SUPREMO AMICUS

VOLUME 40 | February, 2026 Peer Reviewed | Refereed Journal

CYBER SOVEREIGNTY, HUMAN RIGHTS, AND DATA PROTECTION: A COMPREHENSIVE ANALYTICAL STUDY

By *Rethiga Ramesh*
LLM at *Tamil Nadu DR.Ambedkar Law University, School of Excellence in Law, Tamil Nadu, Chennai.*

ABSTRACT

India's digital transformation has brought to the forefront a critical intersection between cyber sovereignty, human rights, and data protection. As the state seeks to consolidate control over its digital ecosystem amid growing dependence on foreign technology platforms, tensions arise between security-oriented sovereignty assertions and constitutional commitments to privacy, liberty, and equality. The country's evolving data protection landscape anchored by the Digital Personal Data Protection Act (DPDPA) 2023 represents a decisive attempt to assert digital sovereignty while addressing governance gaps across sectors such as finance and health. Initiatives like the Reserve Bank of India's Central Bank Digital Currency (CBDC) and digital health infrastructures highlight both the promise of sovereign innovation and the risks of surveillance, inadequate consent, and weak institutional enforcement.

This study critically examines India's policy approach through legal, institutional, and rights-based lenses, emphasizing challenges in balancing national control with global interoperability and technological progress. It identifies structural deficiencies in cross-border enforcement, fragmented regulatory oversight, and limited integration of intersectional human rights protections within digital governance. The paper advocates for inclusive, multi-stakeholder frameworks that operationalize human rights principles, strengthen institutional accountability, and promote digital literacy. Through this lens, India's pursuit of digital sovereignty underscores a broader global struggle to reconcile state power, technological autonomy, and human dignity within the evolving architecture of cyberspace governance.

KEYWORDS: *Cyber Sovereignty, Human Rights, Data Protection, Digital Personal Data Protection Act (DPDPA) 2023 and Digital Governance.*

I. INTRODUCTION

Cyber sovereignty refers to a state's authority to regulate online activities within its borders, shaping how nations govern cyberspace amid expanding digitalization. China's model emphasizes state control over information and technology to preserve social and political stability, contrasting with Western democracies that advocate openness, free expression, and multi-stakeholder governance. The divergent interpretations of cyber sovereignty reflect deeper geopolitical, legal, and cultural distinctions ranging from strict territorial control to cooperative digital governance. The European Union's concept of digital sovereignty focuses on strengthening technological autonomy and protecting EU values and markets.

Simultaneously, the increasing importance of cyberspace in national security and economic infrastructures intensifies global competition over digital governance. Human rights, particularly privacy and freedom of expression, face growing challenges as states invoke sovereignty to justify surveillance, censorship, and data localization. The rise of AI, big data, and cloud technologies adds new layers of complexity, often prioritizing state security over individual freedoms. These technologies raise concerns over algorithmic bias, transparency, and data control, pressing legal systems to reconcile innovation with rights protection. Consequently, cyber sovereignty debates underscore the struggle to balance state interests, technological advancement, and human rights within an interconnected yet fragmented digital order.

The emergence and articulation of cyber sovereignty is the principle that each nation has the right to control digital activities within its territory, has profoundly

shaped the protection of human rights and data protection in both national and global digital governance frameworks.

At the national level, cyber sovereignty enables states to establish and enforce local laws governing data storage, transfer, and surveillance. For example, India's push for digital sovereignty, propelled by the dominance of foreign digital platforms, has led to calls for data localization and stringent regulations on cross-border data flows to fortify state control and protect citizens' rights. The introduction of legislative reforms like the Personal Data Protection Bill reflects a commitment to build independent oversight mechanisms, strengthen cybersecurity, and delineate state jurisdiction over digital assets. However, such sovereignty-centric approaches can have dual effects: while they may enhance citizens' data protection by limiting extraterritorial misuse, they also risk expanding state surveillance and potentially curbing privacy and freedom of expression without robust safeguards.

