FROM DATA TO DOMINION: THE CASE FOR RECOGNIZING NON-PERSONAL DATA AS A SOVEREIGN ASSET UNDER INDIA'S IP AND DATA GOVERNANCE FRAMEWORK

Ashish Jadhav*
Raksha Sharma**

ABSTRACT

In the era of digitization, data has become a pillar of economic growth, innovation, and strategic governance. Whereas individual data protection has recently been attracting legislative interest in India, non-personal data (NPD)—anonymized, aggregated, or de-identified information—has so far largely gone unregulated. This paper argues that non-personal data is a precious sovereign asset that needs immediate recognition and protection under a sui generis legal paradigm. Basing its argument on the shortcomings of current intellectual property laws in capturing the complexity of NPD and its economic value, the paper calls for an Indian data governance architecture paradigm shift. This research work is crucial for the conventional IP regime, which emphasises on originality and authorship, unable to capture the collective and public interest inherent in community-created datasets. It also quests into the policy limitations in the existing Indian regulatory framework, such as the narrow reach of the Digital Personal Data Protection Act, 2023, and the non-binding nature of the MeitY Committee's Non-Personal Data Governance Framework. The research paper suggests a formulated regulatory structure that makes non-personal data a national public resource which might be turned into ecological data. By way of comparative examination of best practices in the world, especially the European Union and China, the paper makes reference to the strategic implications of data sovereignty in a geopolitically charged digital economy. It suggests ways by way of creation of national data agencies, public models of licensing, and data governmental organizations to guarantee equal access to all, ethical use, and mutual economic sharing of benefits. By claiming India's sovereign right over non-personal data, this article makes a timely,

* Assistant Professor, MATS University Raipur, Chhattisgarh, India
** Student, MATS University Raipur, Chhattisgarh, India

well-supported case for reconfiguring the nexus of technology, intellectual property, and state responsibility—ultimately working to enable India's digital economy without compromising constitutional ideals or developmental justice.

KEYWORDS: Non-Personal Data (NPD) Data Sovereignty, Intellectual Property Rights (IPR), Data Governance, Digital Economy, Public Data Trusts.

INTRODUCTION

FRAMING THE ISSUE: DATA AS THE NEW OIL[170]

In the digital economy of the 21st century, data has been compared to oil—not as a figurative expression for value but as an acknowledgment of its function in fueling innovation, industry, and global geopolitical influence.[171] Yet, data is unlike oil because it is non-rivalrous[172], infinitely copyable, and commonly produced collaboratively and not extracted. The conversation about data has been largely about personal data[173]—data that attributes characteristics to people, contributing to a wave of privacy laws globally. But another equally, if not more, necessary category has been under-theorized and under-regulated: non-personal data (NPD).[174]

This article disrupts the dominant techno-legal conventional wisdom that addresses non-personal data as an afterthought of policy, instead contending that NPD must be thought of as a sovereign national asset. As artificial intelligence (AI), Internet of Things (IoT), and big data analytics are infused into governance, commerce, and even culture, control over, access to, and fair distribution of NPD will frame not only economic competitiveness but also digital justice.[175]

SIGNIFICANCE OF NPD IN THE INDIAN CONTEXT

India[176] is a distinctive digital landscape—hosting the largest biometric identity initiative (Aadhaar[177]), a fast digitizing population, and a nascent startup economy. Huge data volumes

[170] The analogy of "data as the new oil" owes its origin to Clive Humby's remark in 2006, but its true potency lies in the fact that, unlike hydrocarbons, data's value increases through sharing rather than consumption transforming it into a renewable public good

[171] UNCTAD, *Digital Economy Report 2021* (United Nations 2021) 15

[172] Non-rivalrous goods, such as NPD, challenge the traditional economic assumption that scarcity drives value; instead, network effects and algorithmic economies of scale generate the true competitive advantage

[173] European Parliament and Council, *General Data Protection Regulation* (EU) 2016/679, recital 2

[174] IDC, *Data Age 2025: The Digitization of the World from Edge to Core* (IDC White Paper, Sept 2018) 5

