The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

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.

FROM ARTICLE 39 TO DIGITAL PUBLIC INFRASTRUCTURE: CONSTITUTIONALISING DATA, WELFARE, AND ALGORITHMIC GOVERNANCE

~Ashish Kumar Swain

ABSTRACT

The Directive Principles of State Policy, particularly Article 39 of the Constitution of India, impose on the State a duty to secure the distribution of material resources of the community so as to best serve the common good. This article argues that digital public infrastructure, including broadband networks, Aadhaar, the Unified Payments Interface, and welfare delivery platforms, constitutes a new category of material resource to which Article 39 applies with full force. Drawing on the theory of the commons, constitutional text, and comparative policy experience, the article proposes a DPSP-linked Digital Commons Charter as a framework of constitutional-policy norms to govern data sharing, algorithmic fairness, and public-service digitalisation. It is argued that the Digital Personal Data Protection Act, 2023, though a welcome development, addresses only one dimension of the problem and that a broader constitutional framework grounded in the Directive Principles is necessary to ensure that digital infrastructure serves public interest rather than private accumulation.

INTRODUCTION

When the framers of the Indian Constitution inserted the Directive Principles of State Policy into Part IV, they were thinking primarily about land, factories, and financial credit. Article 39, which directs the State to ensure that the ownership and control of material resources are distributed to serve the common good,[1] was drafted with the inequalities of an agrarian colonial economy in mind. Seven decades later, the most consequential material resource in

[1]Constitution of India, 1950, art 39.

the Indian economy is not agricultural land or industrial capital but data, and the infrastructure through which data flows.

India has built, at extraordinary speed, a set of digital public goods that collectively form what is now called the India Stack: Aadhaar, the biometric identification system covering over 1.3 billion residents; the Unified Payments Interface, which processes billions of transactions monthly; and a growing family of welfare delivery platforms, from the CoWIN vaccination system to the Direct Benefit Transfer architecture. These systems are not merely technical conveniences. They are the infrastructure through which the State exercises its welfare functions, through which citizens access their entitlements, and through which vast quantities of personal and transactional data are generated, held, and used.

This article makes two related arguments. First, that digital public infrastructure of this kind is a material resource within the meaning of Article 39, and that the constitutional duty to govern it in the public interest is not a matter of legislative choice but of constitutional obligation. Second, that while the Digital Personal Data Protection Act, 2023 (DPDP Act) offers a framework for individual data rights, it does not address the structural questions about who controls digital infrastructure and how it is governed. Filling that gap requires a Digital Commons Charter grounded not just in data protection law but in the Directive Principles themselves.

PART I: ARTICLE 39 AND THE CONSTITUTIONAL THEORY OF THE COMMONS

1. THE DIRECTIVE PRINCIPLES AS JUSTICIABLE POLICY NORMS

The standard account of the Directive Principles treats them as non-justiciable aspirations, politically significant but legally unenforceable. This account is incomplete. In *Kesavananda Bharati v. State of Kerala,*[2] the Supreme Court held that the harmony between Fundamental Rights and Directive Principles is itself a feature of the Constitution's basic structure. Subsequent decisions have read specific Directive Principles into justiciable rights through Article 21. The right to livelihood, recognised in *Olga Tellis v. Bombay Municipal Corporation,*[3] was derived partly from the directive in Article 39(a) that citizens have the right to an adequate means of livelihood. The right to health and the right to education followed the same interpretive path.

---

[2]*Kesavananda Bharati v. State of Kerala*, AIR 1973 SC 1461.
[3]*Olga Tellis v. Bombay Municipal Corporation*, AIR 1986 SC 180.

What this body of jurisprudence establishes is that the Directive Principles, read alongside Article 21, generate constitutional-policy obligations that constrain legislative and executive action. A law or policy that actively defeats a Directive Principle, or that concentrates control of material resources in private hands in a manner that forecloses their public benefit, is not constitutionally neutral. The question is whether the same logic applies to digital infrastructure.

2. DIGITAL INFRASTRUCTURE AS MATERIAL RESOURCE

The text of Article 39(b) refers to the distribution of the "material resources of the community." The Supreme Court has never exhaustively defined this phrase. In the early cases, it was applied to land and natural resources. There is no principled reason, however, why the concept should be limited to tangible assets. What matters is whether a resource is material to the economic and social life of the community and whether its concentration in private hands without public oversight produces the kinds of inequalities and exclusions that the Directive Principles were designed to address.

Digital infrastructure meets both criteria. Broadband connectivity is as foundational to economic participation today as road access was in an earlier era.[4] Aadhaar is the gateway through which over a billion people access welfare entitlements, financial services, and government platforms.[5] The data generated by these systems is not merely a private commercial asset; it is a product of collective social activity, generated by millions of citizens going about their daily lives. To treat this data as belonging entirely to the platforms and agencies that collect it, to be monetised or withheld as those entities see fit, is to permit exactly the kind of concentration of community resources that Article 39(b) was intended to prevent.