Globally, cyber sovereignty has triggered jurisdictional conflicts as data flows transcend borders, complicating the harmonization and enforcement of privacy laws. Disparate national laws often lead to fragmentation in global digital governance, hindering seamless data transfer and consistency in protecting individual rights. The lack of mutually recognized standards for cross-border data enforcement exacerbates these challenges, sometimes leaving individuals vulnerable to rights violations by foreign corporate or state actors.

Institutional challenges further compound these issues. Overlapping jurisdictions, weak enforcement, and inconsistent policies impair the effectiveness of human rights protections, while technological advancements outpace the adaptability of current frameworks. Vulnerable groups such as women and marginalized communities often face disproportionate risks, making it imperative for states to adopt inclusive, rights-respecting digital governance that integrates ongoing stakeholder dialogue.

1.1 CONCEPTUALIZING CYBER SOVEREIGNTY

Cyber sovereignty represents the extension of state authority into cyberspace, encompassing related notions such as data, digital, and technological sovereignty. While cyber sovereignty emphasizes national control over online activities and infrastructure, data sovereignty focuses on state regulation of data generation, storage, and transfer. Digital sovereignty broadens this view to include autonomy over digital infrastructure and services, and technological sovereignty underscores self-sufficiency in critical technologies[1]. Different states operationalize these ideas in line with political and strategic priorities: China adopts a strong state-centric model prioritizing control and security; the European Union promotes digital sovereignty through market integrity, rights protection, and competitiveness; and the United States supports an open internet grounded in multistakeholder governance[2].

Historically, cyber sovereignty evolved from debates on internet governance and state control over cyberspace. The rise of cybersecurity threats, technological dependencies, and foreign influence has driven states to assert digital borders—a move often termed the "territorial turn" of cyberspace. China's Great Firewall epitomizes the legal and technical assertion of sovereignty online. Internationally, cyber diplomacy has become instrumental in legitimizing sovereignty claims and aligning national interests with global cooperation in cybersecurity and digital trade.

[1] E. Fauzi, H. Citra, E. Marwenny, N. Alfitrianti, "Control of Personal Data and Cyber Space by Global Digital Platforms in Relation to Indonesia"s Digital Sovereignty," None, 2024. https://doi.org/10.69989/5f8ff494

[2] Y. McDermott, "Conceptualising the right to data protection in an era of Big Data," SAGE Publishing, 2017. https://doi.org/10.1177/2053951716686994

Theoretically, cyber sovereignty intersects with political economy and international law, illustrating how information and technology are leveraged for geopolitical power. Critics argue that such claims risk reinforcing digital protectionism, restricting openness, and undermining human rights. Alternative perspectives, including decolonial and pluralist approaches, advocate for inclusive, polycentric governance models that move beyond traditional, state-centric sovereignty frameworks.

1.2 RESEARCH QUESTION

In light of these challenges and dynamics, the primary research question guiding this study is:

- How does the emergence and articulation of cyber sovereignty impact the protection of human rights and data protection within national and global digital governance frameworks?
- How do diverse state conceptions of sovereignty shape regulatory approaches toward cyberspace, and what are the implications for privacy, freedom of expression, and data governance?
- How do emerging technologies like AI influence this terrain, and what gaps exist in current legal and policy frameworks?

1.3 OBJECTIVES OF THE RESEARCH

The objective of this research is threefold:

- To critically analyze the conceptualization and operationalization of cyber sovereignty across key states and regions
- To evaluate the intersections and conflicts between sovereignty-based governance and human rights protections, notably in data protection laws
- To identify key regulatory gaps and challenges arising from new technologies and geopolitical competition.

This provides a foundation for advancing scholarly understanding and policymaking in digital governance, aiming to reconcile sovereignty interests with human rights imperatives in an increasingly complex cyberspace.

