THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

June 17, 2025

Rights in the Aadhaar Machine

By: John Simte

A recent judgement of the Supreme Court engages with the consequences of failures in digital public infrastructures that deny rightful entitlements.

In April 2025, the Supreme Court of India delivered a landmark judgment in *Pragya Prasun & Ors. v. Union of India*, declaring a fundamental right to inclusive and meaningful digital access. The petitioners, who had been denied essential services, highlighted how existing identification and verification protocols, particularly those involving facial recognition, video authentication, and gesture-based inputs, failed to accommodate physical conditions such as facial injuries, visual impairments, or restricted mobility. The petitioners' inability to meet these rigid requirements led to their exclusion from digital platforms delivering welfare and public services.

The court held that these exclusions violated the principles of equality, dignity, and autonomy and called for a structural rethinking of how digital infrastructure is designed and regulated. At its core, the ruling widens the horizon of legal recognition and opens a deeper inquiry: how are digital systems designed, who are they designed for, and how do they respond to the full range of human diversity?

> Exclusion is rationalised as error, and individuals are expected to conform to a system that was never designed with them in mind.

India's prevailing model of digital governance has been described by the researcher Mila T. Samdub as being animated by a "Bangalore ideology," one that replaces deliberative democracy with platform efficiency and imagines public administration as a coding problem. Designed and implemented by engineers and bureaucrats, often in partnership with private entities, they have limited avenues for democratic input or redress. Exclusion is rationalised as error, and individuals are expected to conform to a system that was never designed with them in mind.

Aadhaar, the Unique Identification (UID) project, is a prime example. Its core promise is that biometric and demographic data will allow seamless, cross-platform verification of individual identity. This promise rests on the assumption that bodies are stable, legible, and consistently machine-readable.

For large segments of the Indian population, that assumption does not hold. Elderly individuals fail iris scans due to ageing. Manual labourers with worn fingerprints from years of physical work are unable to pass fingerprint verification. Children's biometric profiles change as they grow, producing mismatches in systems that expect biometric constancy. Gender non-conforming persons face authentication challenges due to discrepancies between lived identity and official records.

> Democratic citizenship is compromised when access to public services hinges on biometric compatibility or flawless documentation.

These experiences are not isolated. They stem from a structural logic that limits access to those who meet a narrow profile of digital legibility. When the body cannot be authenticated, the person becomes invisible to the state and excluded from the circuit of rights and services. In 2017, Santoshi Kumari, an 11-year-old girl from Jharkhand, died of starvation after her family's ration entitlement was cancelled due to an Aadhaar-related failure. System errors like this are all too common and cumbersome to sort out. The denial of rations, education, or income due to a data mismatch or unscanned fingerprint is an outcome of a design that assigns responsibility to the individual for failures produced by the system itself. When something goes wrong, the default assumption is that the user made a mistake.

> [In *Puttaswamy II,] f*ailures in authentication were treated by the court as "disputed questions of fact," and it declined to examine their constitutional implications.

The legal imprimatur for Aadhaar was the majority judgment in *Puttaswamy II* (2018), which relied on proportionality to uphold the constitutionality of Section 7 of the Aadhaar Act, which mandates Aadhaar for welfare entitlements. The judgment accepted the state's

claim that no beneficiary would be denied for lack of Aadhaar, and took assurances and circulars at face value, without accounting for ground-level implementation failures. However, the court dismissed reports of systemic exclusion as either anecdotal, unverified, or unsubstantiated. Submissions and studies documenting failures in authentication were treated by the court as "disputed questions of fact," and it declined to examine their constitutional implications. It was on this foundation that the court held the privacy trade-off to be minimal and proportionate.

Justice D.Y. Chandrachud's dissent in *Puttaswamy II* focused squarely on the structural risks of embedding biometric authentication in essential service delivery. He warned that systems premised on biometric uniformity and centralised databases entrench inequality when they fail to accommodate human diversity. These systems assume a normative user – able-bodied, digitally fluent, and machine-legible – and in effect marginalise those whose bodies or circumstances do not align. In Chandrachud's view, the denial of essential services due to failed authentication would be a breach of constitutional protections. He argued that the constitutionality of such systems must be tested against their real-world impact, particularly on the most vulnerable.

Nonetheless, following the majority ruling in *Puttaswamy II*, digital infrastructure (and the use of Aadhaar authentication) expanded along the very axis the dissent had cautioned against. Precise biometric matches and rigid compliance with authentication protocols became both universal and ubiquitous, and the burden has disproportionately affected those most reliant on welfare safety nets.

> *Pragya Prasun* affirms that constitutional entitlements endure even when technological systems are inaccessible.

In this landscape, *Pragya Prasun* offers a constitutional course correction to reassert the primacy of rights in the architecture of public systems. The judgment engages directly with the consequences of the failure of digital public infrastructures. *Pragya Prasun* affirms that constitutional entitlements endure even when technological systems are inaccessible. Inaccessibility is treated as a system-level failure, and digital infrastructures are subject to constitutional review. The ruling restores constitutional scrutiny to how systems are designed, implemented, and governed.

Importantly, the judgement notes that when digital systems assume standardised user behaviour, they overlook the range of physical, sensory, and cognitive diversity in the population. Petitioners flagged specific features, such as compulsory blinking during live capture, perfect alignment with facial templates, and interpretation of motion graphics, as rendering platforms inaccessible to persons with disabilities. *Pragya Prasun* found that these embedded design defaults imposed a disproportionate burden on individuals with non-normative bodies and held that such structural barriers amounted to violations of Articles 14, 15, and 21 of the Constitution. It expanded the site of constitutional injury from the user's limitations to also include the architecture of the system itself.

> Systems must be shaped around those they have historically left out. Only then can digital infrastructure foster inclusion and avoid reproducing erasure.

To remedy this, it issued 20 targeted directions to reconfigure the digital Know Your Customer (KYC) framework. These include enforcing accessibility standards across all platforms, allowing paper-based and offline options, validating thumb impressions as legitimate authentication methods, and removing rigid interpretations of "liveness" that prevent access. Regulatory institutions, including the Reserve Bank of India, Securities and Exchange Board of India, and the Department of Telecommunications, have been instructed to revise protocols, conduct accessibility audits, and establish assistance mechanisms for those who require them.

> The judgment also signals that the architecture of access is equally the architecture of belonging.

By placing legal responsibility within the design of systems, the judgment also signals that the architecture of access is equally the architecture of belonging. Democratic citizenship is compromised when access to public services hinges on biometric compatibility or flawless documentation. A fingerprint mismatch or failed facial scan does not cancel an individual's legal standing. The person standing before a screen, at a kiosk, or with a banking correspondent remains a rights-bearing citizen. As digital systems increasingly mediate access to welfare, finance, education, and civic entitlements, their architecture shapes the conditions of visibility and participation. Design choices determine who is recognised and who is excluded. This recognition imposes concrete obligations on institutions. Accordingly, public infrastructure must reflect the diversity of bodies, social and cultural contexts, and the material constraints that define real-world access.

Andrew Feenberg reminds us that design is never neutral. Every technological form encodes assumptions about users, authority, and legitimacy. When systems are calibrated for conformity, they validate only those who match their internal logic. What appears efficient in code may conceal profound social injury. Exclusion becomes a predictable outcome of design and cannot be treated as a mere operational oversight. Correcting these demands entails more than mere interface changes. It requires confronting the politics embedded in architecture, logic, and use. Systems must be shaped around those they have historically left out. Only then can digital infrastructure foster inclusion and avoid reproducing erasure.

John Simte is a lawyer and legal researcher.