access to information, and privacy, illustrating how sovereignty claims can consolidate governmental power at the expense of individual liberties.[14]

- **India**

  India occupies a hybrid position between open and sovereign paradigms. The Information Technology Rules impose content moderation duties on platforms, including takedown requirements and traceability obligations. Proposed data protection legislation echoes GDPR's individual rights framework but incorporates exemptions

[12] *Digital Sovereignty and Citizens' Rights*, European Movement International, https://europeanmovement.eu/policy/digital-sovereignty-and-citizens-rights-2/ (last visited Oct 7, 2025).
[13] Supra, at 3.
[14] Marilia Maciel, *Digital sovereignty: The end of the open internet as we know it? (Part 1)*, https://www.diplomacy.edu/blog/digital-sovereignty-the-end-of-the-open-internet-as-we-know-it-part-1/ (last visited Oct 7, 2025).

ISSN: 2582-6433

for national security and public order. Moreover, India's frequent internet shutdowns authorized under the Temporary Suspension of Telecom Services Rules illustrate the assertion of state control over connectivity in response to security concerns. These shutdowns, while intended to maintain public order, disrupt economic activity, education, and healthcare, demonstrating the human rights costs of sovereigntist measures. At the same time, India's robust digital market and civil society advocacy continue to push for greater transparency and rights protections in line with open internet values.[15]

Human Rights Implications

Freedom of Expression and Censorship

The tension between digital sovereignty and open internet principles manifests most prominently in conflicts over freedom of expression and censorship. Digital sovereignty measures often enable states to control online discourse through content filtering, platform blocking, and takedown requirements that can severely restrict citizens' ability to express dissenting views or access diverse information sources. India's Information Technology Rules exemplify this challenge, requiring platforms to remove content deemed harmful to public order or national security, leading to criticism that these provisions are used to suppress political opposition and journalistic inquiry. Similarly, Russia's digital sovereignty framework has evolved from early internet freedom rhetoric to comprehensive censorship apparatus designed to eliminate anonymity and control information flows, fundamentally transforming freedom of expression from a right into a state-granted privilege.[16]

Conversely, open internet environments theoretically protect expressive freedoms through minimal content restrictions and platform neutrality. However, the absence of regulatory oversight has enabled the proliferation of misinformation, hate speech, and coordinated inauthentic behavior that can undermine democratic discourse. The landmark *Shreya Singhal v. Union of India*[17] case demonstrates judicial recognition that digital expression requires constitutional protection, with India's Supreme Court striking down overly broad

[15] "No Internet Means No Work, No Pay, No Food", Internet Shutdowns Deny Access to Basic Rights in "Digital India", https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic (last visited Oct 7, 2025).
[16] David Inserra, *Pro-Brazilian Censors Strike Back: Digital Sovereignty Versus Free Speech Online*, CATO INSTITUTE (Sep 25, 2024), https://www.cato.org/blog/pro-brazilian-censors-strike-back-digital-sovereignty-versus-free-speech-online
[17] Shreya Singhal v. Union of India, AIR 2015 SC 1523.

ISSN: 2582-6433

criminalization of online speech while acknowledging the need for reasonable restrictions. The challenge lies in defining these reasonable restrictions without creating chilling effects on legitimate expression, particularly as digital platforms increasingly serve as essential forums for public debate and civic engagement.[18]

Privacy and Data Protection

Privacy rights represent another critical battleground where sovereignty and openness create competing frameworks for protecting individual autonomy. Digital sovereignty initiatives frequently emphasize data localization and territorial control over personal information as means of protecting citizen privacy from foreign surveillance and corporate exploitation. India's Digital Personal Data Protection Act exemplifies this approach, establishing comprehensive rights including access, correction, erasure, and consent withdrawal while requiring domestic storage of sensitive data. The European Union's GDPR demonstrates how sovereignty claims can enhance privacy protection through stringent consent requirements and user rights, while maintaining cross-border data flows under adequate protection standards.[19]

