

The Aadhaar Paradox

A Promise of Inclusion, A Reality of Exclusion
in India's Welfare System



The debate over Aadhaar is not about technology;
it is about the constitutional right to life.



***“No person shall be deprived
of his life or personal liberty
except according to procedure
established by law.”***

Article 21 of the Constitution of India

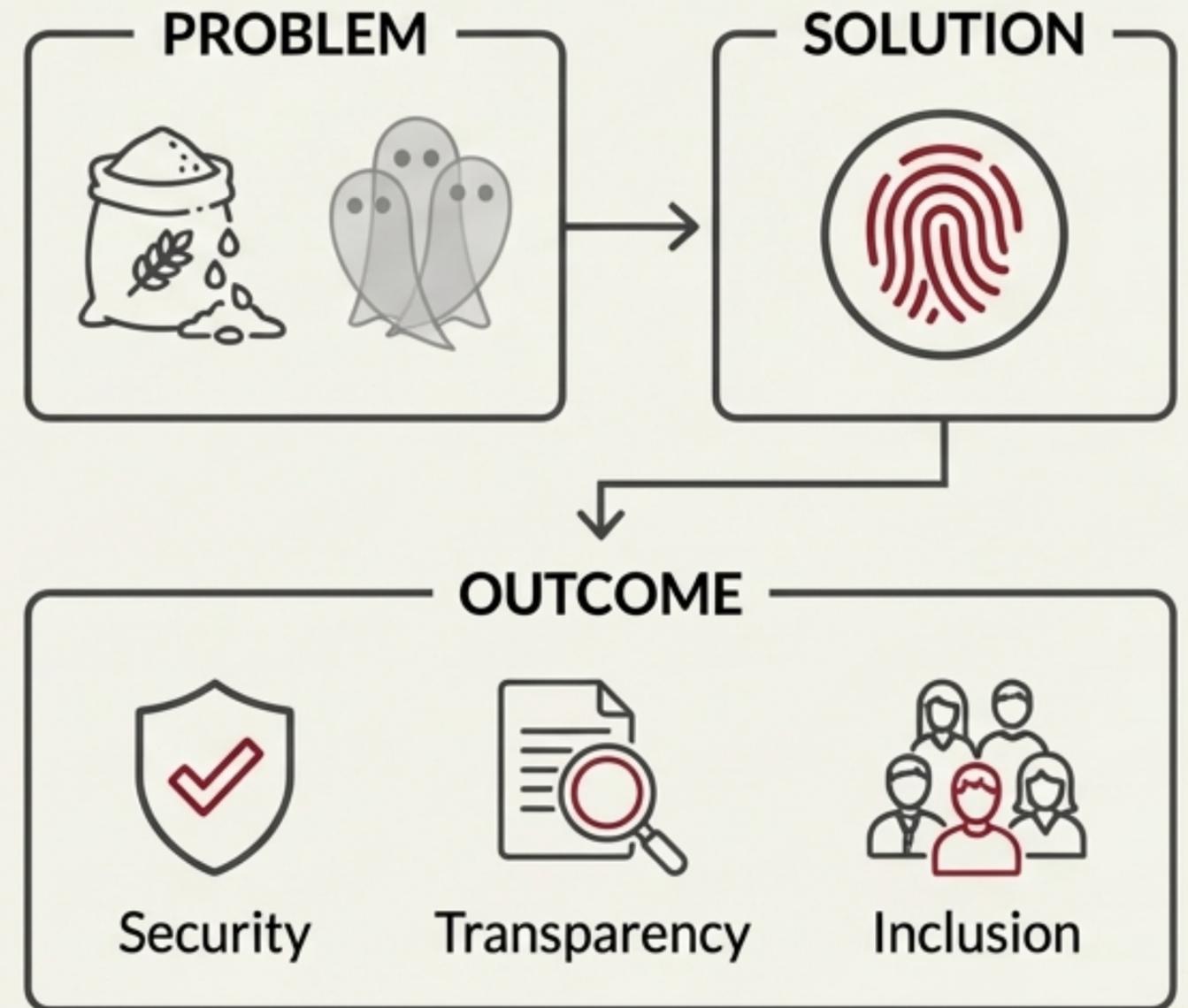


***“Every time I visit the ration
shop, I am told that my
biometrics do not work.”***

Jasoda Munda, 47, a daily wage labourer who
went eight to nine months without rations.

