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

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL SOVEREIGNTY VS CORPORATE HEGEMONY: AN ANALYSIS OF INDIAN PRIVACY LAW

AUTHORED BY - SRISHTI DARJI
SY.B.ALL.B Student
KES' Shri. Jayantilal H. Patel Law College
Mumbai University.

ABSTRACT

Today, data is far more than just raw information—it has become one of the most powerful resources contested by both governments and global technology corporations. This has created a "tug of war" between countries that want to set their own rules and global tech corporations that currently dominate the digital world. This paper examines these tensions through the lens of India's evolving data protection framework, the Digital Personal Data Protection Act, 2023 (DPDP Act) and its operational rules notified in November 2025. India's data protection laws are part of a larger postcolonial discourse, in which the dominance of a handful of Western technology corporations is seen as replicating historical patterns of extraction and dependency. While the DPDP Act introduces meaningful rights for data principals, its broad government exemptions, weakened enforcement structures, and retreat from strict data localization end up both resisting and accommodating corporate power. The paper concludes by reflecting whether India's model can serve as a viable 'third way' in global digital governance.

I. Introduction

In the modern digital age, data has become the most contested resource of our time. As societies transition into a data-driven economy, power no longer resides solely with sovereign states but is increasingly wielded by technology corporations. Managing personal data gives entities structural power that challenges traditional notions of sovereignty and the foundational principle of Westphalian sovereignty. With over 850 million internet users and a projected trillion-dollar digital economy by 2030, India faces critical questions about who governs data.[1] It is a question of democratic agency, economic autonomy, and postcolonial identity.

[1]Rau's IAS, Digital Sovereignty: India's Strategic Imperative in the Emerging Tech Order (2025), available at https://compass.rauias.com (last visited Apr. 11, 2026). India hosts over 850 million internet users and its digital economy is projected to exceed $1 trillion by 2030.

ISSN: 2582-6433

The concept of digital sovereignty has entered the vocabulary of governments across the ideological spectrum. From the European Union's General Data Protection Regulation (GDPR) to China's Great Firewall, states have developed varying instruments to assert jurisdictional control over digital infrastructure, data flows, and platform governance. Yet, each model raises debates about whether it protects individual data rights or serves state control over national resources.

India's path to data governance has been protracted, spanning more than a decade of consultations, withdrawn bills, and politically charged negotiations with Silicon Valley. The final enactment of the Digital Personal Data Protection Act in August 2023, and the notification of its implementing Rules in November 2025, represent a defining moment in that journey.[2]

India has made an attempt at self-reliance to reduce its dependence on foreign Big Tech companies through the Digital Personal Data Protection Act, 2023 and the subsequent Rules of 2025. This paper provides a critical analysis of how India, through these legislative measures, aims to ensure data protection and digital sovereignty over the hegemony of technology giants.

II. The Legislative History of Indian Privacy Law

A. The IT Act Era (2000–2017)

Until the enactment of the DPDP Act in 2023, India lacked a comprehensive, standalone data protection statute. Personal data was regulated, inadequately, under Section 43A of the Information Technology Act, 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.[3] This framework was narrow in scope—it applied only to corporate entities, and not the government—protecting only a defined category of 'sensitive personal data,' leaving the vast majority of personal data unprotected. In the assessment of many experts, the framework was designed to protect the business interests of India's information technology sector rather than the privacy of Indian citizens.

[2]Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023) [hereinafter DPDP Act]; Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, notified Nov. 13, 2025 [hereinafter DPDP Rules 2025].

[3]Information Technology Act, No. 21 of 2000, India Code (2000); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Ministry of Communications & Information Technology.

ISSN: 2582-6433

B. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)

The real turning point in India's privacy jurisprudence came with the Supreme Court's landmark ruling by a nine-judge constitutional bench in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017).[4] The Court held, unanimously, that the right to privacy is a fundamental right under Article 21 of the Constitution of India, inhering in every person as a natural and inseparable dimension of individual dignity and autonomy. Beyond establishing privacy as a constitutional value, the judgment explicitly identified informational privacy—the right of individuals to control data about themselves—as a core component of that right. This framing set the foundation for all subsequent debates about data protection legislation.