However, sovereignty-based privacy frameworks can paradoxically weaken individual privacy by concentrating data control within state institutions that may lack robust oversight mechanisms. India's interception regime expansion illustrates how digital sovereignty can become a pretext for enhanced surveillance capabilities that undermine the very privacy rights they purport to protect. Meanwhile, open internet models often rely on market-based privacy protections that have proven inadequate against surveillance capitalism and data monetization practices. The recognition of privacy as a fundamental right under Article 21 of the Indian Constitution in the *Justice K.S. Puttaswamy* case[20] establishes a framework for evaluating both sovereignty and openness paradigms against constitutional standards of personal autonomy and dignity.[21]

[18] Ian Barber and Maria Paz Canales, *What would a human rights-based approach to platform regulation look like?*, GLOBAL PARTNERS DIGITAL (July 30, 2024), https://www.gp-digital.org/what-would-a-human-rights-based-approach-to-platform-regulation-look-like/

[19] Data Protection Laws of the World, *DLA PIPER*, https://www.dlapiperdataprotection.com/?t=law&c=IN (last visited Oct 7, 2025).

[20] K.S. Puttaswamy vs. Union of India (2017), 10 SCC 1.

[21] *Privacy in Peril: India's Interception Regime*, Jyoti Panday and Saumya Jain (Dec 13, 2024), https://www.legalbluebook.com/bluebook/v22/rules/18-the-internet-electronic-media-and-other-nonprint-resources/18-2-the-internet

ISSN: 2582-6433

Access to Information and Digital Divide

The digital divide represents a fundamental human rights challenge that affects how both sovereignty and openness paradigms impact access to information. Internet access has gained recognition as a human right essential for exercising other fundamental freedoms, with the UN General Assembly declaring connectivity access a basic human right in 2016. The COVID-19 pandemic starkly illustrated how digital exclusion perpetuates social, economic, and political disparities, with approximately 3.7 billion people lacking internet access disproportionately affecting low-income communities, rural populations, and marginalized groups.

Digital sovereignty measures can exacerbate information access inequalities through internet shutdowns, content blocking, and technical fragmentation that isolate populations from global information networks. India's extensive use of internet shutdowns the highest globally demonstrates how sovereignty assertions can deny entire communities access to essential services, economic opportunities, and democratic participation. These shutdowns disproportionately harm vulnerable populations dependent on digital connectivity for livelihoods, education, and healthcare, transforming access restrictions into violations of the right to life and dignity. Conversely, open internet principles promote universal access and global connectivity but may fail to address structural inequalities that prevent meaningful participation in digital spaces, particularly for communities lacking adequate infrastructure or digital literacy.

Democratic Participation and Civic Engagement

Digital governance frameworks profoundly shape possibilities for democratic participation and civic engagement in contemporary societies. Open internet environments can enhance democratic discourse through e-democracy tools including online voting systems, digital forums, and real-time polling applications that increase civic participation and government transparency. These platforms enable marginalized voices to participate in political processes and facilitate direct communication between citizens and representatives, potentially strengthening democratic foundations through increased accessibility and inclusivity.[22]

However, unregulated digital spaces can also undermine democratic processes through platform manipulation, algorithmic amplification of divisive content, and foreign interference

[22] Takahisa Kawaguchi, *How democratic states are regulating digital platforms*, INSTITUTE OF GEOECONOMICS (Apr 10, 2024), https://instituteofgeoeconomics.org/en/research/2024041057049/

ISSN: 2582-6433

operations that distort public debate. Social media platforms' role in spreading misinformation and coordinating harmful activities, from election fraud claims to incitement of violence, demonstrates how open systems can become vectors for democratic destabilization. Digital sovereignty approaches attempt to address these challenges through platform regulation and content governance requirements, but risk creating authoritarian control mechanisms that suppress legitimate dissent and civic organization.[23]