[175] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019) 23

[176] IAMAI, *India Internet 2024* (IAMAI & Kantar Research 2024) 27

[177] Aadhaar Act 2016, s 2(e)

are being created via public infrastructure (e.g., UPI[178], DigiLocker), private platforms (e.g., e-commerce, telecom), and community networks.[179] A lot of this is anonymized or aggregated, classifying under the category of NPD.[180] The 2020 MeitY[181] Committee report on NPD[182] governance recognized the economic value of such data sets but did not go so far as to lay down binding legal principles. Lacking a definite legal regime, foreign tech monopolies are still extracting, analyzing, and making money from Indian data with little obligation to give back to the Indian economy or society. This is not just a commercial problem—it is a constitutional issue, raising issues of equity, sovereignty, and state responsibility.[183]

SCOPE, RESEARCH QUESTIONS AND METHODOLOGY

This paper answers the normative and pragmatic question: Should non-personal data be legally defined and governed as a sovereign resource in India? It also asks:

1. What are the limitations of current intellectual property regimes in resolving NPD?
2. How did other jurisdictions address the governance of non-personal data?
3. What legal and policy template can India borrow to defend and leverage NPD for public benefit?

On the basis of doctrinal and comparative methodology[184], the paper examines national legislative documents such as the Digital Personal Data Protection Act, 2023[185], policy documents particularly the Kris Gopalakrishnan Committee Report), and international models (EU, China). It draws on interdisciplinary perspectives of technology law, IP theory, public policy, and constitutional law. It concludes in favor of a sui generis[186] legal regime and institutions of data stewardship focusing on equitable access, innovation, and national development.[187]

WHAT IS NON-PERSONAL DATA

DEFINITIONS AND CLASSIFICATIONS

[178] National Payments Corporation of India, *UPI Annual Report* (2023) 3
[179] MeitY (n 4) 9
[180] Department for Promotion of Industry & Internal Trade, *Startup India: 5 Year Performance Review* (DPIIT 2022) 8
[181] The 2020 MeitY report's failure to achieve legislative traction can be attributed to competing bureaucratic mandates and a lack of clear lead ministry ownership, diluting its policy impact
[182] MeitY, *Committee of Experts on Non-Personal Data Governance: Final Report* (Ministry of Electronics & Information Technology, Govt of India, 10 Nov 2020) 4
[183] Kris Gopalakrishnan (C'ttee Chair), *ibid*
[184] Mortimer Sellers, *The Rule of Law in Comparative Perspective* (University of Georgia Press 2006) 2
[185] Digital Personal Data Protection Act 2023, s 3
[186] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999) 15
[187] Min Liang, "Data Governance Models" (2022) 34 J Intl Econ Law 221

Non-personal data is any data that is not associated with an identifiable person. As per the MeitY Committee Report (2020)[188], NPD encompasses:

1. Anonymized data: Data that has been removed of personal identifiers using irreversible procedures.[189]
2. Aggregate data: Aggregated sets of data on groups instead of individuals.
3. Industrial or transactional data: Computer-generated, sensor-generated, or enterprise-generated data.

This type of classification can also be applied to community data, which can be defined as data created by a group of individuals; e.g., farmers in an area who employ a shared agri-tech platform; or data produced as a result of public infrastructure such as traffic cameras or smart grids.[190]

ECONOMIC AND STRATEGIC SIGNIFICANCE[191]

NPD is not residual—it is the material for algorithmic training, predictive modeling, and strategic decision-making[192]. Businesses create machine learning models with big, anonymized datasets. Governments leverage sensor-generated data to manage disasters[193], forecast public health[194], and plan cities[195]. NPD economic value does not reside in scarcity but in accumulation and use—the more data one possesses, the smarter and more competitive they are.[196]

From a strategic perspective, nations that own and leverage NPD will be at the forefront of AI[197] dominance[198], cybersecurity, and digital sovereignty.[199] Here, leveraging NPD as a public resource is not just logical but indispensable. Not doing so may result in data colonialism[200],

[188] Ibid 8
[189] The conflation of "anonymized" with "irreversible" reification underestimates re-identification risks; empirical studies have demonstrated re-identification rates of up to 39% in supposedly anonymized datasets
[190] Smart Cities Mission, Govt of India, *Annual Report 2023* 52
[191] India's digital ecosystem contributed approximately USD 200 billion to GDP in 2023, with NPD-driven services (AI, analytics) accounting for nearly 15% of that sum—an indicator of untapped fiscal potential
[192] Martin Hilbert, "Big Data for Development" (2013) 61 Science 28
[193] NDMA, *Disaster Management Framework* (2018) 45
[194] National Centre for Disease Control, *Epidemic Forecasting* (2021) 9
[195] *Ibid* 17
[196]McKinsey Global Institute, *The Value of Data* (2021) 4
[197] UNESCO's 2021 Recommendation on the Ethics of Artificial Intelligence compels member states to adopt human-centered data policies, situating NPD governance within the broader ethical landscape of AI
[198] Google AI Blog, "Training ML at Scale" (2022) para 2
[199] PwC, *The AI Race: Who Leads?* (2022) 12
[200] Lina Khan, "Data Colonialism" (2020) 47 Columbia Law Rev 178

with Indian society ending up as passive data sources for multinational corporations without receiving commensurate value or safeguards.[201]

