Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Code, Consent, and Constitutionalism: Governing India's Digital Public Infrastructure

Arka Bhattacharya[a]

[a]Advocate

Received 21 August 2026; *Accepted* 21 September 2026; *Published* 25 September 2026

This paper critically examines India's emerging Digital Public Infrastructure (DPI), exemplified by Aadhaar for digital identity, the Unified Payments Interface (UPI) for real-time payments, and the Open Network for Digital Commerce (ONDC) for open e-commerce, which has fundamentally transformed access to public and private services for over a billion people. These technological innovations are analysed through a rigorous constitutional lens, focusing specifically on the jurisprudential intersections of informational privacy, informed consent, and algorithmic governance. The study begins by situating India's DPI within its broader socio-legal context, addressing both its unprecedented global scale and the attendant security and privacy challenges. Through doctrinal case studies, this paper evaluates Aadhaar's constitutional litigation before the Supreme Court alongside its documented data vulnerabilities, UPI's complex trade-offs between financial inclusion and transactional privacy, and ONDC's promise of democratized commerce juxtaposed against its current governance ambiguities. These narratives illustrate the precise flashpoints where fundamental rights have been either upheld or infringed. Furthermore, the paper analyses the constitutional frameworks governing these digital infrastructures, exploring how Article 21's guarantee of life and personal liberty encompasses the rights to privacy and dignity, and how Article 14's mandate of equality and non-arbitrariness guards against discriminatory digital architectures. Finally, the analysis incorporates comparative perspectives contrasting regulatory frameworks in the European Union, the United States, Brazil, Australia, and Estonia and critiques India's Digital Personal Data Protection Act, 2023 (DPDP Act) for its deficit of regulatory independence and algorithmic safeguards. Ultimately, the paper proposes comprehensive legal, technical, and institutional reforms to ensure that digital 'code' remains firmly subordinated to constitutionalism.

Keywords: *digital public infrastructure, constitutionalism, privacy, algorithmic governance, data protection.*

INTRODUCTION

India has engineered a Digital Public Infrastructure (DPI) of unparalleled global scale. Analogous to foundational physical utilities such as railways or power grids, this DPI comprises interoperable layers of identity, payments, and data exchange specifically architected to facilitate institutional trust nationwide. At the core of this ecosystem lie three foundational pillars: digital identity (Aadhaar), digital payments (UPI), and an open e-commerce network (ONDC). Rather than operating as proprietary, profit-driven ventures, these platforms were deliberately constructed as shared national assets and public goods. Through this architectural design, the state has streamlined direct benefit transfers, integrated millions of unbanked individuals into the formal economy, and catalysed substantial domestic innovation.

Empirical deployment metrics underscore the scale of this transformation. Since its inception in 2009, Aadhaar, India's 12-digit biometric identification system, has enrolled approximately 1.3 billion residents. Concurrently, UPI processes more than 10 billion transactions per month as of 2025. Operating in tandem, these systems have reduced customer onboarding and identification costs from an estimated $10–20 to approximately 27 cents per verification, significantly mitigating exclusion across the welfare and banking sectors. Meanwhile, ONDC, launched in 2021 by the Department for Promotion of Industry and Internal Trade (DPIIT), seeks to democratise the digital marketplace by enabling neighbourhood *kirana* stores, small-scale farmers, and niche vendors to transact via open protocols rather than relying on monopolistic, closed-loop platforms.

RESEARCH PROBLEM

Despite these socio-economic advancements, the rapid expansion of DPI raises urgent constitutional questions. These infrastructural layers aggregate and process vast quantities of sensitive personal data at population scale, rely on complex and often opaque algorithms, and are frequently mandated or heavily steered by the state apparatus. As analysts at the World Economic Forum observe, when digital architectures serve 1.3 billion people, the 'security stakes are high,' as data breaches and linkage attacks can cascade rapidly across

interconnected services.[1] Moreover, algorithmic bias and opaque automated decision-making within these networks risk perpetuating historical socio-economic inequalities. Reported security incidents such as a data leak compromising the records of over 20 million officials underscore these systemic architectural vulnerabilities. Consequently, the central problem addressed in this paper is how to subject this expansive, code-based governance architecture to rigorous and effective constitutional scrutiny.

RESEARCH OBJECTIVES

1. To expand the overarching paradigm of constitutionalism across India's Digital Public Infrastructure.
2. To interrogate how the foundational principles of informed consent, procedural due process, and fundamental rights intersect with the code-based governance of identity, payment, and commerce networks.
3. To critically examine Aadhaar, UPI, and ONDC through targeted doctrinal case studies of both technological innovations and fundamental rights infringements.
4. To advance the doctrinal analysis of Articles 21 (life and privacy), 14 (equality), and 19 (expression and information) through a contemporary digital-governance lens.
5. To systematically evaluate India's Digital Personal Data Protection (DPDP) Act, 2023, identifying its structural enforcement gaps and deficit of algorithmic accountability.
6. To formulate concrete legal, technical, and institutional reforms designed to align India's DPI with core constitutional mandates.

RESEARCH QUESTIONS

1. How do the constitutional principles of informed consent and procedural due process intersect with the code-based governance of India's identity, payment, and commerce networks?
2. In what specific jurisprudential respects does India's approach to digital governance and data protection compare with established regulatory frameworks in the European Union, the United States, Brazil, Australia, and Estonia?