C. From the Srikrishna Committee to the DPDP Act (2018–2023)

Following the *Puttaswamy* judgment, the Government of India constituted a Committee of Experts chaired by retired Supreme Court Justice B.N. Srikrishna. The Srikrishna Committee's 2018 report and accompanying draft bill were notable for their substantive ambition: they proposed strong data localization requirements, an independent Data Protection Authority, and a comprehensive rights framework.[5] Critically, the Committee was skeptical of the government, believing the government itself should be subjected to the same high standards as private actors.

The legislative journey of the bill from the initial vision to the final 2023 Act was marked by a series of revisions. The Personal Data Protection Bill, 2019, underwent a thorough review by a Joint Parliamentary Committee, was completely withdrawn in August 2022, and was replaced by a substantially revised draft in November 2022—each iteration seeing a weakening of data localization requirements, an expansion of government exemptions, and a reduction in the independence of the proposed regulatory authority.[6] The DPDP Act, finally passed in August 2023 and operationalized through Rules notified in November 2025, reflects the cumulative effect of these retreats.

D. Meta Platforms & WhatsApp v. Competition Commission of India

The wider struggle over digital autonomy reached its peak when the Supreme Court of India, in its proceedings while hearing *Meta Platforms Inc. & WhatsApp v. Competition*

[4]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) (nine-judge constitutional bench holding privacy a fundamental right under Article 21 of the Constitution of India).
[5]Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology 2018).
[6]Personal Data Protection Bill, 2019, Bill No. 373 of 2019, as introduced in Lok Sabha, Dec. 11, 2019; withdrawn Aug. 3, 2022; draft Digital Personal Data Protection Bill, 2022 released for public consultation Nov. 18, 2022.

ISSN: 2582-6433

Commission of India,[7] characterized the company's take-it-or-leave-it policy as a 'decent way of committing theft' of users' data. The Court's consideration of this case influenced the opt-out mechanism of Section 6 of the DPDP Act, 2023, which mandates that consent must be free, informed, and specific, allowing users to accept a service while rejecting data tracking. However, critics argue that in an opt-out system data tracking is turned on by default, requiring users to manually disable it in settings—meaning most data tracking continues unchecked. An opt-in regime, establishing privacy as the default setting, would be preferable.

III. Digital Sovereignty and Corporate Hegemony: A Theoretical Framework

A. The Concept of Digital Sovereignty

Digital sovereignty, as a concept, has evolved from its origins in cybersecurity discourse into a multidimensional political and legal category.[8] It refers to a state's capacity to govern its own digital space—the data generated within its borders, the infrastructure through which that data travels, and the platforms that mediate its citizens' interactions. Scholars have identified at least three distinct registers of the concept: sovereignty as state control over digital infrastructure and platforms; sovereignty as individual autonomy over personal data; and sovereignty as economic self-determination in the digital economy.

These registers are frequently in tension with one another. State sovereignty over digital platforms can be deployed in ways that diminish individual autonomy—as China's experience amply demonstrates. Conversely, an emphasis on individual data rights, as embedded in the EU's GDPR approach, may do little to disturb the structural dominance of foreign corporations. India's policy discourse has been shaped by all three registers simultaneously, producing a framework that is at once nationalistic, rights-oriented, and economically protective.

B. Corporate Hegemony and Surveillance Capitalism

The dominant position of a small cluster of American technology corporations—Google, Meta, Amazon, Microsoft, and Apple—in the global data economy constitutes a form of structural power that exceeds the regulatory reach of most nation-states. These corporations operate transnational data extraction systems embedded in the everyday digital lives of billions

[7]Meta Platforms Inc. & WhatsApp LLC v. Competition Commission of India, SLP (C) No. 6063 of 2024 (Supreme Court of India, 2024).
[8]Julia Pohle, Attributes of Digital Sovereignty: A Conceptual Framework, 14 J. Internet L. & Pol'y (2025); see also Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa, Policy & Internet (Jiang & Belli eds., 2024).

ISSN: 2582-6433

of people, particularly in the Global South.[9]

The theoretical concept of 'surveillance capitalism,' associated with the work of Shoshana Zuboff,[10] describes this system: corporations collect 'behavioral surplus'—data generated as a result of the digital trail left behind every time a user engages with an application—which is then converted into predictive products sold to advertisers and other clients. The profits of this system are privatized by corporations; the social costs—surveillance, manipulation, and erosion of privacy—are borne collectively by users and publics. Because these technology giants operate globally, they often escape the direct regulatory reach of the states whose citizens' data are being harvested.