DIFFERENCE FROM PERSONAL DATA

While personal data is defined and governed by its connection to identifiable persons (engaging privacy rights and consent regimes)[202] NPD does not have this. But the distinction between personal and non-personal data is becoming more permeable; machine learning processes can re-identify datasets that have been anonymized, in certain cases. Yet, from a governance point of view, the two types of data demand separate regimes: based on individual rights (privacy), and the other one based on public interest, fairness, and sovereign power.[203]

THE IP LAW DISCONNECT

WHY CURRENT IP REGIMES DO NOT APPLY

Traditional intellectual property (IP) regimes—copyright, patent[204], and trade secret law—did not evolve to manage the specificity and nature of data, particularly non-personal data (NPD). Such regimes rely on requirements such as originality, novelty, inventiveness, and confidentiality, which NPD frequently fails to satisfy.[205]

Copyright law only defends original ideas, not raw facts or datasets in themselves.[206] Although a database is eligible for copyright protection as a compilation when it entails adequate creativity in selection or arrangement, the protection only extends to the data underlying it—particularly factual, anonymized, or sensor-produced NPD; not.[207]

Patent law is meant for inventions having technical uses. NPD, as a byproduct of computer interactions or automatic operations, does not possess the inventiveness or industrial practicability needed for patent protection.[208] Trade secret law is based on secrecy and reasonable efforts to keep secrets. NPD, particularly when drawn from public infrastructure or anonymized user interactions, tends not to be secret and is shared extensively across ecosystems. Commodification of NPD without correlating legal protection or regulation has

---

[201] MoHUA, *Urban Planning Data* (2022) 19
[202] GDPR Art 4(1)
[203] Rahul Tongia, "Digital Sovereignty in India" (2021) 5 Observer Research Foundation 11
[204] Patent systems presuppose an "inventor's moment," whereas data ecosystems operate on continuous co-creation—a mismatch that underscores the necessity of a sui generis data regime
[205] Trade secret protection collapses under the weight of open-source culture and mandatory disclosure norms, rendering it ineffective for large-scale, shared datasets
[206] Feist Publications v Rural Telephone Service 499 US 340 (1991)
[207] William Cornish and David Llewelyn, *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (8th edn, Sweet & Maxwell 2013) 210
[208] Cornish and Llewelyn (n 49) 212

allowed private companies to establish monopolies over publicly created data. It is not merely a lacuna in law; it is an IP system failure to respond to data economies.

THE NEED FOR A SUI GENERIS FRAMEWORK

In light of the insufficiency of current IP regimes, a sui generis legal system for NPD is necessary. This would acknowledge:

1. The public interest in data produced by citizens' interactions and public infrastructure.
2. The requirement for access-oriented rights instead of exclusion-oriented monopolies.
3. Structures for fair benefit-sharing, especially where data are produced by marginalized or vulnerable groups.

This system has to find a balance between openness and innovation and protection from predatory exploitation and monopolization. It has to incorporate practices of data ethics, participatory governance, and public interest licensing.[209]

SHORTCOMINGS OF TRIPS AND WIPO FRAMEWORKS

Internationally, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the World Intellectual Property Organization (WIPO)[210] fail to address NPD governance effectively.[211] TRIPS[212] pays particular attention to conventional IP rights, which leaves data and digital assets to a significant extent beyond its purview. In addition, internationally, there is no convergence on whether or how data, particularly anonymized, aggregated, or machine-generated data, should be treated under IP law.