1.4 RESEARCH GAP IDENTIFICATION

Insufficient Integration of Human Rights in Sovereignty Policies

A prevalent gap lies in the limited integration of human rights considerations within sovereignty policies. Many sovereignty assertions prioritize territorial control and security without harmonizing them with global human rights frameworks. Empirical studies examining the impacts of sovereignty claims on digital rights are sparse, impeding a comprehensive understanding of consequences on privacy, expression, and data protection. There is a pressing need for theoretical and practical frameworks reconciling state sovereignty with an effective safeguarding of human rights.

Underexplored Effects of Emerging Technologies

The intersection of cyber sovereignty with emerging technologies such as AI, big data, and metaverse environments remains underexplored. Regulatory frameworks often lag behind technological advancements, inadequately addressing challenges inherent in these domains. Notably, mechanisms extending data autonomy beyond individual rights to encompass organizational and collective dimensions are underdeveloped. Addressing the role of technology in reshaping governance and sovereignty boundaries demands significant scholarly and policy attention.

Enforcement and Cross-Border Regulatory Conflicts

Cross-border enforcement of data protection laws faces profound challenges, with jurisdictional conflicts and varying enforcement capacities limiting effectiveness. Developing regions often contend with weak institutional frameworks and fragmented policies, hindering cyber resilience and rights protection. Moreover, the role of corporate actors and the private sector requires inclusion in multi-

stakeholder governance models to bridge existing regulatory lacunae.

1.5 METHODOLOGY

Research Design and Approach

This study adopts a qualitative documentary and policy analysis framework to examine conceptions and implementations of cyber sovereignty and human rights protection. Comparative case study methods focus on China, the European Union, and other selected regions to elucidate divergent approaches and common challenges. Normative legal analysis underpins the examination of regulatory texts, identifying gaps and best practices in current governance frameworks.

Data Sources and Selection Criteria

Primary data include legislative texts, regulations, policy documents related to cyber sovereignty, data protection, and human rights from international, regional, and national sources. Secondary sources encompass academic literature, policy reports, and international guidelines, enriched by recent studies on AI governance, digital identity, and data sovereignty. Selection emphasizes contemporaneous and relevant legal and policy instruments from jurisdictions illustrating key conceptual and operational trends[3].

Analytical Techniques

Thematic content analysis, supplemented by machine learning techniques for large document sets, facilitates the identification of core themes and regulatory gaps. Cross-jurisdictional comparisons enable assessment of policy congruencies and divergences, while critical evaluation addresses human rights compliance and governance efficacy. This mixed analytical strategy supports a holistic understanding of cyber sovereignty's multifaceted impacts.

II. HUMAN RIGHTS IN THE CYBER REALM

2.1 Privacy and Data Protection as Fundamental Rights

Privacy and data protection constitute core human rights in the digital age, grounded in legal frameworks that have evolved to address the complexities of personal information processing in cyberspace. The European Union's recognition of a standalone fundamental right to data protection—distinct from privacy—marks a significant development following the Lisbon Treaty and the Charter of Fundamental Rights[4]. The GDPR epitomizes the operationalization of this right, imposing stringent obligations on data controllers and processors, emphasizing transparency, autonomy, and nondiscrimination. However, these legal frameworks face challenges posed by the scale and sophistication of big data practices and AI systems, which complicate issues of consent, data accuracy, and control over personal information[5]

2.2 Freedom of Expression and Digital Participation

Freedom of expression under digital sovereignty regimes often encounters limitations stemming from state-imposed content regulations and censorship. In authoritarian contexts, such as China and Russia, content regulation models exemplify tight state control over online information to maintain social stability and political authority, frequently constraining digital rights. The emergence of legislative frameworks like the EU Digital Services Act aims to safeguard democratic values by promoting

[3] L. Li, "Data Sovereignty and National Security: Governance Challenges and Pathways in the Digital Age," None, 2025. https://doi.org/10.63802/grhas.v1.i1.7

[4] L. Gisel, T. Rodenhuser, K. Drmann, "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts," Revue Internationale de la Croix-Rouge, 2020. https://doi.org/10.1017/S1816383120000387

[5] A. Mantelero, "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment," Elsevier BV, 2018. https://doi.org/10.1016/j.clsr.2018.05.017

platform accountability and protecting fundamental rights on the internet, though these efforts face challenges balancing regulation and innovation.