The Promise: A seamless digital key to unlock welfare for 800 million people.

- The National Food Security Act (2013) entitled up to 75% of the rural and 50% of the urban population to subsidised food grains.
- However, the system was plagued by identity fraud, duplicate beneficiaries, and 'ghost' recipients, leading to significant leakages.
- In 2017, Aadhaar biometric authentication was made mandatory for the Public Distribution System (PDS) to ensure subsidies reached genuine beneficiaries, enhance efficiency, and curb corruption.
- The goal was to create a 'single source of truth' for identity, forming the backbone of India's digital public infrastructure.

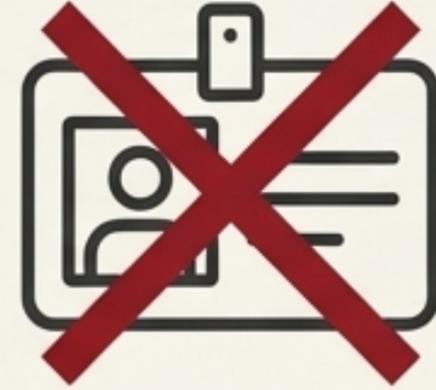


The government claimed unprecedented savings by eliminating fraud and duplication.



₹2.7 lakh crore

Savings attributed to the Direct Benefit Transfer (DBT) scheme, enabled by Aadhaar, through the avoidance of 'leakages'. (Source: Finance Minister Nirmala Sitharaman, 2024 Budget Speech).



5.03 crore

'Duplicate and fake/non-existent' ration cards were deleted from the system as of March 2023. (Source: Dept. of Food and Public Distribution).

The official narrative presented this reduction not as potential exclusion, but as a victory for administrative efficiency and fiscal prudence. The fall in beneficiaries was treated as savings.



The Reality: A fragile biometric lock that excludes the most vulnerable.

The system assumes a stable, machine-readable body, but fingerprints and irises change with age, manual labour, and disability. This is not a 'glitch,' but a fundamental design flaw.

Case Study 1: Bonjh Hembrom, 88: An elderly indigenous farmer. His fingerprints, worn smooth by age, repeatedly failed authentication at the ration shop. He was turned away empty-handed.

Case Study 2: Sukra Oram, 83: An Adivasi woman. Her fingers, bent with age, could not be straightened for the scanner. She was denied her pension and rations for the last 16 months of her life and passed away in July.