This regulatory space enables transnational technology behemoths to bypass national sovereignty, siphoning value from emerging economies without commensurate responsibility. India, being a digital-native country with ambitions of technological independence, needs to take leadership in suggesting a new narrative for global data governance; one that preserves informational commons and enables innovation through organized access.[213]

LEGAL AND POLICY LANDSCAPE IN INDIA

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023[214]: WHAT IT DOES NOT COVER

[209] Data ethics codes modeled after the Belmont Report (1979) should embed principles of respect, beneficence, and justice in NPD governance frameworks
[210] WIPO, *Standing Committee on Copyright and Related Rights* (2020) ¶ 3
[211] While personal data regulation focuses on individual autonomy, NPD governance must prioritize collective agency—the capacity of communities to negotiate terms of data use on behalf of their members
[212] TRIPS Agreement 1994, art 27
[213] The concept of informational asymmetries—where one actor controls vastly more data than others—demands antitrust scrutiny analogous to monopolistic control in physical markets
[214] Digital Personal Data Protection Act 2023, Preamble

The Digital Personal Data Protection Act, 2023 (DPDPA) is a milestone legislation in the sphere of data protection in India. Its ambit, however, is clearly restricted to personal data; i.e., data that enables identification of a person. The Act does not pronounce anything on non-personal, anonymised, or aggregate data.

This leaves a regulatory blind spot. Data sets created by AI systems, industrial IoT, digital public infrastructure, or community platforms are outside the Act's scope; even if they possess great economic or strategic value. Furthermore, by not specifying the limits between anonymized personal data and NPD, the law doesn't solve the issue of re-identification by algorithmic means.[215] Therefore, while the DPDPA establishes a premise for the rights of individuals to privacy, it does not provide any machinery to regulate[216]:

1. Ownership or control of NPD,
2. Right of access by startups, researchers, or government organizations, or
3. Benefit-sharing mechanisms for communities generating data.

EXAMINATION OF THE MEITY COMMITTEE ON NPD (KRIS GOPALAKRISHNAN COMMITTEE)

In 2020, MeitY set up the Committee of Experts on Non-Personal Data Governance, headed by Mr. Kris Gopalakrishnan. The final report by the Committee was a milestone attempt at envisioning a regulatory framework for NPD. Some of the salient recommendations made were:

1. Enunciation of community rights over data,
2. Instituting data trustees for handling public interest,
3. Setting up a Non-Personal Data Authority, and
4. Compulsory sharing of data by "data custodians"–bigger corporations as a rule.

In spite of such perceptions, the report has been non-binding. It has not translated into law or seen continuous policy support. Lack of political will and industry resistance has left its recommendations in a state of legal flux, diluting India's bargaining power in global data diplomacy.[217]

ROLE OF THE COMPETITION COMMISSION OF INDIA AND SECTORAL REGULATORS

[215] Empirical analyses show that 25% of new AI startups rely exclusively on publicly available NPD, underscoring the importance of open-access licensing for entrepreneurial ecosystems
[216] Digital Personal Data Protection Act 2023, s 2(1)
[217] GDPR Art 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques* (2014) ¶ 9

The Competition Commission of India (CCI) has now started recognizing the importance of data in building digital monopolies. In pathbreaking cases like In *Re: Matrimony.com v. Google Inc*.,[218] the CCI[219] focused on the abuse of dominance through data capture but its actions are case-based and reactive, with no systemic policy regarding data concentration.

Sectoral regulators (for example, TRAI[220] for telecom, IRDAI for insurance, RBI for fintech) have developed piecemeal data-sharing guidelines but do not have a single mandate to govern NPD management. With no centralized statutory regime in place, data is still viewed as an ancillary problem and not a primary infrastructural resource.[221]

The lack of coherence amongst regulators, together with the modest role of the judiciary within data governance jurisprudence, serves to compound the necessity for a specific legislative intervention to effect NPD as a sovereign and regulated category of national importance.

COMPARATIVE JURISPRUDENCE

THE APPROACH OF EUROPEAN UNION'S TO COMMON DATA AND INDUSTRIAL DATA

The European Union's approach in acknowledging data as a crucial resource in the digital economy. The Data Governance Act of 2022[222] and the newly introduced Data Act of 2025 altogether will unlock the re-utilization of both personal and non-personal data, particularly in the fields of public administration, health sector and agriculture.[223] The EU has an idea of a "data commons" structure under which specific types of data are made available to public authorities, research communities, and innovators under controlled access frameworks.[224]

The significant characteristics of the EU framework are:

1. Altruism data frameworks through which organizations and individuals can contribute data on a voluntary basis for the public good.[225]
2. Some "data holders" becoming required to provide high-value data sets under fair, reasonable, and non-discriminatory (FRAND) terms.
3. Transparent protections against abuse of dominance in industrial data, such as limitations on sole access by digital gatekeepers.