3. THE COMMONS FRAMEWORK

The concept of the commons, developed most rigorously by Elinor Ostrom,[6] refers to resources that are held collectively and governed by shared rules rather than individual property rights or pure State ownership. Ostrom's work showed that communities can govern common resources sustainably through institutional arrangements that are neither market-based nor

---

[4]Ministry of Electronics and Information Technology, Government of India, *India's Trillion Dollar Digital Opportunity* (2019) 9.
[5]UIDAI, *Aadhaar Enrolment Statistics*, accessed 1 May 2024 <uidai.gov.in>.
[6]Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge University Press 1990) 30.

bureaucratic, provided those arrangements are designed around principles of inclusive access, clear rules, participatory governance, and accountability.

Digital commons theory extends this framework to non-rivalrous informational resources.[7] Data, unlike land, is not depleted when used; one person's access does not diminish another's. This makes digital resources particularly suitable for commons governance. The argument is not that data should be nationalised or that private companies should be dispossessed of what they generate, but that data and digital infrastructure which carry public functions or are produced through mass public participation must be governed with reference to public interest norms, not solely on the basis of whoever has the technical capacity to collect and store it.

PART II: THE CURRENT FRAMEWORK AND ITS CONSTITUTIONAL GAPS

1. THE DPDP ACT, 2023: SCOPE AND LIMITATIONS

The Digital Personal Data Protection Act, 2023 is India's first comprehensive data protection legislation. It establishes a framework of individual rights over personal data: the right to know what data is being collected, the right to correct it, and the right to have it erased.[8] The Act creates obligations for data fiduciaries, the entities that determine the purposes and means of data processing, and establishes a Data Protection Board to adjudicate complaints.

These are genuine contributions. The DPDP Act addresses the individual dimension of the data protection problem: the relationship between a particular person and the entity that holds their data. What it does not address is the structural or collective dimension. It does not regulate how digital infrastructure owned or operated by the State is designed, how the data generated by welfare programmes is used, whether algorithmic systems used in public service delivery are audited for fairness, or how citizens as a community rather than as individuals have any say in how their collective data is governed. These are not gaps in the DPDP Act that can be filled by secondary legislation. They require a different constitutional-policy framework entirely.

---

[7]Yochai Benkler, 'Commons-Based Peer Production and Virtue' (2006) 14 Journal of Political Philosophy 394, 396.

[8]The Digital Personal Data Protection Act, 2023, s 4.

2. THE AADHAAR EXPERIENCE

The constitutional history of Aadhaar illustrates the gap clearly. In the 2019 Aadhaar judgment,[9] the majority upheld the scheme on the basis that it served the Directive Principles' objectives of targeted welfare delivery. Justice Chandrachud, dissenting, raised concerns that the mandatory linkage of Aadhaar to welfare entitlements effectively conditioned the exercise of fundamental rights on submission to biometric surveillance.[10] Whatever view one takes of the merits, the case demonstrates that digital infrastructure carrying welfare functions raises constitutional questions that cannot be resolved purely within the framework of individual privacy rights. The question of how a biometric database of over a billion people is governed, who has access to it, on what terms, and subject to what accountability mechanisms is a question about the governance of a community resource, not just about individual data protection.

3. ALGORITHMIC GOVERNANCE AND ARTICLE 14

A further gap in the existing framework concerns algorithmic decision-making in public services. Welfare entitlements, tax assessments, and policing priorities are increasingly determined, at least in part, by automated systems. These systems are largely opaque.[11] The DPDP Act does not require algorithmic transparency or impact assessments for systems used by the State. Yet where an algorithm determines whether a citizen receives a ration card or a welfare payment, the right to equality under Article 14 is squarely engaged. Arbitrary or discriminatory algorithmic outputs, even where unintentional, constitute State action and must be amenable to constitutional scrutiny. The current legal framework offers no systematic mechanism for this.

PART III: TOWARDS A DIGITAL COMMONS CHARTER

The proposal here is not for fresh legislation in the conventional sense, though legislative action may eventually be required. It is for a set of constitutional-policy norms, derived from the Directive Principles and the Fundamental Rights, that should inform the design, operation, and governance of digital public infrastructure. These norms are gathered here under the label of a Digital Commons Charter. The Charter is not a draft Bill; it is a

---

[9] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 (Aadhaar-5J).
[10] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1, paras 334-339 (Chandrachud J, dissenting).
[11] Frank Pasquale, *The Black Box Society* (Harvard University Press 2015) 3.

framework of principles that any law, regulation, or executive policy governing digital public infrastructure should be required to respect.

PILLAR 1: EQUITABLE ACCESS AS CONSTITUTIONAL BASELINE

Article 39(a) directs the State to ensure that citizens have adequate means of livelihood.[12] Article 41 directs it to secure the right to work and public assistance. Read together in the context of an economy where digital access is a precondition for employment, banking, education, and welfare, these Directive Principles generate a constitutional imperative for universal and affordable digital connectivity. The Digital Commons Charter should establish equitable digital access as a baseline obligation, meaning that no welfare entitlement may be conditioned on digital access without the State first ensuring that such access is genuinely available to the intended beneficiaries. This is not a new right created by the Charter; it follows from the constitutional obligations that already exist.