"The machine does not recognise me." - Sukra Oram

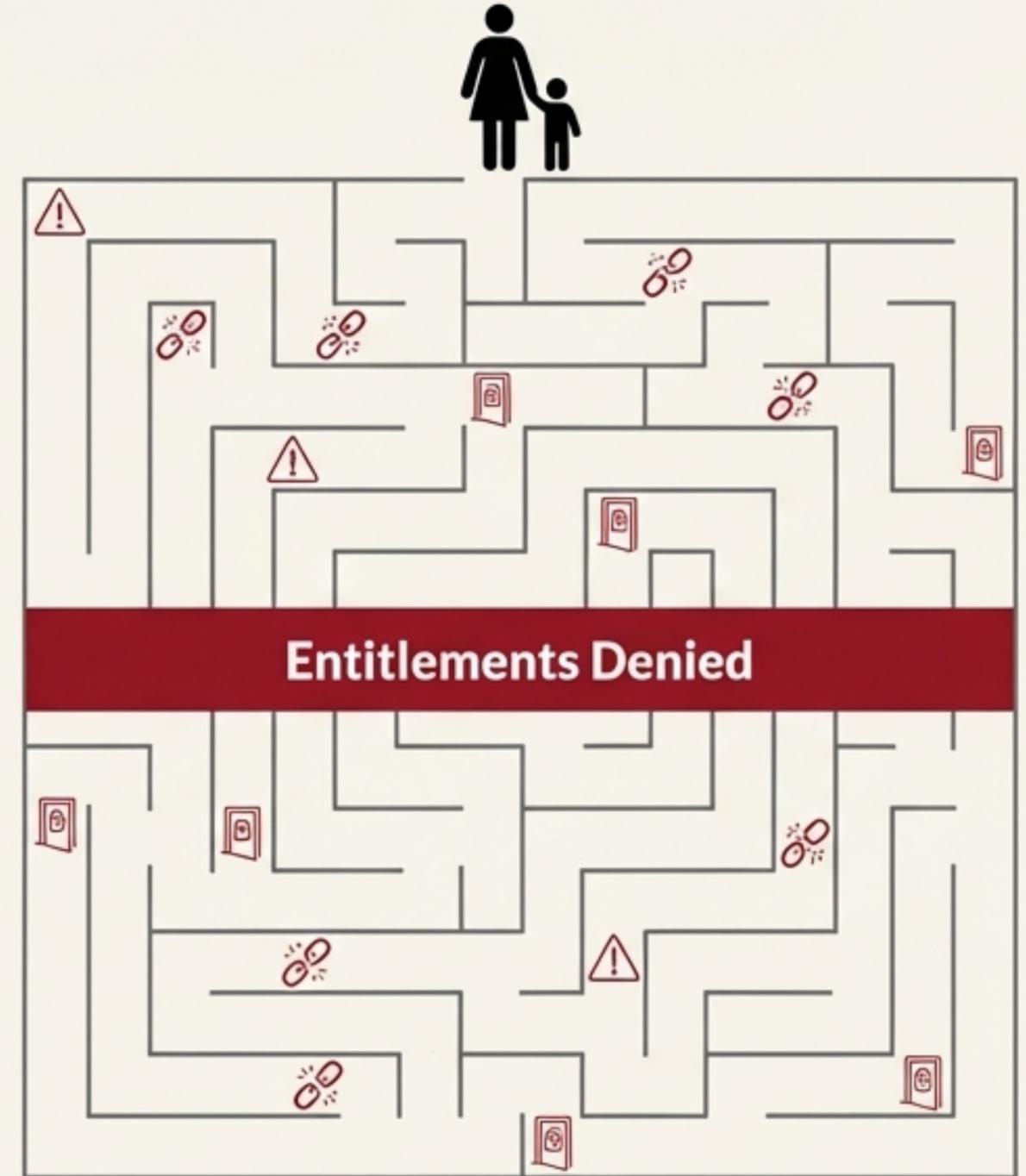
Beyond biometrics, citizens are lost in a maze of data errors and digital divides.

Failure Point 1: Data Mismatches & Deletions

- **Case:** '11-year-old Arjun Hembrom died after his family's ration card became inactive due to a name mismatch between the card and Aadhaar.'
- **Case:** 'Masuri Pingua's six-member family lost rations in 2017 after their card was 'apparently deleted from the portal'.

Failure Point 2: The Burden of 'Digital Literacy'

- **Case:** '11-year-old Jyotsna Samad's name was deleted from her family's card during an 'online update'.
- **Insight:** 'Making Aadhaar seeding mandatory overlooks women's lower access to mobile phones (only 38% ownership in India) and digital skills, forcing dependence on male relatives and restricting autonomy.'



For some, a failure to authenticate has become a death sentence.



Santoshi Kumari, 11 years old.

In Jharkhand, Santoshi died of starvation in 2017. Her family's ration card was cancelled because it had not been linked to an Aadhaar number. The denial of subsidised food grains led directly to her death, becoming a national symbol of Aadhaar's deadly consequences.

“To deny food is to lead a family to destitution, malnutrition and even death. No failure rate in the provision of social welfare benefits can be regarded as acceptable.”

- Justice A.K. Sikri, K.S. Puttaswamy v. Union of India

The 'savings' from Aadhaar are built on a foundation of mass exclusion.