IV. The DPDP Act, 2023: Key Provisions and Structural Limitations

A. Cross-Border Data Transfers and the Retreat from Localization

The Act's approach to cross-border data transfers represents a significant departure from earlier legislative drafts. Whereas the Personal Data Protection Bill, 2019 had proposed mandatory localization of 'sensitive personal data,' the 2023 Act instead provides that data may be transferred to any country except those specifically restricted by the Central Government through notification.[11] No such list of restricted countries had been published as of April 2026.[12]

By adopting a permissive default—where data transfers are permitted to all countries not specifically blacklisted, rather than a restrictive default confining transfers to a whitelist of safe, approved countries—this approach significantly weakens the data sovereignty dimension of the legislation. Transnational data flows that characterize the current system of corporate hegemony continue largely unimpeded, as no restrictive notifications have been issued to date.

B. Enforcement Architecture: The Data Protection Board

The Data Protection Board of India functions as an adjudicatory body for data disputes. It imposes penalties of up to INR 250 crore on companies violating its provisions, making non-

[9]Nick Couldry & Ulises A. Mejias, The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism (Stanford Univ. Press 2019).
[10]Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs 2019).
[11]DPDP Act, supra note 2, §§ 3, 4. The Act's extraterritorial application extends to processing outside India in connection with offering goods or services to data principals within India.
[12]DLA Piper, Data Protection Laws in India, Data Protection Laws of the World (updated Feb. 2026), available at https://www.dlapiperdataprotection.com (last visited Apr. 11, 2026). The Act adopts a blacklist model; no restricted-country list had been published as of April 2026.

ISSN: 2582-6433

compliance costly.[13] Unlike powerful regulatory bodies such as SEBI or GDPR supervisory authorities, however, the Board is not fully shielded from government influence. Furthermore, because the Board's mandate is purely adjudicatory rather than regulatory, it lacks the power to issue proactive guidance, leaving it ill-equipped to address a technological landscape that evolves faster than legal proceedings. Critically, where a government department is accused of a data breach, the case is heard by the same Board whose members are appointed and removable by the same Central Government.[14] This structure may deter the Board from holding state actors accountable.

C. Significant Data Fiduciaries

Section 10 of the DPDP Act introduces the concept of 'Significant Data Fiduciaries' (SDFs)—large technology companies whose data processing activities pose heightened risks—and subjects them to more complex compliance requirements than ordinary data fiduciaries. SDFs are required to invest in advanced data governance policies and cybersecurity infrastructure and to undergo independent audits, enhancing their accountability.

D. Rights of Data Principals

The Act confers a range of rights on 'data principals'—individuals to whom personal data pertains. These include the right to information about personal data processed; the right to correction and erasure; the right to grievance redressal; and the right to nominate another person to exercise rights in case of incapacity or death. The personal data of users must be erased when the purpose for which it was collected is fulfilled. Children's data receives heightened protection, requiring parental consent for processing minors' data. These provisions represent a genuine advance over India's prior legal framework.

However, the DPDP Act has significant limitations. It heavily relies on consent, but in reality, users cannot genuinely negotiate with technology giants—if one does not agree to an application's policy, one effectively loses access to essential infrastructure. The law characterizes this as 'free consent,' but it is often coerced in practice.[15] Moreover, while Section

[13]DPDP Act, supra note 2, Sched. I (prescribing penalties up to INR 250 crore); cf. Council Regulation 2016/679, art. 83, 2016 O.J. (L 119) 1 (EU) (GDPR penalty ceiling of 4% of global annual turnover or EUR 20 million, whichever is greater).
[14]DPDP Act, supra note 2, §§ 17, 18. The Central Government may exempt any government instrumentality from provisions of the Act by notification. Storage limitation and the right of erasure do not apply to government bodies.
[15]Society on AI Governance and Ethics, Privacy, Power and Sovereignty: India's Big Data Paradox, Medium (Oct. 27, 2025). A significant portion of India's data is stored and processed abroad, raising concerns about weakened state sovereignty.