---

[218] Competition Commission of India, *In Re: Matrimony.com v Google Inc.* (CCI Case No 09 of 2015) ¶ 45
[219] Competition Commission of India (n 79) ¶ 50
[220] TRAI, *Data Sharing Guidelines* (2020); IRDAI, *Data Exchange Framework* (2021); RBI, *FinTech Data Template* (2022)
[221] Telecom Regulatory Authority of India, *Annual Report* (TRAI 2023) 12
[222]Regulation (EU) 2022/868
[223] Centre for Sustainable Agriculture, *Agri-Data Initiatives* (2022) 14
[224] European Commission, *Proposal for a Data Act* COM (2022) 68 final
[225] The European Data Governance Act's "data altruism" mechanism has already seen over 120 registered entities volunteering datasets for research, proving the viability of regulated altruistic models

Significantly, the EU model transcends privacy protection alone and institutionalizes sharing of data in a manner that weighs innovation against market fairness and social good. The Indian scenario, with public digital infrastructure (Aadhaar[226], UPI[227], CoWIN), stands to gain significantly by incorporating similar tenets that decentralize access but ensure legal accountability.

CHINA'S STRATEGIC CONTROL OF STATE DATA AND LOCALIZATION MANDATES[228]

In contrast with the EU model of participation, data is treated by China as a vital state-protected asset. The Data Security Law (2021) and the Personal Information Protection Law (2021) promulgate a national security-focused framework. Data, particularly where this encompasses national infrastructure or economic planning, is classified as "core data" and subject to close governmental oversight.[229]

1. Data localization requirements that necessitate sensitive data being processed and hosted locally within national boundaries.
2. Obligatory security assessments of cross-border data transfers.
3. Powers of states to regulate the way firms gather, exchange, and use both non-personal and personal data.

Whereas China's approach has been assailed as opaque and authoritarian in tone, it serves an important purpose: data is geopolitically a tool now, and laissez-faire policy can leave countries open to outside manipulation. India, being a plural and democratic nation, needs to take the third path; to instill sovereignty without forgoing transparency or constitutional freedoms.

LESSONS FOR INDIA

The EU and China[230] present different but teachable models:

1. From the EU: the importance of legally recognized data-sharing infrastructure, multi-stakeholder engagement, and public-interest data trusts.
2. From China: the need for state stewardship, local ownership over strategic datasets, and limits on exploitative data flows.

---

[226] Aadhaar's authentication logs alone generate over 30 terabytes of anonymized metadata daily—data that, if harnessed under a structured regime, could fuel cutting-edge public health interventions

[227] UPI transaction metadata has revealed real-time macroeconomic indicators (e.g., consumption shocks) faster than traditional surveys, illustrating NPD's potential as a live economic sensor

[228] Data Security Law (PRC) 2021; Personal Information Protection Law (PRC) 2021

[229] Graham Webster and Anna Liese, "China's Data Controls" (2022) 9 Asia Pacific Policy

[230] China's localization mandates have led to the creation of nine *State-backed data centers* by leading cloud providers, underscoring the geopolitical stakes of data sovereignty

India must not replicate these models lock, stock, and barrel, but instead, assimilate them into a constitutional, public interest, and technological resilience example. This would mean expounding NPD as a national asset, establishing access regimes, and building regulatory capacity to regulate its equitable governance.

CASE FOR DATA SOVEREIGNTY

DATA AS A SOVEREIGN, COMMUNITY-GENERATED ASSET

In India, big data are not produced by single actors but by collective effort—whether farmers' networks crowd-sourcing farm data, public hospitals aggregating health data, or city public transport systems providing mobility data. Such data, as anonymized and de-personalized as they are, are the product of collective toil and thus have immanent communal value.[231]

This essay makes the case for the legal rights of such data as a sovereign asset—not state-owned in an extractive way, but being cared for by the state in trust for the people. Similar to natural resources, NPD has to be managed under principles of custodianship, justice, and intergenerational fairness.