4.39 Crore

The number of ration recipients deleted from the PDS system between 2013 and 2021. Entries lacking an Aadhaar number were often identified as 'ghosts' and removed.



10 Crore

The estimated number of people excluded from the NFSA safety net due to delays in conducting the Census, which is used to determine PDS beneficiary quotas.

"A fall in the number of genuine beneficiaries is now treated as savings or a reduction in government expenditure. ... Aadhaar seems to have become a tool to impede access to existing benefits." – Reetika Khera, Economics Professor, IIT Delhi

The system's primary flaw is not technical, but philosophical: it was designed to mistrust the poor.

Concept: Framing Bias

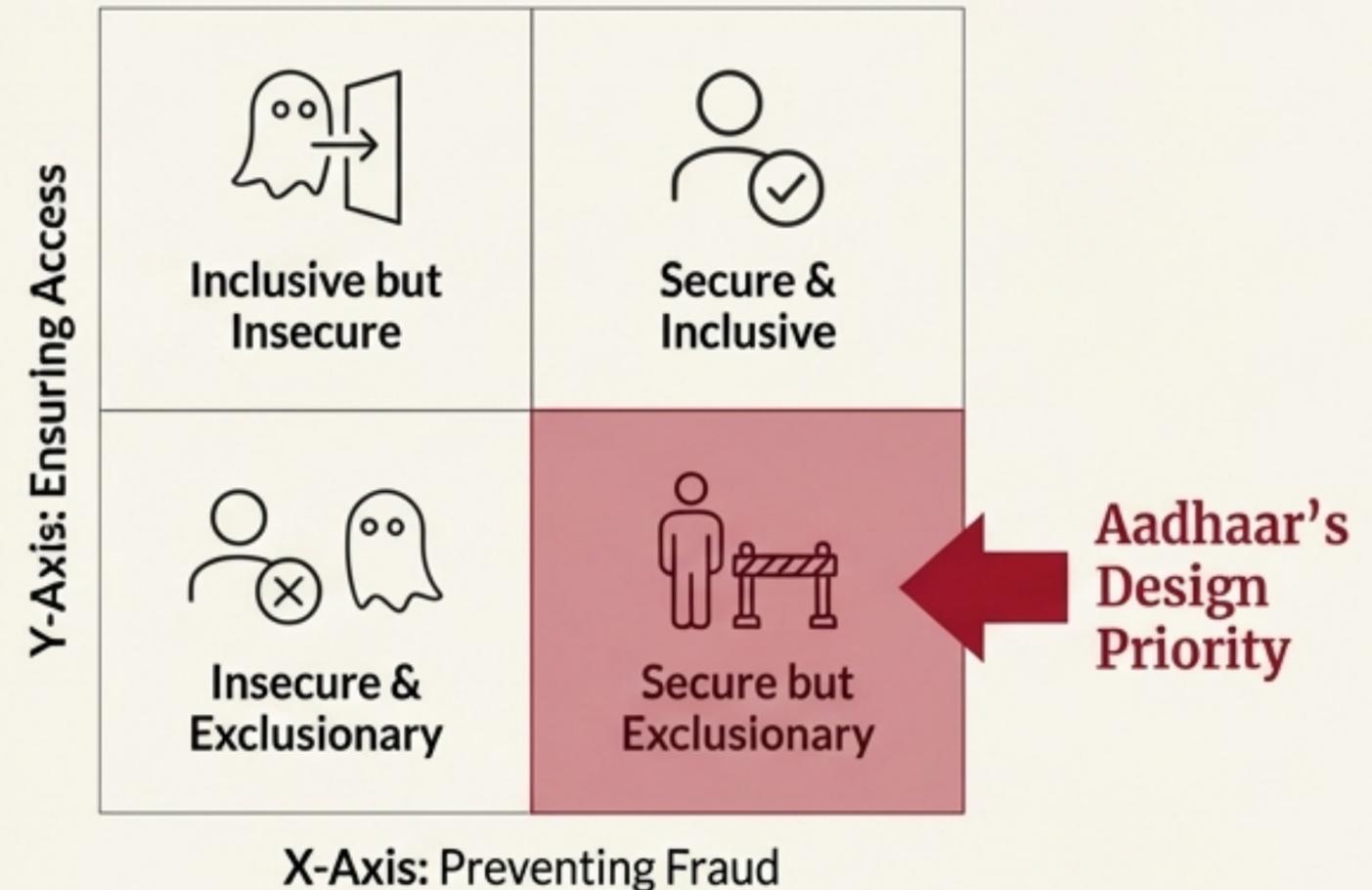
Definition: When the way a problem is formulated biases the outcome.