The European Union's Digital Services Act represents an attempt to balance democratic participation with platform accountability through transparency requirements and content moderation standards that preserve expressive freedoms while addressing harmful content. However, the challenge remains ensuring that regulatory frameworks enhance rather than constrain civic engagement, particularly given the tendency for content moderation systems to over-remove permissible political speech and disproportionately impact marginalized communities. Effective protection of democratic participation requires governance models that can adapt to evolving threats while maintaining robust safeguards for political expression, assembly, and association rights in digital spaces.[24]

Internet Fragmentation and Global Interoperability

Internet fragmentation often termed the “splinternet” refers to the process by which the global internet fractures into isolated national or regional networks due to divergent regulatory, technical, or political imperatives. Digital sovereignty initiatives such as data localization mandates, national firewalls, and content controls contribute directly to this phenomenon by requiring that data generated within a territory be stored or processed locally, thereby impeding seamless cross-border data flows and increasing latency for international traffic. Sovereign internet laws in China and Russia exemplify how technical measures such as deep packet inspection and domain name system filtering enforce national boundaries in cyberspace, undermining the end-to-end principle that historically enabled unfettered global connectivity.[25]

Fragmentation poses significant challenges for global interoperability of critical infrastructure. Undersea cable disruptions and regional network separations reduce redundancy and resilience, making networks more vulnerable to localized failures and cyberattacks. For businesses and

[23] Id. at 19.
[24] Supra, at 10.
[25] Supra, at 9.

ISSN: 2582-6433

researchers, fragmented architectures complicate cloud services deployment and data sharing, increasing operational costs and legal compliance burdens. The 2024 Internet Governance Forum's discussions highlighted how fragmentation disproportionately affects developing countries with limited resources to build sovereign data centers, exacerbating the digital divide and entrenched inequalities in access to information and economic opportunities.[26]

From a human rights perspective, splintered networks risk undermining freedom of expression and access to information by creating jurisdictional silos where content deemed lawful in one jurisdiction is criminalized or inaccessible in another. This segmented environment complicates advocacy efforts that rely on transnational solidarity and knowledge exchange, weakening global civil society coalitions and impeding collective action on issues such as climate change, human rights abuses, and public health emergencies. Ensuring global interoperability, therefore, requires international cooperation to harmonize data governance standards, promote mutual recognition of cybersecurity frameworks, and safeguard the open architecture that underpins the internet's role as a driver of innovation, human rights, and inclusive development.[27]

Conclusion

The competing paradigms of digital sovereignty and open internet each offer vital contributions to digital governance but fall short when pursued in isolation. Digital sovereignty empowers states to protect national security, cultural values, and economic autonomy, yet it often does so at the expense of individual freedoms, generating network fragmentation, censorship, and unequal access. Conversely, the open internet model maximizes freedom of expression, innovation, and global collaboration but struggles to safeguard privacy, prevent corporate overreach, and ensure accountability. The resulting landscape is one of fragmented networks and uneven rights protections that disproportionately impact vulnerable communities and undermine the internet's potential as a global public good.

A sustainable path forward requires hybrid governance frameworks that integrate the legitimate aims of sovereignty security, cultural preservation, and economic resilience with the

[26] Vladimer Svanadze, Maksim Iavich and Viktoriia Lukashenko, *Geopolitical and Technical Dimensions of Internet Fragmentation*, 3991 CEUR 578, 580-586 (2025).
[27] Id. at 23.

ISSN: 2582-6433

fundamental human rights enshrined in open internet principles. Such frameworks must be adaptive, rights-based, and inclusive, leveraging multistakeholder input and international cooperation to navigate the complex dynamics of emerging technologies and geopolitical rivalries. By harmonizing regulatory standards and fostering interoperable architectures, the global community can uphold both state interests and universal digital rights, ensuring that the internet continues to advance human dignity, democracy, and shared prosperity.