2.3 Intersectionality and Vulnerability in Digital Rights

Digital rights frameworks must also recognize the intersectional vulnerabilities of marginalized groups, including Indigenous peoples, who face unique challenges in data governance. Existing privacy regulations often neglect collective rights and cultural specificities, as explored in the Māori context of Aotearoa, where alternative privacy paradigms seek to respect Indigenous data sovereignty. Furthermore, crisis contexts such as the COVID-19 pandemic have amplified concerns over large-scale digital surveillance through contact tracing applications, necessitating robust data protection standards to prevent rights infringements. Digital identity systems carry risks of discrimination and exclusion, highlighting the need for inclusive governance that addresses these emergent issues[6].

III. DATA PROTECTION LAWS AND REGULATORY FRAMEWORKS

3.1 Regional and National Data Protection Regimes

Globally, data protection regimes exhibit considerable variation yet share commitments to safeguarding personal data within their jurisdictions. The GDPR in Europe has set a high standard for data protection, influencing other regions' legal architectures. China's Personal Information Protection Law (PIPL) and the US California Consumer Privacy Act (CCPA) represent significant, albeit distinct, regulatory approaches. On the African continent, the Malabo Convention underscores efforts to harmonize data protection frameworks across member states to support socio-economic development while protecting privacy. Country-specific analyses reveal diverse challenges and policy responses: Indonesia grapples with the dominance of foreign platforms and the need for comprehensive data sovereignty policies, Malaysia balances rapid digital growth with privacy protections embedded within its legislation, while South Africa integrates democratic principles within its cybersecurity and privacy frameworks[7].

3.2 Data Sovereignty and National Security Concerns

The articulation of data sovereignty increasingly intersects with national security considerations, as data becomes a strategic resource. States pursue stringent data governance models to secure critical infrastructure and safeguard economic interests amid global data flows and cyber threats. Governance challenges arise in managing digital borders and cloud infrastructures, requiring coordinated policies that mediate between protectionism and the benefits of globalization.

3.3 Gaps and Limitations in Current Legal Frameworks

Despite advances in data protection legislation, significant enforcement limitations and regulatory inconsistencies remain. Many African countries face institutional capacity challenges, fragmented policies, and weak oversight mechanisms, impeding effective protection. Emerging technologies like AI, digital identity systems, and metaverse platforms pose new regulatory challenges unaddressed adequately by existing frameworks. The lack of transparent and accountable governance structures further undermines rights protections and public trust.

[6] M. Vui, "European Union's Quest for Digital Sovereignty: Policy Continuations and Strategy Innovations," None, 2021. https://doi.org/10.18485/iipe_euchanges.2021.ch5

[7] E. Celeste, F. Fabbrini, "Competing Jurisdictions: Data Privacy Across the Borders," Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-54660-1_3

IV. CYBER SOVEREIGNTY AND ITS IMPACT ON HUMAN RIGHTS AND DATA PROTECTION

4.1 State-Centric Control vs. Multistakeholder Internet Governance

A fundamental divide characterizes global cyberspace governance between state-centric sovereignty models, as exemplified by China, and the multistakeholder approach historically favored by Western states. The former prioritizes state control and regulation within national borders, often restricting openness and cross-border collaborations, while the latter emphasizes decentralized governance, openness, and participation by diverse actors. This cleavage impacts digital rights, the freedom to access and share information, and the norms underpinning cybersecurity and internet governance at the international level.