[1] 'Security-by-design lessons from India's digital public infrastructure journey' (*World Economic Forum (WEF)*, 02 October 2025) <https://www.weforum.org/stories/2025/10/security-by-design-india-digital-public-infrastructure/> accessed 12 August 2026

3. What structural enforcement gaps, executive exemptions, and algorithmic accountability deficits are embedded within India's Digital Personal Data Protection Act, 2023?

RESEARCH HYPOTHESES

- The prevailing regulatory framework governing India's DPI, most notably the DPDP Act 2023, is structurally and procedurally insufficient to safeguard the fundamental constitutional rights of citizens.

- The highly centralised nature of India's data protection enforcement architecture, compounded by sweeping executive exemptions, poses a severe threat to algorithmic accountability and procedural due process.

- Proactively embedding procedural due process, algorithmic transparency, and egalitarian design into the core architecture of DPI enables the state to harness digital efficiency without compromising constitutionally guaranteed liberties.

RESEARCH METHODOLOGY

This study employs a doctrinal and comparative legal methodology. It critically analyses primary legal texts, specifically the Constitution of India and the DPDP Act, 2023, alongside landmark judicial pronouncements to map the prevailing constitutional paradigm. Additionally, the paper utilises in-depth case studies of Aadhaar, UPI, and ONDC to evaluate the practical divergence between technological implementation and constitutional mandates. Finally, a comparative legal analysis evaluates India's statutory framework against international regulatory benchmarks to ground the paper's normative recommendations.

LITERATURE REVIEW

Existing scholarship reveals a persistent tension embedded within the architecture of Digital Public Infrastructures. Global cybersecurity analyses caution that the population scale of India's DPI introduces systemic vulnerabilities; when platforms encompass over a billion users, security failures carry severe consequences and data breaches can cascade across integrated digital networks. Within the domain of digital finance, contemporary scholarship

highlights that UPI presents a pronounced dichotomy between broadened financial inclusion and acute data-privacy trade-offs.[2] Similarly, legal literature examining automated decision-making emphasises that while constitutional equality mandates that 'similarly situated people' be treated alike, artificial intelligence systems frequently subvert this principle by reflecting and amplifying historical societal prejudices.[3]

Comparative legal scholarship further illustrates divergent international approaches to digital governance.[4] Whereas the European Union's General Data Protection Regulation (GDPR) and Artificial Intelligence Act institute robust regulatory oversight and restrict solely automated decision-making, the United States relies on a fragmented patchwork of sectoral privacy statutes. Elsewhere, Brazil enshrines explicit statutory rights to review automated decisions,[5] while Estonia operationalises decentralised, privacy-by-design interoperability.[6] Conversely, policy studies examining Australia's centralised 'My Health Record' system underscore the acute risks of aggregating sensitive public data without stringent institutional accountability.[7] Finally, contemporary legal critiques of India's DPDP Act, 2023 emphasise that its envisioned Data Protection Board is overly centralised and lacks institutional independence,[8] while the statute itself merely mandates baseline data accuracy without establishing a meaningful right to explanation or review for automated decisions.[9] This paper

[2] Dr Sadhana Prajapati and Prof Sunil Kumar, 'Indian Digitally Payment Systems: UPI, ULI, CBDC - Challenges, Opportunities and Prospects' (2025) 2(4) Advances in Consumer Research <https://acr-journal.com/article/indian-digitally-payment-systems-upi-uli-cbdc-challenges-opportunities-and-prospects-1593/> accessed 12 August 2026

[3] Amal Singh Patel, 'Algorithmic Bias And The Quest For Equal Justice in India' (*Virtuosity Legal,* 09 September 2025) <https://virtuositylegal.com/algorithmic-bias-and-the-quest-for-equal-justice-in-india/> accessed 12 August 2026

[4] Vasanthika Srinath, 'AI & Algorithmic Sovereignty in India' (*Dhirubhai Ambani University*) <https://sol.daiict.ac.in/thought-leadership/ai-algorithmic-sovereignty-in-india/> accessed 12 August 2026

[5] Camila Mariotto, 'Brazilian legal framework on automated decision-making' (*International Bar Association,* 09 June 2024) <https://www.ibanet.org/Brazilian-legal-framework-on-automated-decision-making> accessed 12 August 2026

[6] 'X-Road' (*e-Estonia Briefing Centre*) <https://e-estonia.com/solutions/interoperability-services/x-road/> accessed 08 October 2026

[7] Helen Davidson, 'My Health Record failed to manage cybersecurity and privacy risks, audit finds' *The Guardian* (25 November 2019) <https://www.theguardian.com/australia-news/2019/nov/25/my-health-record-failed-to-manage-cybersecurity-and-privacy-risks-audit-finds> accessed 12 August 2026

[8] 'Enforcement Gaps in India's DPDP Act and the Case for decentralized data protection boards' (*Express Computer,* 04 July 2025) <https://www.expresscomputer.in/guest-blogs/enforcement-gaps-in-indias-dpdp-act-and-the-case-for-decentralized-data-protection-boards/126140/> accessed 12 August 2026

[9] Raktima Roy and Gabriela Zanfir-Fortuna, 'THE DIGITAL PERSONAL DATA PROTECTION ACT OF INDIA, EXPLAINED' (*Future of Privacy Forum,* 15 August 2023) <https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/> accessed 12 August 2026

situates its constitutional analysis precisely within these documented legislative and scholarly gaps.