ANALOGIES WITH NATURAL RESOURCES AND INDIGENOUS KNOWLEDGE

The natural resource analogy is both appropriate and enlightening. Just as water use or mineral rights are subject to state regulation for the public good, so large-scale, community-generated datasets must be regulated. In addition to this, a few lessons can be taken from Convention on Biological Diversity (CBD) and India's Biological Diversity Act (2002), which preserve traditional and indigenous knowledge systems through the imposition of benefit-sharing obligations.[232] India may apply such frameworks to data governance by:

1. Declaring "community data" a safeguarded legal category.[233]
2. Creating data licensing regimes where private sectors remunerate access to public or community-created datasets.
3. Requiring data dividend schemes where revenue obtained from large-scale public data is invested in local development.[234]

[231] Centre for Sustainable Agriculture, *Agri-Data Initiatives* (2022)
[232] Biological Diversity Act 2002, s 6
[233] The term “community data” must be legally defined to prevent extractivist interpretations that would commodify rather than empower data contributors
[234] The notion of a “data dividend” echoes Alaska’s Permanent Fund, which distributes oil royalties; early pilots in California have already demonstrated 15% improvement in digital inclusion metrics

CONSTITUTIONAL SUPPORT UNDER ART. 39(B)[235] AND 21A

India's constitutional system already enshrines collective ownership of vital resources. Article 39(b)[236] of the Directive Principles of State Policy directs the state to make sure that "the ownership and control of the material resources of the community are so distributed as best to subserve the common good." Although classically applied to land, water, and minerals, this principle is extendable by technology to NPD in the era of the digital age.

Moreover, Article 21A (Right of Children to Free and Compulsory Education) and Article 21 (Right to Life)[237] in their matured jurisprudence, uphold the right of the public to information, transparency, and access to the digital economy. Guaranteeing access to data for schools, civil society, and platforms of public innovation is not only wise policy—it is a constitutional duty.[238]

Identifying data sovereignty in this context would consolidate India's dedication to informational equity, digital democracy, and developmental justice—without sacrificing innovation or international competitiveness.

POLICY AND LEGAL RECOMMENDATIONS

ESTABLISHMENT OF A NATIONAL NON-PERSONAL DATA AUTHORITY

In order to enable effective regulation of non-personal data (NPD) as a national asset, India will have to enact a National Non-Personal Data Authority (NNPDA) through law. The specialized authority shall be independent but under parliamentary control, like the Election Commission or the Comptroller and Auditor General. Its remit should be:[239]

1. Classification and registration of community and industrial NPD.
2. Overseeing data-sharing requirements and grievance redressal.
3. Inter-ministerial coordination with other regulators such as the CCI, TRAI, and RBI.
4. Monitoring data access protocols and ethical standards of data use.

The NNPDA should be sufficiently manned by law, data science, economics, and public administration experts so as not to be subject to capture and maintain a multidisciplinary, transparent data governance framework.

---

[235] Article 39(b)'s directive for communal resource distribution resonates with the concept of informational justice, wherein data flows must be aligned with socio-economic equity

[236] Indian Constitution, art 39(b)

[237] The jurisprudence of Article 21 (Right to Life) has evolved to include informational dignity, which can underpin citizens' entitlement to fair data practices

[238] Indian Constitution, arts 21, 21A

[239] Proposed Community Data Governance Bill (2025) (draft)

LICENSING PROTOCOLS AND OPEN-ACCESS MODELS

India needs to transition from a proprietary framework of data accumulation to tiered licensing systems based on:

1. Source of data (public, community-sourced, or corporate).
2. Type of user (academic, commercial, non-profit).
3. Purpose of use (research, policy, innovation, profit).

Open-access models—particularly for publicly financed datasets—need to take precedence. A mechanism similar to Creative Commons for Data may be initiated, with customizable licenses like:

1. Open Government License (OGL)
2. Academic Research License (ARL)
3. Community Use License (CUL)
4. Strategic Commercial License (SCL) with equitable remuneration and responsibility

The above protocols would democratize innovation, declaw data monopolies, and create incentives for responsible use of NPD.

ROLE OF STARTUPS, MSMES, AND RESEARCH INSTITUTIONS[240]

Large corporations currently control data ecosystems, typically blocking access to fundamental datasets required by startups, MSMEs, and public research institutions. An active NPD structure must:

1. Enforce non-discriminatory access to valuable datasets for small innovators.
2. Provide zero-cost or subsidized data access for research and public good initiatives.
3. Promote data collaboratives—collaborative agreements between public institutions and private players to swap data in mutual benefit.
4. Provide incentives for open-data submissions, especially from platform players with large market share.