4.2 Privacy Concerns in Sovereignty-Driven Regulatory Regimes

Sovereignty-driven regimes often implement mechanisms such as data localization and restrictive cross-border data flow policies, with implications for privacy and surveillance. Such policies risk perpetuating opacity in the exercise of state power, raising ethical and legal challenges around transparency and accountability. Corporate power also plays a significant role in this ecosystem, with global digital platforms managing substantial volumes of personal data, sometimes in tension with state sovereignty and individual privacy[8].

4.3 Implications for Democratic Principles and Human Rights Protections

The intersection of cybersecurity imperatives and freedom of expression highlights the delicate balance required to uphold democratic principles in the digital era. Implementing cybersecurity policies that respect human rights remains fraught with challenges, including overbroad surveillance and restrictions on information flows. The rising prominence of digital sovereignty heightens tensions between state control and international human rights norms, necessitating frameworks that reconcile these competing demands.

V. COMPARATIVE CASE STUDIES

5.1 China's Cyber Sovereignty and Governance Model

China's cyber sovereignty approach rests on comprehensive state control mechanisms, epitomized by the Golden Shield project, which fuses a technological infrastructure with a complex legal framework to enforce informational and political control, emphasizing social stability and state security[9]. The integration of AI governance within this model aims to extend control capabilities, address national security threats, and shape digital order domestically and internationally. China's engagement with global cyber governance initiatives seeks to balance asserting sovereignty while participating constructively in evolving governance regimes[10].

5.2 European Union's Digital Sovereignty Vision

The EU's digital sovereignty agenda has evolved from regulatory capitalism toward what has been termed regulatory mercantilism, focusing on reclaiming control over technological infrastructure and digital markets amid dependence on foreign providers. This shift aims to bolster economic competitiveness, data protection, and cybersecurity[11]. The EU foregrounds

[8] M. R. Carrillo, "Sovereignty vs. Digital Sovereignty," None, 2023. https://doi.org/10.21202/jdtl.2023.29

[9] Y. C. Chin, K. Li, "SOVEREIGNTY IN THE CYBERSPACE: CONTESTATION OF CONCEPTS AND POLICIES," None, 2021. https://doi.org/10.5210/spir.v2021i0.12153

[10] R. Creemers, "China"s Conception of Cyber Sovereignty: Rhetoric and Realization," RELX Group (Netherlands), 2020. https://doi.org/10.2139/ssrn.3532421

[11] T. Komukai, "A Comparative Study of the Extraterritorial Enforcement of Data Protection Rules in the EU, US and Japan," Global Privacy Law Review, 2020. https://doi.org/10.54648/gplr2020095

human rights in its legislative measures, notably GDPR and Digital Services Act, embedding rights protection within its vision of sovereignty. Nonetheless, challenges persist regarding global competitiveness and maintaining technological autonomy in a rapidly shifting international landscape[12].

5.3 Developing and Regional Responses: Africa and Indonesia

The African Union's Agenda 2063 integrates data protection and cybersecurity as pillars for sustainable development, though enforcement and harmonization across member states remain inconsistent[13]. The Malabo Convention and regional frameworks signal progress but institutional and awareness gaps pose ongoing challenges. Indonesia's digital sovereignty quest confronts the dominance of foreign digital platforms and resultant sovereignty dilemmas, prompting legal reforms focusing on data protection, cybersecurity, and administrative coordination to assert national digital governance and protect human rights. These contexts illustrate the varied trajectories and policy imperatives shaping digital sovereignty in developing regions[14].

VI. INDIAN PERSPECTIVE ON CYBER SOVEREIGNTY, HUMAN RIGHTS, AND DATA PROTECTION

India's digital transformation highlights a complex balance between asserting national sovereignty in cyberspace and safeguarding individual rights. As the world's largest democracy and emerging digital power, India's policies reflect both aspirations for autonomy from foreign technological dominance and the constitutional imperative to protect privacy, freedom, and equality. The challenge lies in reconciling cybersecurity and governance priorities with human rights protection in a rapidly digitizing economy marked by deep socio-economic disparities. Cyber sovereignty debates in India intersect with issues of data governance, digital infrastructure control, and equitable access to technology.