AADHAAR: IDENTITY, INCLUSION, AND PRIVACY

The Aadhaar Project and Judicial Response: Introduced in 2009 as a voluntary identification mechanism intended to streamline welfare distribution, the Aadhaar project had enrolled the vast majority of Indian residents by 2017. The enactment of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 provided retrospective statutory backing and controversially mandated Aadhaar authentication for accessing numerous state subsidies and essential services. Proponents emphasised the platform's technological capabilities: biometric de-duplication, digital authentication that verifies identity without disclosing underlying transaction details, and the logistical capacity to execute Direct Benefit Transfers (DBT). These features undeniably advanced key inclusion objectives by enabling millions of rural and economically marginalised citizens to establish a verifiable legal identity and claim statutory entitlements.

Simultaneously, however, Aadhaar generated profound privacy and fundamental rights concerns. Its centralised database, the Central Identities Data Repository (CIDR), aggregated the fingerprints, iris scans, and demographic data of over 1.3 billion individuals, creating an architecture wherein subsidies, financial payments, and digital interactions could be tethered to a single permanent identifier. Legal scholars and civil liberties advocates warned that this centralised structure facilitated mass profiling, state surveillance, and the erosion of individual autonomy, concerns that were reinforced by multiple high-profile data leaks affecting both citizen and official records.

The Supreme Court of India adjudicated these competing socio-economic and constitutional imperatives across a protracted litigation saga. In the watershed 2017 decision of *Justice K.S. Puttaswamy v Union of India* (*Puttaswamy I*), a unanimous nine-judge bench declared the right to privacy to be a fundamental right guaranteed under Articles 14, 19, and 21 of the Constitution.[10] This ruling established the doctrinal foundation for the 2018 Aadhaar judgment (*K.S. Puttaswamy v Union of India (II)*), wherein a 4:1 majority largely upheld the constitutional validity of the Aadhaar Act as a legitimate mechanism for welfare delivery,

[10] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

while striking down or reading down specific provisions that failed the constitutional test of proportionality.[11] Writing for the majority, Justice A.K. Sikri held that targeted subsidy delivery and the socio-economic upliftment of the impoverished constituted legitimate state aims, and subjected each statutory provision to the three-fold test of legality, legitimate state aim, and proportionality.[12]

Crucially, the Court invalidated the mandatory linking of Aadhaar with bank accounts and mobile telephone connections, which had been introduced via 2017 regulatory amendments, characterising such blanket mandates as disproportionate infringements upon informational privacy. Furthermore, the Court prohibited the state from mandating Aadhaar enrolment for minors without parental consent, guaranteeing children an explicit right to opt out upon attaining majority at age 18, and invalidated mandatory Aadhaar linkage for school admissions and educational examinations. Conversely, the Court upheld the mandatory linking of Aadhaar with Permanent Account Numbers (PAN) to curb tax evasion and permitted its continued mandatory use for state welfare subsidies. Through this bifurcation, the majority opinion sought to balance competing facets of human dignity: individual autonomy on the one hand, and the socio-economic right to a dignified standard of living for marginalised welfare beneficiaries on the other.[13]

In arriving at this balance, the Court relied heavily on Article 14's prohibition against arbitrary and overbroad classification, observing that elementary education is an autonomous fundamental right rather than a state 'benefit' or subsidy. Although the majority did not find a direct violation of Article 19 free speech guarantees within the core statutory scheme, it invoked Articles 14 and 21 extensively to delineate the constitutional boundaries of data minimalism and informational autonomy. In a forceful dissent, Justice D.Y. Chandrachud concluded that the entire Aadhaar project, including its deployment for welfare distribution, was unconstitutional and posed an inherent threat to informational privacy and citizen autonomy. Even within the majority ruling, however, the Court established a critical constitutional ceiling: Aadhaar's deployment remains bounded by a

[11] *Justice K S Puttaswamy (Retd) v Union of India* (2019) 1 SCC 1
[12] 'Constitutionality of Aadhaar Act: Judgment Summary' (*Supreme Court Observer,* 26 September 2018) <https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/> accessed 12 August 2026
[13] 'The Indian Supreme Court's Aadhaar judgement: A privacy analysis' *International Association of Privacy Professionals* (09 October 2018) <https://iapp.org/news/a/the-indian-supreme-courts-aadhaar-judgement-a-privacy-perspective> accessed 12 August 2026

'reasonable expectation of privacy,' and its unbridled commercial exploitation by private entities is constitutionally impermissible.

Doctrinal Case Studies: Innovations and Rights Infringements –

A doctrinal assessment of Aadhaar's operational history reveals a sharp contrast between administrative innovation and constitutional vulnerability:

Technological and Administrative Innovations: Aadhaar has standardised real-time biometric authentication across public distribution systems (ration shops) and banking institutions. Government audits indicate that routing Direct Benefit Transfers through the Aadhaar architecture has substantially curtailed ghost beneficiaries and fiscal leakage. Additionally, subject to explicit user consent or statutory authorisation, financial and telecommunications institutions have utilised Aadhaar-based e-KYC to streamline onboarding, while technical protocols such as UID tokenisation, localised regulators, and shortened transaction-log retention periods were introduced to mitigate systemic risk.