PILLAR 2: PUBLIC-TRUST GOVERNANCE OF DIGITAL PUBLIC INFRASTRUCTURE

The India Stack, however operationally efficient, is currently governed through a patchwork of administrative arrangements without a unified constitutional-policy framework. Aadhaar is governed by the Unique Identification Authority of India under the Aadhaar Act, 2016; UPI is governed by the National Payments Corporation of India, a private entity with public functions; and welfare platforms are managed by individual ministries under no consistent governance standard.[13] The Digital Commons Charter should require that all digital infrastructure carrying public functions be governed under a public-trust model. The core obligations of a public trust are to manage the resource for the benefit of the public, to act with transparency, and to be accountable to those whose interests it serves. Applied to digital infrastructure, this means that decisions about data architecture, access policies, and system design must be made with public participation and subject to legislative oversight, not simply within the discretion of the administering agency.

PILLAR 3: DATA SHARING IN THE PUBLIC INTEREST

One of the constitutional concerns with the current data economy is that data generated through public-funded infrastructure, or through the collective activity of citizens using State services, is held in silos and used primarily to serve institutional rather than public interests.

---

[12]Constitution of India, 1950, art 38.

[13]Ministry of Finance, Government of India, *Economic Survey 2022-23*, Vol. I, Ch. 11 (Digital Public Infrastructure).

Article 39(b)'s requirement that the ownership and control of material resources be distributed to serve the common good has a positive dimension: it requires not merely that resources not be concentrated in private hands, but that they be made available in ways that advance collective welfare. The Digital Commons Charter should establish a principle of public-interest data sharing, under which anonymised or aggregated data generated by publicly funded digital systems is made available to researchers, civil society, and other public-interest actors under appropriate safeguards. This principle is consistent with the DPDP Act's consent framework and does not require personal data to be disclosed; it requires that the community resource value of public data be recognised and acted upon.

PILLAR 4: ALGORITHMIC FAIRNESS AND CONSTITUTIONAL ACCOUNTABILITY

Any automated system used by a state actor to make or inform decisions that affect the rights or entitlements of citizens must, under Article 14, be capable of rational justification and must not produce discriminatory outcomes.[14] The Digital Commons Charter should require mandatory algorithmic impact assessments for all such systems before deployment, periodic audits by independent bodies, and the publication of results. Where an algorithmic system is found to produce systematically discriminatory outcomes, it should be suspended pending redesign. Citizens adversely affected by automated public-sector decisions should have a right to human review and to reasons. These requirements follow from existing constitutional obligations and do not depend on the enactment of new rights.

PILLAR 5: DPSP-ANCHORED DIGITAL WELFARE STANDARDS

Articles 38, 39, 41, and 46 of the Constitution collectively describe a welfare State that is actively committed to reducing inequality, securing social and economic justice, and protecting the interests of weaker sections.[15] These provisions should inform the design of welfare delivery platforms. This means, practically, that platforms used to deliver food, housing, health, or educational entitlements must be designed with accessibility for the digitally excluded as a non-negotiable requirement; that exclusion errors caused by technical failures must trigger immediate redress rather than bureaucratic delay; and that the efficiency metrics

[14]Constitution of India, 1950, art 21; *Paschim Banga Khet Mazdoor Samity v. State of West Bengal*, (1996) 4 SCC 37.
[15]Constitution of India, 1950, arts 38, 39, 41, 46.

by which such platforms are evaluated must include constitutional welfare indicators, not only transaction volumes and cost savings.[16]

CONCLUSION

The argument of this article rests on a straightforward proposition: the constitutional obligations imposed by the Directive Principles do not become less applicable because the resources at stake are digital rather than material in the conventional sense. Article 39's mandate to distribute material resources in the public interest applies to broadband infrastructure, to the Aadhaar database, to the UPI architecture, and to welfare delivery platforms, because these systems are, in the most meaningful sense, material resources on which the economic and social participation of hundreds of millions of citizens depends.

The DPDP Act, 2023 is a step in the right direction, but it addresses only the individual privacy dimension of the problem. The structural questions, who governs digital public infrastructure, on what terms data generated by public systems is shared, how algorithmic decisions in welfare delivery are made accountable, and how universal access is secured as a constitutional baseline, require a framework rooted in the Directive Principles themselves. The Digital Commons Charter proposed here is that framework. Its five pillars, equitable access, public-trust governance, public-interest data sharing, algorithmic accountability, and DPSP-anchored welfare standards, are not legislative novelties. Each follows from constitutional obligations that already exist, waiting to be applied to a domain the framers could not have anticipated but would certainly have recognised as calling for constitutional attention.

India's digital infrastructure is a public achievement built on public investment and mass public participation. Governing it as a commons is not a policy preference; on a proper reading of Part IV, it is a constitutional requirement.

---

[16]Reserve Bank of India, *Annual Report 2022-23*, 118 (UPI transaction statistics).