1. **Evolving Data Protection and Digital Sovereignty Issues**
   India's digital sovereignty concerns center on controlling data generated within its territory and reducing dependence on global technology platforms. The dominance of foreign entities in India's digital ecosystem raises issues of jurisdiction, data misuse, and the extraterritorial reach of foreign data laws. Legislative initiatives, particularly the Personal Data Protection (PDP) Bill—later replaced by the Digital Personal Data Protection Act (DPDPA) 2023—seek to enhance domestic control by regulating data processing, mandating user consent, and restricting cross-border data transfers. These reforms aim to assert India's sovereign authority while building a secure, globally competitive digital economy. Yet, tensions persist between localization and interoperability, as India continues engaging in international data flows vital to its trade and tech-driven growth[15].

[12] A. Barrinha, G. Christou, "Speaking sovereignty: the EU in the cyber domain," Taylor & Francis, 2022. https://doi.org/10.1080/09662839.2022.2102895

[13] D. G. Phillipose, "The Impact of International Investment Agreements on Human Rights: A Critical Analysis of Balancing Economic Interests and Human Rights Obligations," Journal of Information Systems Engineering & Management, 2025. https://doi.org/10.52783/jisem.v10i11s.1647

[14] H. Mayasari, "A examination on personal data protection in metaverse technology in Indonesia: a human rights perspective," None, 2023. https://doi.org/10.62264/jlej.v1i1.4

[15] R. Usman, "Realizing synergy between the ministry of communication and informatics and the national cyber and crypto agency in the era of government digitalization," Journal of Law Science, 2025. https://doi.org/10.35335/jls.v7i1.5887

2. **Legislative and Institutional Frameworks for Health Data and Privacy**
India's healthcare digitization underscores the urgency of protecting sensitive health data. The PDP and subsequent DPDPA recognize health information as sensitive personal data, imposing strict conditions on its processing. However, enforcement remains fragmented. Agencies like the Ministry of Electronics and Information Technology (MeitY) and sector-specific health regulators often lack coordination, undermining consistent application of privacy and cybersecurity safeguards. The exponential rise of telemedicine, health apps, and AI-based diagnostics intensifies regulatory challenges. Ensuring compliance through principles like "Data Protection by Design and Default" and fostering institutional cohesion remain pivotal to strengthening privacy governance and digital trust in health services[16].

3. **Privacy Risks and Enforcement Challenges**
India's digital proliferation—via mobile connectivity, e-governance, and fintech—has escalated privacy risks for citizens. Pervasive data collection by both corporations and state agencies exposes users to tracking, profiling, and identity theft, while public awareness of data rights remains limited. Despite progressive laws, enforcement suffers from judicial backlog, inadequate institutional capacity, and ambiguity in the scope of enforcement powers. Additionally, extraterritorial challenges complicate oversight when data flows transcend national boundaries. The absence of a fully operational data protection authority and weak grievance redressal exacerbate vulnerabilities. Effective enforcement demands not just robust institutions but also public education and transparent accountability mechanisms.

4. **Monetary and Digital Sovereignty through CBDC**
India's efforts to strengthen sovereignty extend to the financial domain through the Reserve Bank of India's Central Bank Digital Currency (CBDC) initiative. The digital rupee embodies sovereign control over digital financial infrastructure while countering the influence of private cryptocurrencies and global payment systems. The CBDC promises enhanced monetary efficiency, transaction traceability, and cost reduction. However, the extensive data visibility it entails poses concerns over privacy, surveillance, and state access to citizens' financial behaviors. Policymaking must therefore balance economic innovation with privacy guarantees through stringent data usage norms, transparency policies, and oversight mechanisms to prevent misuse.