Constitutional Rights Infringements: Conversely, recurring security and governance failures have exposed acute constitutional vulnerabilities. In one documented incident, Professor S.S. Prabhu discovered that unauthorised parties could access his personal Aadhaar data simply by manipulating digits of his identification number, exposing critical flaws in access-control architecture. Similarly, security researchers have demonstrated the feasibility of spoofing biometric authentication in controlled laboratory environments using high-resolution artificial fingerprints. In Jammu & Kashmir, reports of police authorities screening civilians' Aadhaar records during anti-terror operations raised serious concerns regarding unauthorised state surveillance. Furthermore, privacy researchers have documented instances of the Unique Identification Authority of India (UIDAI) sharing demographic data with third-party vendors and government departments beyond narrow statutory mandates and without informed user consent.

These operational failures demonstrate how architectural flaws in digital code directly implicate fundamental rights: unauthorised access compromises informational privacy under Article 21, while biometric authentication failures that exclude manual or migrant labourers from essential rations violate the guarantee of substantive equality under Article 14. In *Puttaswamy II*, the Supreme Court sought to mitigate these risks through targeted

judicial remedies, most notably by reading down Section 57 of the Aadhaar Act to prohibit private corporations from demanding Aadhaar for commercial services, and by striking down parts of Section 33 to ensure procedural safeguards and judicial oversight before national-security data disclosures. Together, Articles 21, 14, and 19 form an interlocking constitutional bulwark against coercive biometric profiling, even as the practical equilibrium between administrative efficiency and fundamental rights remains fragile.

UPI: FINANCIAL INNOVATION AND DATA PRIVACY

Architecture and Socio-Economic Impact: Launched in 2016 by the National Payments Corporation of India (NPCI), the Unified Payments Interface (UPI) has fundamentally reconfigured India's retail payments landscape. UPI enables instantaneous interbank fund transfers via mobile applications by routing transactions through Virtual Payment Addresses (VPAs) such as *alice@upi,* thereby masking underlying bank account numbers and IFSC details. By December 2025, the network processed over 10 billion monthly transactions across tens of millions of users. This infrastructure has substantially expanded financial inclusion: micro-merchants can accept digital payments via QR codes without costly point-of-sale hardware, rural workers can remit funds instantaneously, and fintech applications can build credit and financial services directly atop the interoperable UPI protocol. UPI's widespread adoption stems from two core design choices: mandatory network interoperability and a zero-or-negligible consumer fee structure. Unlike proprietary card networks or closed-loop digital wallets, UPI connects participating banks and third-party application providers (TPAPs) onto a unified settlement layer, making formal digital finance accessible at the economic last mile.

Transactional Privacy and Consumer Protection: Beneath its seamless consumer interface, however, UPI generates an expansive and granular trail of personal metadata. Every transaction records the payer, payee, timestamp, geolocation, monetary value, and merchant category. While the NPCI maintains macro-level records for settlement and reconciliation, participating banks and private third-party applications accumulate detailed longitudinal histories of individual financial behaviour. As financial and legal scholars observe, the 'collection of large amounts of transaction data raises privacy concerns,' particularly because private, profit-driven fintech platforms actively monetise behavioural insights. Third-party UPI applications frequently request broad mobile device permissions and operate under

heterogeneous data-handling policies, enabling consumer spending patterns to be mined for targeted advertising or commercial profiling without meaningful notice or informed consent.

Although the Supreme Court has not yet adjudicated a landmark constitutional challenge specifically targeting UPI data practices, emerging disputes highlight the stakes involved.

Rural farmers utilising UPI at agricultural auctions, for instance, are rarely informed that their digital transaction records may be visible to market regulators and third-party data brokers. Similarly, SIM-swap frauds and application-level exploits have raised questions regarding authentication resilience and the state's positive obligation to secure public digital rails. Furthermore, the growing integration of UPI profiles with Aadhaar-linked merchant settlement and credit frameworks risks merging citizens' financial and biometric identities. In 2023, a Public Interest Litigation (PIL) filed before the Delhi High Court alleged that certain prominent fintech applications were sharing UPI-linked KYC data with foreign corporate entities in circumvention of statutory consent channels—a dispute that underscores how payment metadata flows directly implicate informational privacy.

At the same time, UPI's regulatory framework has strengthened consumer agency in several procedural respects. Multi-factor authentication via cryptographic tokens and UPI PINs generates verifiable audit trails, while the Reserve Bank of India's (RBI) *Payment Systems Vision 2025* and NPCI guidelines mandate real-time grievance redressal and account-freezing mechanisms for unauthorised transactions. Nevertheless, these regulatory safeguards operate primarily as administrative consumer-protection measures rather than enforceable constitutional guarantees.

DOCTRINAL CASE STUDIES IN THE UPI ECOSYSTEM

Digital Financial Inclusion: Historically, rural micro-entrepreneurs lacked formal credit histories, excluding them from institutional banking. Financial institutions increasingly evaluate verified UPI transaction records to assess creditworthiness, exemplified by a pilot lending programme in Uttar Pradesh that extends agricultural input credit to farmers based on their digital produce sales. By mitigating information asymmetry, such initiatives advance substantive economic equality in harmony with Article 14 of the Constitution.

Transactional Privacy Breaches (Hypothetical): Consider a scenario wherein a private payment application exposes a user's complete transaction history through an unsecured Application Programming Interface (API). The public disclosure of granular financial records would directly infringe the user's fundamental right to informational privacy under Article 21 and expose them to targeted harassment, underscoring the constitutional necessity of binding security standards across all UPI intermediaries.