ISSN: 2582-6433

12 of the Act allows for erasure, there is no explicit right to have data removed from search engines or third-party records. Additionally, one of the most significant ways corporations invade privacy—cross-platform data synchronization through tracking pixels and cookies—remains inadequately addressed, enabling the aggregation of user identities across different applications and platforms even absent explicit consent.

V. Comparative Perspective

A. The European Model: Rights-Based Sovereignty

The European Union's approach to data governance is the most comprehensive effort to assert democratic governance over digital infrastructure. The GDPR confers strong individual rights, backed by independent supervisory authorities empowered to impose meaningful penalties. Through the 'Brussels Effect,' the EU has compelled companies operating globally to raise their privacy standards in order to maintain access to the European market. Enforcement actions against Meta and its subsidiaries, resulting in fines exceeding €405 million, have demonstrated that regulators are capable of imposing significant consequences on even the largest technology companies.

However, the EU model is not without its problems. The compliance burden falls disproportionately on smaller businesses, and the ubiquity of cookie-consent banners has produced 'consent fatigue,' leading users to click through permissions without meaningful deliberation. Enforcement also remains uneven across Member States. Despite these shortcomings, the EU model represents a serious attempt to place citizens, not corporations, at the center of data governance.

B. The Chinese Model: State-Centric Sovereignty

China's approach to digital sovereignty represents the opposite pole of the regulatory spectrum. Through its Personal Information Protection Law, Data Security Law, and the technical architecture of the 'Great Firewall,' China has built a system that simultaneously protects against foreign corporate surveillance while enabling pervasive domestic state surveillance.[16] This has allowed domestic giants such as Alibaba, TikTok, and ByteDance to thrive without significant competition from Western technology corporations.

The Chinese model achieves a form of technological sovereignty through market protection, regulatory support for domestic champions, and authoritarian control of information

[16]Jiang & Belli, supra note 3, at 15–17 (describing China's Personal Information Protection Law, No. 1188 of 2021, and its Data Security Law as establishing a semi-autarkic yet state-directed digital economy).

ISSN: 2582-6433

flows—but at the cost of freedom of speech and personal privacy. As a model for democratic India, it is both geopolitically and constitutionally unavailable: India's Supreme Court has affirmed privacy as a fundamental right, and its civil society and independent judiciary provide institutional constraints on state overreach that have no counterpart in China.

C. India's 'Third Way'

India's approach focuses on digital public infrastructure as a means of balancing privacy with innovation, rather than relying on legal restrictions or state surveillance. India's Digital Public Infrastructure stack—encompassing Aadhaar, UPI, the Open Network for Digital Commerce (ONDC), and the Account Aggregator framework—represents genuine institutional innovation: open-standard, interoperable infrastructure that enables economic inclusion while potentially limiting the lock-in effects of proprietary platforms.[17] This approach allows the country to protect personal data while still encouraging economic growth, ensuring that digital infrastructure serves the public good without sacrificing personal freedom.

VI. Evaluating the DPDP Act as a Sovereignty Instrument

The DPDP Act is a step forward in limiting corporate control over Indian citizens' data. For the first time, Indians have enforceable rights to information, correction, erasure, and grievance redressal, even against companies based outside India. The Act's creation of a Significant Data Fiduciary category subjects high-risk companies to independent audits and enhanced accountability measures.

However, critics worry that the current enforcement system is too weak to deter large technology companies, for whom the maximum penalties may represent an acceptable cost of doing business rather than a genuine deterrent. Additionally, because the government retreated from strict data localization, the flow of data to foreign entities remains largely unchanged.

A. The Sovereignty Paradox

There is a deep irony in the DPDP Act: while the legislation claims to protect India's sovereignty and integrity, it simultaneously expands the government's power over individual data while offering citizens fewer protections against the state itself.[18] This creates a situation

[17]Carnegie Endowment for International Peace, Understanding India's New Data Protection Law (Oct. 2023), available at https://carnegieendowment.org (last visited Apr. 11, 2026).
[18]Prateek Waghre, India's Search for Digital Sovereignty, Tech Policy Press (2025) (noting that asserting

ISSN: 2582-6433

where the sovereignty being defended is the government's power to control information, rather than the people's power over their own lives. Experts warn that merely transferring control from a technology platform to the government does not necessarily mean citizens gain more freedom—it often simply makes it easier for the state to monitor and control its own population.