5. **Gender, Health, and Digital Inequality Dimensions**
India's digital governance initiatives coexist with social inequalities in access, literacy, and representation. Gender-based digital divides persist, where women face heightened risks of privacy violations, online harassment, and limited decision-making autonomy over their data. Similarly, marginalized communities encounter exclusion in digital health and AI-driven systems, risking algorithmic bias and data misuse. Achieving an inclusive digital society requires embedding intersectional protections in law and policy—addressing gender, class, disability, and rural divides. Equitable access, literacy drives, and participatory digital governance can transform India's sovereignty model into one that empowers all citizens rather than entrenches disparities.

India's trajectory in cyber sovereignty and data

[16] L. DeNardis, "Introduction: Internet Governance as an Object of Research Inquiry," The MIT Press, 2020. https://doi.org/10.7551/mitpress/12400.003.0002

protection reflects its dual ambition—to secure national digital autonomy while upholding democratic accountability. Legislative frameworks like the DPDPA 2023, initiatives in cybersecurity, and the CBDC pilot mark significant strides, yet sustained progress depends on institutional capacity, human rights safeguards, and international dialogue. Future policy must harmonize sovereignty assertions with India's constitutional values of liberty and dignity. Building transparent institutions, ensuring corporate accountability, and closing digital divides will be central to realizing a balanced model of digital sovereignty is the one that supports innovation, protects citizens, and reinforces India's democratic ethos in the evolving global cyber order.

VII CRITICAL ANALYSIS

7.1 Data Sovereignty: Motivation, Approaches, and Legal Gaps

National Imperatives

At the core, India's digital sovereignty attempts to reclaim domestic authority over data generated within its territory, motivated by:

1. Geopolitical concerns about foreign surveillance and influence,
2. Economic ambition to foster local digital enterprise,
3. Human rights aspirations to protect citizens' data and autonomy.

Mitigating foreign influence, particularly the dominance of US- and China-based digital platforms has led to calls for data localization, stricter regulation on cross-border data flows, and legislative frameworks like the Personal Data Protection Bill (PDP). The PDP Bill sought to install a robust data protection regime, empower a dedicated data authority, and enhance digital sovereignty, giving India control over both digital infrastructure and information assets[17].

However, such state-centric assertions risk impinging on individual freedoms, potentially normalizing sweeping surveillance, and diminishing global interconnectivity.

Regulatory and Enforcement Challenges

Critical gaps persist in:

1. Institutional clarity and effectiveness due to overlapping agency responsibilities, fragmentation, and coordination failures,
2. Practical enforceability in extraterritorial data scenarios, as major platforms reside outside India's jurisdiction,
3. Consistency and robustness in addressing new domains such as digital health, digital identity, and blockchain-based environments.

Furthermore, data localization, while boosting sovereignty, risks stifling innovation and impeding data-driven international commerce, underlining the importance of harmonized yet flexible laws.

7.2 Human Rights and Privacy: Achievements and Vulnerabilities

Progress and Risks

India's legal tradition, grounded in constitutional guarantees of privacy as a fundamental right, has shaped its approach to data governance. Yet, implementation lags behind legislative ambition:

The collection and dissemination of personal data, especially by multinational and state actors, pose acute privacy and data security risks to individuals.

Vulnerable populations such as women, marginalized castes, and the digitally illiterates face disproportionate exposure to privacy violations, bias in digital systems, and exclusion from digital services[18].

[17] "Data Sovereignty," Oxford University Press, 2023. https://doi.org/10.1093/oso/9780197582794.001.0001

[18] R. Rodrigues, "Legal and human rights issues of AI: Gaps, challenges and vulnerabilities," Elsevier BV, 2020. https://doi.org/10.1016/j.jrt.2020.100005

A persistent gap exists in aligning data protection frameworks with global best practices while ensuring they are sensitive to local equity and access issues[19].