Opaque Algorithmic Lending: Numerous fintech platforms utilise automated credit-scoring algorithms to offer instant microloans based on UPI metadata. Because machine-learning models can inadvertently encode socio-economic bias, such as penalising seasonal or low-income agricultural workers, an unexplained algorithmic loan denial deprives the applicant of procedural due process under Articles 14 and 21, exposing a critical regulatory vacuum in Indian law.

ONDC: OPEN COMMERCE AND GOVERNANCE AMBIGUITIES

Architectural Overview: Incorporated in late 2021, the Open Network for Digital Commerce (ONDC) represents India's most recent expansion of the DPI model into the e-commerce sector. Envisioned by the central government as an 'Internet for commerce,' ONDC is neither a standalone consumer application nor a centralised marketplace; rather, it is an open-standard, interoperable network protocol that enables buyers and sellers to transact across disparate platforms.[14] By unbundling the e-commerce value chain, a consumer using one buyer application can discover and purchase goods listed by a merchant on a separate seller application, with fulfilment executed by independent logistics providers plugged into the same open protocol.

Structurally, this architecture seeks to counter platform monopolies by enabling small grocers, rural artisans, and independent vendors to access a nationwide consumer base without submitting to the commissions or proprietary ranking algorithms of dominant e-commerce marketplaces. Major incumbent platforms, including Amazon, have announced plans to integrate technical connectors with ONDC, while alpha testing has expanded across dozens of Indian cities with backing from the NPCI, the RBI, and key union ministries.

[14] Tejasi Panjiar and Prateek Waghre, 'Open Network for Digital Commerce (ONDC): An Explainer' (*Internet Freedom Foundation,* 10 March 2023) <https://internetfreedom.in/ondc-an-explainer/> accessed 12 August 2026

Incorporated as a non-profit company under Section 8 of the Companies Act, ONDC is promoted as a public digital utility and publicly commits neither to store nor to monetise transaction-level data.

Constitutional Rights and the State-Action Dilemma: Despite its public-interest mandate, ONDC's institutional structure presents acute constitutional accountability challenges. Crucially, because ONDC is constituted as a private Section 8 company rather than a statutory authority, it is not formally classified as a state actor and currently falls outside the ambit of the Right to Information (RTI) Act, 2005 and standard public audit regimes. Because fundamental rights under Part III of the Constitution are primarily enforceable against 'the State' under Article 12, this corporate structure creates a significant remedial gap: if ONDC's routing protocols or network policies arbitrarily exclude a vendor or consumer, aggrieved parties lack a direct constitutional writ remedy under Articles 32 or 226 against ONDC itself. By contrast, Estonia's X-Road infrastructure and India's RBI-regulated payments ecosystem operate under clearer statutory or regulatory oversight mandates.

Data governance within the ONDC framework remains similarly ambiguous. Although ONDC's strategy documents state that transactional data will remain siloed within participating buyer and seller applications, a large corporate conglomerate operating both buyer-side and seller-side interfaces could lawfully aggregate and correlate user data across the network through broad, boilerplate consent terms. Moreover, ONDC plans to publish anonymised, aggregate market metrics to guide network participants. As cybersecurity researchers consistently demonstrate, datasets containing even a 'handful of data points' are highly susceptible to retroactive de-anonymisation and re-identification. Absent binding statutory prohibitions, ONDC's open data flows risk facilitating cross-platform consumer profiling and anti-competitive coordination.

To illustrate the constitutional implications, consider a hypothetical scenario in which a network-level discovery or ranking protocol subtly favours large, equity-linked corporate vendors, systematically relegating a rural artisan's listings to secondary search pages without transparent criteria. While such algorithmic distortion directly implicates the artisan's right to non-arbitrary treatment under Article 14 and the right to carry on a trade or business under Article 19(1)(g), ONDC's private legal status insulates the network from direct constitutional review. Although ONDC fosters economic inclusion by reducing digital onboarding friction

and promoting market competition in the spirit of Article 19(1)(g), full constitutional alignment requires bringing the entity within the ambit of Article 12 and enacting statutory user-protection mandates.

THE CONSTITUTIONAL FRAMEWORK: PRIVACY, EQUALITY, AND EXPRESSION

The deployment of population-scale DPI must comport with the supreme law of the land. Within Part III of the Indian Constitution, Articles 21, 14, and 19 form a unified 'golden triangle' that governs digital and algorithmic state action.

Article 21: Informational Privacy, Dignity, and Procedural Due Process: Article 21 provides that '[n]o person shall be deprived of his life or personal liberty except according to procedure established by law.' In *Puttaswamy I* (2017), the Supreme Court unanimously held that the right to privacy is an intrinsic component of life and personal liberty under Article 21 and pervades Part III of the Constitution.[15] The Court conceptualised privacy expansively to encompass bodily integrity, decisional autonomy, and informational self-determination, a doctrinal foundation so robust that Justice Chandrachud's observation that 'sexual orientation is an essential attribute of privacy' subsequently anchored the decriminalisation of consensual same-sex relations via the reading down of Section 377 of the Indian Penal Code.

For the governance of DPI, *Puttaswamy I* and *Puttaswamy II* entrenched a rigorous four-prong proportionality standard: any state curtailment of privacy must be backed by law, pursue a legitimate state aim, demonstrate a rational nexus to that aim, and adopt the least intrusive means necessary. Applied to digital governance, this doctrine requires the state to justify the architectural scope of every data-collection mandate. While requiring Aadhaar authentication for targeted welfare subsidies satisfied proportionality in *Puttaswamy II*, extending that mandate to private banking and telecommunications failed constitutional scrutiny. Consequently, wholesale or unredressed state aggregation of biometric and financial metadata violates Article 21.