B. The Path Not Taken

Looking back at the original legislative vision is instructive. The 2018 Srikrishna Committee draft was considerably more robust than the current law: it proposed a truly independent data protection authority, strict data localization requirements for sensitive data, and a symmetrical system in which the government and private companies would be subject to the same rules.[19] These protections were gradually diluted through a process that occurred not through open parliamentary debate but rather through trade negotiations, pressure from technology lobbyists, and political deal-making.

A striking illustration of this 'backing down' occurred in early 2025, when India removed the equalization levy on digital advertisements during trade negotiations.[20] This reveals a fundamental structural constraint: when a country's desire to regulate technology giants' conflicts with its need for favorable trade relations with powerful states, the regulatory impulse typically yields. This is not merely an Indian problem—it reflects the global imbalance of power between nation-states and transnational corporations.

VII. Conclusion

India's DPDP Act, 2023 is a landmark legal step. For the first time, the world's most populous country has a comprehensive statutory framework for the protection of personal data. It translates the right to privacy—already recognized as a fundamental right by the Supreme Court—into practical legal obligations, compelling companies to comply with government-set standards rather than self-regulation.

However, the Act is also the product of significant compromises. To preserve global business and trade relationships, the government relaxed data localization requirements and granted itself broad exemptions from certain privacy obligations. These compromises generally favor large corporations and the state rather than the ordinary citizen.

sovereign state power over corporations does not necessarily translate into greater agency for citizens).

[20]Tech Policy Press, supra note 18 (reporting India withdrew a 6% equalization levy on digital advertising services in early 2025, reportedly in the context of trade negotiations).

ISSN: 2582-6433

Ultimately, legislation alone cannot resolve the structural power imbalance between states and technology giants. To achieve genuine digital sovereignty, India must develop indigenous technological capacity, engage constructively with other nations on global governance frameworks, and ensure that sovereignty is understood as protecting the rights of the people rather than merely augmenting the power of the government. India stands at a crossroads: it possesses the potential to develop a democratic digital model superior to China's authoritarian control or Europe's compliance-heavy approach. Whether the DPDP Act will realize this potential or serve primarily as an instrument of state power remains the defining question for Indian data governance in the years ahead.

REFERENCES

A. Primary Sources

i. Legislation

Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, notified Nov. 13, 2025.

Information Technology Act, No. 21 of 2000, India Code (2000).

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Ministry of Communications & Information Technology.

Personal Data Protection Bill, 2019, Bill No. 373 of 2019, as introduced in Lok Sabha, Dec. 11, 2019; withdrawn Aug. 3, 2022.

Council Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU).

ii. Cases

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

Meta Platforms Inc. & WhatsApp LLC v. Competition Commission of India, SLP (C) No. 6063 of 2024 (Supreme Court of India, 2024).

B. Secondary Sources

i. Books

Couldry, Nick & Ulises A. Mejias, *The Costs of Connection: How Data Is Colonizing Human*

ISSN: 2582-6433

Life and Appropriating It for Capitalism (Stanford University Press, 2019).

Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

ii. Journal Articles and Book Chapters

Jiang, Min & Luca Belli, *'Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa'* in Jiang & Belli (eds), *Policy & Internet* (2024).

Pohle, Julia, *'Attributes of Digital Sovereignty: A Conceptual Framework'* (2025) 14 *Journal of Internet Law & Policy*.

iii. Reports and Official Documents

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

Carnegie Endowment for International Peace, *Understanding India's New Data Protection Law* (October 2023), available at <https://carnegieendowment.org> (last visited Apr. 11, 2026).

DLA Piper, *Data Protection Laws in India*, Data Protection Laws of the World (updated February 2026), available at <https://www.dlapiperdataprotection.com> (last visited Apr. 11, 2026).

iv. Online Sources and Articles

Rau's IAS, *'Digital Sovereignty: India's Strategic Imperative in the Emerging Tech Order'* (2025), available at <https://compass.rauias.com> (last visited Apr. 11, 2026).

Society on AI Governance and Ethics, *'Privacy, Power and Sovereignty: India's Big Data Paradox'*, Medium (October 27, 2025).

Waghre, Prateek, *'India's Search for Digital Sovereignty'*, Tech Policy Press (2025).