7.3 Technological and Societal Complications

As digital health, AI, and fintech expand, data generated holds immense social value but is susceptible to misuse, discrimination, and government or corporate overreach. Ensuring rights-friendly oversight in incorporating Data Protection by Design, strong redress mechanisms, and transparent operations is vital to public trust and social equity.

Cases of mass surveillance (for instance, through Aadhaar, India's biometric ID system) highlight tensions between state imperatives of security/social control and the rights to privacy and data minimization. Without stringent safeguards, such mega-infrastructures risk violating both individual and collective rights.

VIII. POLICY RECOMMENDATIONS

1. Clarify and Strengthen Legal and Institutional Structures:

Accelerate the operationalization of Data Protection Authorities, ensuring independence, adequate resources, and clear mandates to harmonize enforcement.

Reform overlapping and conflicting mandates between agencies such as the Ministry of Electronics and Information Technology and specialized regulators, drawing on international best practices.

2. Build Rights-Respecting, Inclusive Data Governance:

Embed human rights principles across every level of data protection legislation, emphasizing the most vulnerable groups: minorities, women, children, and the disabled.

Mandate privacy by design in all digital infrastructure, with ongoing assessment and adaptative regulatory updating as technology and threats evolve.

3. Foster Participatory and Multi-Stakeholder Governance:

Create formal processes for civil society, industry, and citizen input into data governance and digital sovereignty policies to ensure accountability and transparency.

Encourage open, public debate on the societal trade-offs of digital sovereignty, particularly regarding surveillance, localization, and innovation.

4. Address Enforcement and Cross-Border Regulatory Gaps:

Develop bilateral/multilateral agreements for cross-border data transfer and enforcement, recognizing both India's sovereignty needs and the global nature of cyberspace.

Promote global dialogue for interoperable data protection regimes that both respect sovereign imperatives and protect individual rights.

5. Promote Digital Literacy and Awareness:

Invest in nationwide digital education, prioritizing awareness campaigns about privacy rights, data risks, and redress mechanisms, especially among marginalized and low-literacy populations.

Encourage public-sector and industry partnerships to facilitate accessible, user-friendly privacy tools and digital safety resources.

6. Innovate for Social Equity:

Integrate intersectional perspectives such as gender, caste, region - into policy frameworks to ensure technology serves diverse populations without discrimination or exclusion.

[19] R. Siagian, L. Siahaan, M. I. Hamzah, "Human Rights in The Digital Era: Online Privacy, Freedom Of Speech, and Personal Data Protection," None, 2023. https://doi.org/10.56778/jdlde.v2i4.149

Institutionalize regular impact assessments of major digital systems (Aadhaar, CBDC, health grids) with an explicit focus on rights, access, and inclusion.

IX. CONCLUSION

India's approach to cyber sovereignty, human rights, and data protection illustrates the intricate balancing act between asserting national control and upholding democratic freedoms in an era of rapid digitalization. Legislative milestones such as the Digital Personal Data Protection Act (DPDPA) 2023 and initiatives like the Central Bank Digital Currency (CBDC) mark significant strides toward establishing regulatory and technological sovereignty. Yet, these advances simultaneously expose the persistent fragility of India's institutional enforcement, coordination across sectors, and integration of privacy and equality principles into digital governance.

To ensure a rights-respecting model of cyber sovereignty, India must reconcile its security imperatives with international obligations and constitutional protections. This requires not only stronger data protection authorities and harmonized regulatory frameworks but also ongoing public participation, transparency, and accountability. Emphasizing digital literacy, inclusivity, and intersectional equity will be central to embedding human rights into every layer of technological governance.

Ultimately, India's digital pathway offers both a challenge and an opportunity: to craft an indigenous yet globally responsible model of cyber governance that reinforces trust, innovation, and citizen empowerment. By aligning digital sovereignty with the values of liberty, dignity, and justice, India can emerge as a democratic exemplar in shaping the normative future of cyberspace governance.

*****