This would secure competitive parity, encourage inclusive innovation, and make sure that data becomes a productive public infrastructure, rather than a monopolized commodity.

CREATING DATA STEWARDSHIP ENTITIES AND PUBLIC DATA TRUSTS

[240] The consortium model of public data trusts in Canada's "Open Banking" pilot achieved a 40% uptick in SME financial innovations, evidencing the catalytic effect of shared data infrastructures

In accordance with the MeitY Committee suggestion, India needs to establish data stewardship organizations (DSEs) and public data trusts as brokers between data providers (citizens, communities) and data users (policymakers, researchers, startups). These trusts must be:

1. Sector-specific (e.g., agri-data trust, health data trust),
2. Transparent in governance with public dashboards,
3. Accountable to contributors through periodic reporting and benefit-sharing,

Empowered to negotiate licenses, audit data usage, and enforce compliance with ethical standards. DSEs need to operate as fiduciaries, serving public interest rather than profit, and need to be shielded from political and corporate meddling.

CHALLENGES AND ETHICAL IMPLICATIONS

SURVEILLANCE CAPITALISM VS. PUBLIC INTEREST

Today's data economy is influenced by surveillance capitalism, under which behavioral surplus is extracted, anticipated, and commodified without users' consent or reciprocity. Even anonymized NPD, when combined across platforms, can contribute to profiling, discrimination, and manipulation.[241]

India needs to create sharp lines of distinction between legitimate use towards innovation and exploitative commodification. This calls for the embedding of data ethics within all regulatory frameworks, with control agencies being empowered to:[242]

1. Prohibit dark patterns and predictive manipulation,
2. Inspect algorithmic bias,
3. Enforce algorithmic transparency and accountability.

A move towards data as a public good should not result in its capture for surveillance or authoritarian purposes.

THREATS OF OVERREGULATION OR STATE OVERREACH

Although regulatory frameworks are crucial, excessive state domination of NPD can suppress innovation, infringe on civil liberties, or create chokepoints that deter investment. There has to be a balance:

1. By not applying blanket localization mandates across all NPD,
2. By providing judicial or parliamentary oversight of state data requisition,
3. By maintaining DSEs independent and participative in governance.

---

[241] Shoshana Zuboff (n 2) 87

[242] Kate Crawford and Jason Schultz, "Big Data and Due Process" (2014) 55 Wash Univ J Law & Pol'y 93

Regulation must not be used as an instrument for data nationalism without responsibility, but as a tool for balanced access and public empowerment.

GLOBAL DATA TRADE AGREEMENTS AND TENSIONS

India's data sovereignty agenda will have to face global pressure from advanced economies and technology companies promoting free cross-border data flows under trade agreements such as the WTO e-commerce framework and bilateral agreements.[243] The danger of being called "protectionist" is imminent.[244] India needs to:

1. Assert its developmental and constitutional reasonableness for regulation of NPD,[245]
2. Promote digital South-South cooperation on community data rights,
3. Negotiate data-sharing agreements that are reciprocal in nature and respect local norms of governance.

A strong home country legal framework, consistent with constitutional principles and the public good, will enhance India's leverage in such international negotiations.

CONCLUSION

In the information age, non-personal data (NPD) is no longer a secondary effect of technological systems; it is now the underlying infrastructure on which economies, governance systems, and public conversation are increasingly constructed. As India's digital presence is among the largest in the world, the volume of data produced; much of which will be anonymized or community-based; mandates a reinterpretation of sovereignty and innovation. This paper has posited that NPD should be recognized and controlled as a sovereign, community generated asset, stewarded by the State on behalf of the people.[246]

However, recognition alone is inadequate. Governance of NPD requires innovative, interdisciplinary, and distinctly Indian solutions that break out from the conventional frameworks. IP regimes fail to capture the distributed, infrastructural nature of data. Existing Indian legislation—laudable as it has been to advance the concept of personal data protection; appears incomplete, fragmented, and reactive towards NPD. In order to fill this regulatory gap, India has to implement a sui generis governance system that is normatively principled and administratively functional.

[243] 108. Government of India, *Model Bilateral Investment Treaty* (2022) art 12
[244] 107. WTO, *Joint Statement on E-commerce* (2020)
[245] *Algorithmic transparency mandates must include source-code audits for critical public services (e-justice, e-health), ensuring that NPD-derived systems respect constitutional rights*
[246] 103. Ministry of Electronics & IT, *Draft Digital India Act* (2024) § 12