Furthermore, Article 21 guarantees substantive and procedural due process. Legal scholarship increasingly recognises that when public authorities deploy automated

[15] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

algorithms to allocate welfare or adjudicate civil entitlements, procedural fairness mandates prior notice, algorithmic explainability, and an accessible avenue for human appeal. If an opaque algorithm erroneously flags a beneficiary as ineligible and terminates essential food or pension subsidies without a human-readable rationale, the state infringes the citizen's right to live with human dignity under Article 21. Reflecting growing judicial sensitivity to this hazard, the Kerala High Court issued a policy in July 2025 explicitly prohibiting judicial officers from using artificial intelligence tools to generate judicial reasoning or legal conclusions. This institutional caution reinforces the principle that Article 21 demands intelligible, human-verifiable reasoning whenever state action affects life or liberty.

Article 14: Substantive Equality and Algorithmic Non-Arbitrariness: Article 14 guarantees equality before the law and the equal protection of the laws, operating as a constitutional prohibition against state arbitrariness as articulated in *E.P. Royappa v State of Tamil Nadu*. Under this doctrine, DPI architectures cannot institute irrational classifications or impose exclusionary digital barriers. In *Puttaswamy II*, the Supreme Court invoked Article 14 to invalidate mandatory Aadhaar linkage for school examinations because conditioning a universal fundamental right on biometric verification lacked a rational nexus to a legitimate subsidy scheme. By extension, if the state were to mandate UPI exclusively for all basic banking operations without accommodating citizens who rely on cash due to infrastructural or digital exclusion, such a policy would fail the test of non-arbitrariness under Article 14.

Algorithmic governance implicates Article 14 with particular acuity. Machine-learning models trained on historically skewed socio-economic datasets frequently replicate and amplify systemic bias, for instance, by assigning adverse credit-risk scores to specific religious, caste, or geographic communities. As legal scholars emphasise, constitutional equality requires that 'similarly situated people' be treated alike, yet opaque AI models routinely subvert this guarantee by operationalising proxy discrimination. Similarly, if a facial-recognition or biometric algorithm deployed within a state DPI exhibits higher false-rejection rates for marginalised demographics, resulting in the denial of public services, it violates Article 14's commitment to substantive equality. Likewise, if an automated public-housing allocation system prioritises applicants from affluent postal codes or dominant caste backgrounds without human review, affected citizens possess a compelling constitutional

claim under Article 14 read with Article 21, necessitating that all public-sector algorithms adhere to auditable, non-discriminatory criteria.

Article 19: Freedom of Expression, Information, and Digital Commerce: Article 19(1)(a) guarantees the freedom of speech and expression, which encompasses the right to receive and impart information across digital media, while Article 19(1)(g) protects the right to practise any profession, or to carry on any occupation, trade, or business. Within the DPI ecosystem, arbitrary deactivation of a citizen's digital payment profile or mandatory identity traceability across communication platforms can chill protected expression under Article 19(1)(a). In *Shreya Singhal v Union of India* (2015), the Supreme Court struck down Section 66A of the Information Technology Act, 2000 as unconstitutionally vague and overbroad, affirming that digital speech enjoys full protection under Article 19(1)(a) and may only be curtailed by narrowly tailored restrictions falling strictly within Article 19(2).

Moreover, informational autonomy under Article 21 intersects directly with economic liberty under Article 19(1)(g). If biased routing protocols or arbitrary platform rules exclude an independent driver or small merchant from a state-backed digital network such as ONDC, such exclusion directly burdens their constitutional right to trade under Article 19(1)(g) alongside Article 14. Accordingly, regulatory frameworks governing DPI intermediaries must remain strictly proportionate and safeguard open participation.

COMPARATIVE PERSPECTIVES ON DATA AND ALGORITHMIC GOVERNANCE

Evaluating India's regulatory trajectory alongside established international jurisdictions illuminates concrete legal mechanisms for embedding constitutionalism into digital infrastructure.

Jurisdiction	Primary Regulatory Framework	Key Governance & Algorithmic Safeguards	Core Lesson for India's DPI
European Union	GDPR (2016) & EU AI Act	Article 22 restricts solely automated decisions;	Demonstrates how an enforceable 'right to

		mandatory DPIAs; strict risk-based conformity assessments and human oversight for high-risk AI.	explanation,' independent regulators, and pre-deployment algorithmic audits can be codified into binding law.
United States	Fourth Amendment (Katz); Sectoral Laws (HIPAA, Privacy Act); State Laws (CCPA)	Fragmented sectoral rules; reliance on post-facto adversarial litigation and proposed federal bills (e.g., Algorithmic Accountability Act).	Illustrates that absent unified national mandates, private DPI intermediaries (such as third-party payment apps) easily evade consistent algorithmic accountability.
Brazil	Lei Geral de Proteção de Dados (LGPD, 2018)	Article 20 grants an explicit statutory right to request review of solely automated decisions and disclosure of decision criteria, though mandatory human review was diluted.	Provides a pragmatic Global South model for statutory algorithmic review rights while warning against diluting mandatory human-in-the-loop oversight.