Policy Recommendations

- Establish international agreements on minimum human rights protections in digital governance that bind states to uphold freedom of expression, privacy, and access to information even when exercising digital sovereignty.
- Develop interoperable data governance standards that facilitate cross-border data flows under mutually recognized safeguards, minimizing fragmentation while respecting national security and cultural concerns.
- Implement transparent oversight mechanisms for emergency measures such as internet shutdowns and content takedowns, including judicial review and clear sunset clauses to prevent indefinite restrictions on fundamental rights.
- Strengthen multistakeholder governance bodies by ensuring equitable representation of civil society, technical experts, and marginalized communities in policymaking processes, fostering accountability and legitimacy.
- Promote adaptive regulation of emerging technologies such as artificial intelligence and blockchain through risk-based frameworks that embed human rights impact assessments and enable periodic policy reviews.
- Encourage capacity-building in developing and least-connected regions to close the digital divide, investing in infrastructure, digital literacy, and inclusive policies that guarantee universal access and meaningful participation in the digital ecosystem.

References

1. *Internet Rights & Principles Coalition*, Internet Governance Forum United Nations, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf
2. Julia Pohle and Thorsten Thiel, *Digital Sovereignty*, 9(4) Concepts of digital society 3 (2020).

ISSN: 2582-6433

3. *Joint Statement on Protecting Human Rights Online and Preventing Internet Shutdowns in Times of Armed Conflict*, Freedom Online Coalition, *https://freedomonlinecoalition.com/joint-statement-on-protecting-human-rights-online-and-preventing-internet-shutdowns-in-times-of-armed-conflict/*
4. *History of the Internet*, WIKIPEDIA, https://en.wikipedia.org/wiki/History_of_the_Internet
5. Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, *A Brief History of the Internet, https://www.internetsociety.org/internet/history-internet/brief-history-internet/*
6. Julien NOCETTI, A Splintered Internet? Internet Fragmentation and the Strategies of China, Russia, India and the European Union, IFRI (Feb 27, 2024), https://www.ifri.org/en/studies/splintered-internet-internet-fragmentation-and-strategies-china-russia-india-and-european
7. *Digital Sovereignty and Citizens' Rights*, European Movement International, https://europeanmovement.eu/policy/digital-sovereignty-and-citizens-rights-2/
8. Marilia Maciel, *Digital sovereignty: The end of the open internet as we know it? (Part 1),* https://www.diplomacy.edu/blog/digital-sovereignty-the-end-of-the-open-internet-as-we-know-it-part-1/
9. "No Internet Means No Work, No Pay, No Food", Internet Shutdowns Deny Access to Basic Rights in "Digital India", https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic
10. David Inserra, *Pro-Brazilian Censors Strike Back: Digital Sovereignty Versus Free Speech Online*, CATO INSTITUE (Sep 25, 2024), https://www.cato.org/blog/pro-brazilian-censors-strike-back-digital-sovereignty-versus-free-speech-online
11. Shreya Singhal v. Union of India, AIR 2015 SC 1523**.**
12. Ian Barber and Maria Paz Canales, *What would a human rights-based approach to platform regulation look like?*, GLOBAL PARTNERS DIGITAL (July 30, 2024), https://www.gp-digital.org/what-would-a-human-rights-based-approach-to-platform-regulation-look-like/
13. Data Protection Laws of the World, *DLA PIPER*, https://www.dlapiperdataprotection.com/?t=law&c=IN
14. K.S. Puttaswamy vs. Union of India (2017), 10 SCC 1.

ISSN: 2582-6433

15. *Privacy in Peril: India's Interception Regime*, Jyoti Panday and Saumya Jain (Dec 13, 2024), https://www.legalbluebook.com/bluebook/v22/rules/18-the-internet-electronic-media-and-other-nonprint-resources/18-2-the-internet
16. Takahisa Kawaguchi, *How democratic states are regulating digital platforms*, INSTITUTE OF GEOECONOMICS (Apr 10, 2024), https://instituteofgeoeconomics.org/en/research/2024041057049/
17. Vladimer Svanadze, Maksim Iavich and Viktoriia Lukashenko, *Geopolitical and Technical Dimensions of Internet*
18. *Fragmentation*, 3991 CEUR 578, 580-586 (2025).

***