Australia	My Health Record (MHR) Framework	Transitioned from opt-in (2012) to opt-out (2018); a 2019 national audit revealed severe privacy lapses, with only 8.2% of emergency accesses meeting criteria.	Cautions against coercive opt-out defaults and centralized data aggregation without strict access controls, as over 2.5 million citizens opted out due to eroded trust.
Estonia	X-Road Interoperability Platform	Decentralized open-source data exchange; mandatory end-to-end encryption, digital signatures, and immutable real-time citizen audit logs.	Proves that population-scale DPI can achieve seamless interoperability through decentralized architecture and transparent access logs rather than monolithic databases.

European Union: Rights-Based Algorithmic Regulation: The European Union has established the most comprehensive statutory regime for data protection and algorithmic accountability. The General Data Protection Regulation (GDPR, 2016) codifies strict data minimisation, purpose limitation, and independent regulatory oversight via national Data Protection Authorities. Crucially, Article 22 of the GDPR grants individuals the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects, mandating meaningful human intervention and fostering a statutory 'right to explanation' ethos. Furthermore, where processing poses

high risks to fundamental rights, controllers must conduct prior Data Protection Impact Assessments (DPIAs).

Complementing the GDPR, the EU Artificial Intelligence Act (proposed in 2021) institutes a tiered, risk-based regulatory framework. AI systems deployed in critical public infrastructure, creditworthiness assessment, and employment screening are classified as 'high-risk' and subjected to mandatory pre-market conformity assessments, algorithmic traceability, and human oversight principles echoed in UNESCO's global AI ethics recommendations. Grounded in Article 8 of the EU Charter of Fundamental Rights, the European model operationalises informational self-determination and guarantees citizens an enforceable 'algorithmic choice' that is notably absent from India's DPDP Act.

United States: Sectoral Fragmentation and Adversarial Remedies: In contrast, the United States lacks a unified federal constitutional or statutory right to informational privacy and algorithmic fairness. While Fourth Amendment jurisprudence stemming from Katz v United States recognises a 'reasonable expectation of privacy' against state intrusion, federal statutory protection remains compartmentalised across sectoral enactments such as the Health Insurance Portability and Accountability Act (HIPAA) and the Privacy Act of 1974. Although state-level statutes such as the California Consumer Privacy Act (CCPA) grant comprehensive consumer data rights, national coverage remains incomplete. Similarly, algorithmic governance relies largely on post-facto civil litigation, Federal Trade Commission (FTC) enforcement, and unpassed federal proposals such as the Algorithmic Accountability Act. For India, the U.S. experience demonstrates that fragmented regulation leaves private digital intermediaries largely insulated from systematic ex-ante algorithmic auditing.

Brazil: The LGPD and Statutory Review of Automated Decisions: Brazil's Lei Geral de Proteção de Dados (LGPD, 2018) offers a highly relevant comparative benchmark for a large emerging democracy. Alongside recognising data protection as a fundamental constitutional right and establishing a National Data Protection Authority (ANPD), Article 20 of the LGPD directly regulates automated decision-making. Specifically, Article 20 entitles data subjects to request a review of decisions made solely through automated processing that affect their interests and compels data controllers to provide 'clear and adequate information regarding the criteria and procedures used' upon request. While the Brazilian legislature

controversially removed an explicit requirement that such reviews be conducted by a natural person, the LGPD nonetheless demonstrates how actionable algorithmic transparency rights can be integrated directly into national data protection legislation.

Australia and Estonia: Contrasting Architectural Paradigms: The divergent trajectories of Australia and Estonia illustrate how technical architecture shapes constitutional trust. Australia's centralised digital health repository, 'My Health Record' (MHR), launched as an opt-in system in 2012 before transitioning to a mandatory opt-out model in 2018. A 2019 performance audit by the Australian National Audit Office concluded that cybersecurity and privacy risks were 'not properly managed,' revealing that a mere 8.2% of emergency privacy overrides by healthcare providers satisfied statutory criteria, a failure that prompted over 2.5 million Australians to opt out of the system.

Conversely, Estonia's X-Road platform demonstrates the viability of privacy-by-design DPI. Rather than aggregating citizen records into a monolithic central repository akin to Aadhaar's CIDR, X-Road operates as a decentralised, open-source data-exchange layer linking independent public and private databases. Every data packet is digitally signed and encrypted in transit, and every query is permanently recorded in a tamper-proof audit log that citizens can inspect in real time to verify exactly which official accessed their data and why. Estonia's architecture proves that state interoperability does not require centralised surveillance.

CRITIQUE OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Although the enactment of India's Digital Personal Data Protection Act, 2023 (DPDP Act) was heralded as a legislative milestone, a rigorous constitutional scrutiny reveals severe structural deficiencies in its regulatory independence, executive exemptions, and omission of algorithmic safeguards.

Hyper-Centralization and Executive Control of the Data Protection Board: The DPDP Act establishes the Data Protection Board of India (DPB) as the sole adjudicatory body responsible for monitoring compliance and imposing statutory penalties.

However, the statute exhibits two profound structural flaws –

Lack of Institutional Independence: All members of the DPB are appointed directly by the Central Government, predominantly from the executive branch, without mandatory judicial selection oversight. Furthermore, Section 27(3) of the DPDP Act empowers the Central Government to issue binding directions to the DPB on matters of national security or public order, effectively subordinating the regulator to executive command and violating the constitutional doctrine of separation of powers.

Administrative Over-Centralization: Establishing a single centralised board in New Delhi to adjudicate disputes across more than one billion data principals and an estimated 50 million data fiduciaries creates an insurmountable administrative bottleneck. Moreover, the Act restricts primary enforcement to Board proceedings and bars citizens from directly approaching specialised civil courts.

Legal commentators and the *Supreme Court Observer* have consequently characterised the DPB as a 'toothless tiger.' Compounding this weakness, the DPDP Act grants the Central Government sweeping authority to exempt any state instrumentality from the Act's provisions via executive notification on broad grounds of sovereignty, security, or public order. Such unchecked executive exemptions bypass parliamentary oversight and subvert the four-prong proportionality standard mandated under Article 21 in *Puttaswamy I* and *Puttaswamy II*.

The Algorithmic Accountability Vacuum: Equally concerning is the DPDP Act's silence on automated decision-making and algorithmic governance. Beyond a baseline stipulation requiring data fiduciaries to ensure that personal data used to make a decision affecting a data principal is 'complete, accurate and consistent,' the statute contains no equivalent to Article 22 of the EU GDPR or Article 20 of Brazil's LGPD. The Act confers no statutory right to an explanation, no right to contest solely automated decisions, no requirement for human-in-the-loop review, and no mandate for Algorithmic Impact Assessments or bias audits. Furthermore, while the Act prescribes financial penalties of up to INR 250 crore for severe data breaches, smaller corporate intermediaries that fall below the threshold of 'Significant Data Fiduciaries' face minimal proactive auditing obligations. Consequently, if a public authority or private fintech intermediary deploys a biased algorithm to deny welfare benefits

or credit, the DPDP Act affords the aggrieved citizen no meaningful legal recourse to interrogate the underlying code.

PROPOSALS FOR LEGAL, TECHNICAL, AND INSTITUTIONAL REFORM

To align India's expanding Digital Public Infrastructure with the transformative vision of the Constitution, this paper proposes seven concrete reforms:

Constitutionalising an Independent Data Protection Authority: Parliament should amend the DPDP Act to replace the executive-controlled DPB with a genuinely independent, decentralised regulatory commission featuring regional benches. Selection committees must include senior members of the judiciary, the leader of the opposition, and independent technical and civil-society experts, with statutory security of tenure insulated from Section 27(3) executive directives.

Establishing an Algorithmic Oversight Mechanism: The legislature should constitute a specialised Algorithmic Oversight Board and mandate pre-deployment Algorithmic Impact Assessments (AIAs) and periodic bias audits for all high-risk DPI systems. Citizens must be granted an enforceable statutory right to explanation and mandatory human review whenever an automated decision affects their legal rights, welfare entitlements, or livelihood.

Expanding Statutory Data Principal Rights: The DPDP Act must be strengthened to codify robust individual rights beyond mere consent withdrawal, including an explicit right to data portability, an enforceable right to erasure, and an unconditional right to opt out of automated behavioural profiling.

Expanding Article 12 State-Action Jurisprudence for DPI Entities: Parliament and the judiciary should formally clarify that core DPI governance entities performing public functions, specifically UIDAI, NPCI, and ONDC, constitute instrumentalities of 'the State' under Article 12 of the Constitution, thereby subjecting them directly to the Right to Information Act, public administrative law, and writ jurisdiction under Articles 32 and 226.

Mandating Privacy-by-Design Technical Standards: Drawing directly from Estonia's X-Road architecture, India's DPI protocols must statutorily mandate federated data storage, end-to-end encryption, strict data minimisation, and immutable citizen-accessible audit logs that record every public or private query made against a citizen's digital records.

Entrenching Affirmative Opt-In Consent and Offline Alternatives: To safeguard decisional autonomy under Article 21 and substantive equality under Article 14, all DPI layers must operate on granular, affirmative opt-in consent and guarantee viable non-digital alternatives so that technological or biometric failures never result in the denial of essential public services.

Instituting Permanent Parliamentary Oversight: Parliament should establish a permanent Joint Parliamentary Committee on Digital Governance empowered to conduct periodic statutory audits of all DPI architectures, data-sharing agreements, and national-security exemptions, mirroring established fiscal oversight mechanisms.

CONCLUSION

India's Digital Public Infrastructure demonstrates how population-scale platforms for identity, payments, and commerce can catalyse socio-economic inclusion and administrative efficiency. Yet, as the operational trajectories of Aadhaar, UPI, and ONDC illustrate, code-based governance simultaneously introduces profound risks of surveillance, exclusion, and algorithmic arbitrariness. Piecemeal administrative guidelines and executive-dominated frameworks cannot resolve these tensions. Instead, India's digital architecture must be subordinated to the normative discipline of constitutionalism, guided by the interlocking guarantees of Articles 21, 14, and 19.

Under the *Puttaswamy* jurisprudence, every technological intrusion upon informational privacy demands strict proportionality and demonstrable necessity. Under Article 14, automated classification systems must be purged of proxy bias and subjected to rigorous non-arbitrariness scrutiny. Comparative international experience confirms that statutory rights to algorithmic explanation, decentralised interoperability, and independent regulatory oversight are entirely compatible with technological innovation. By contrast, the Digital Personal Data Protection Act, 2023 currently falls short of these constitutional imperatives, leaving automated decision-making largely unregulated and insulating state data processing through broad executive exemptions. Only by establishing independent regulatory oversight, codifying enforceable algorithmic rights, and embedding privacy-by-design into the technical architecture of DPI can India ensure that digital code serves as an instrument of constitutional justice upholding the life, liberty, equality, and dignity of every citizen.