An authentication system must balance two types of errors:

- **False Positives:** Letting an imposter through (fraud).
- **False Negatives:** Blocking a genuine user (exclusion).

Aadhaar's Bias:

The system was framed primarily to solve the problem of fraud and leakage. It optimised for minimising false positives, even if it meant tolerating a higher rate of false negatives.



The Result: The goal of 'weeding out ghosts' took precedence over the goal of 'ensuring no one is left behind.' The system was aligned to the value of efficiency, but misaligned with the value of inclusivity.

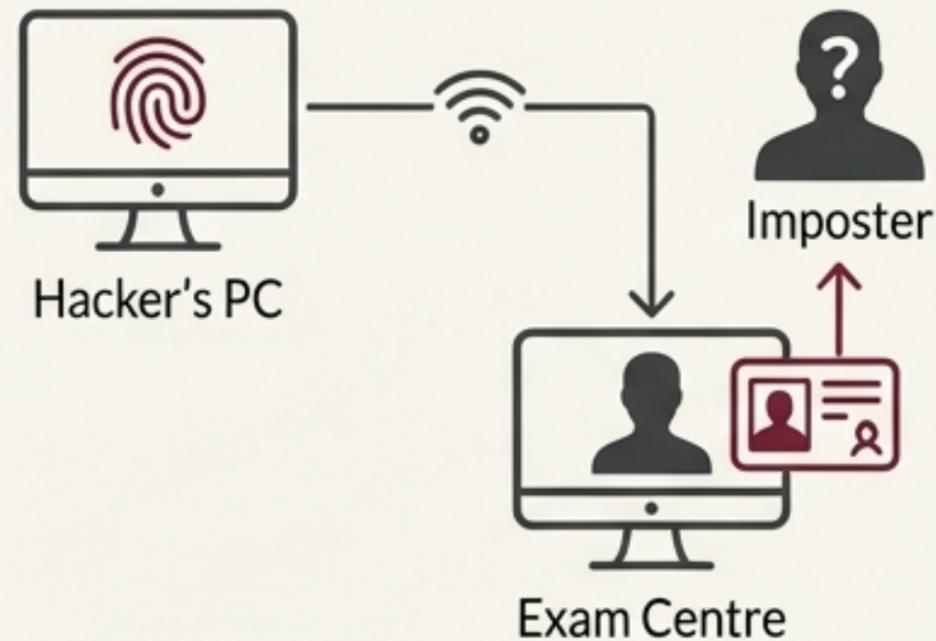
The ultimate irony: a tool to curb corruption becomes a new vector for fraud.

Organised Ration Theft



A CID investigation in Uttar Pradesh uncovered a massive scam where a single Aadhaar card was used to divert rations. Officials and dealers colluded to replace beneficiary data and siphon off food grains.

Sophisticated Exam Cheating



An interstate network in Madhya Pradesh rented Aadhaar centre IDs and cloned biometric data to help unqualified candidates cheat in the Police Constable exam. Imposters were sent to exam centres with altered Aadhaar identities.

Creating Fake Identities



In Jaipur, a fraudster created a counterfeit Aadhaar identity by scanning his toes and using a reverse image of his eye pupils, swindling ₹26 crore from multiple victims.

A prophetic dissent warned that dignity dignity cannot be subject to an algorithm.

Context:

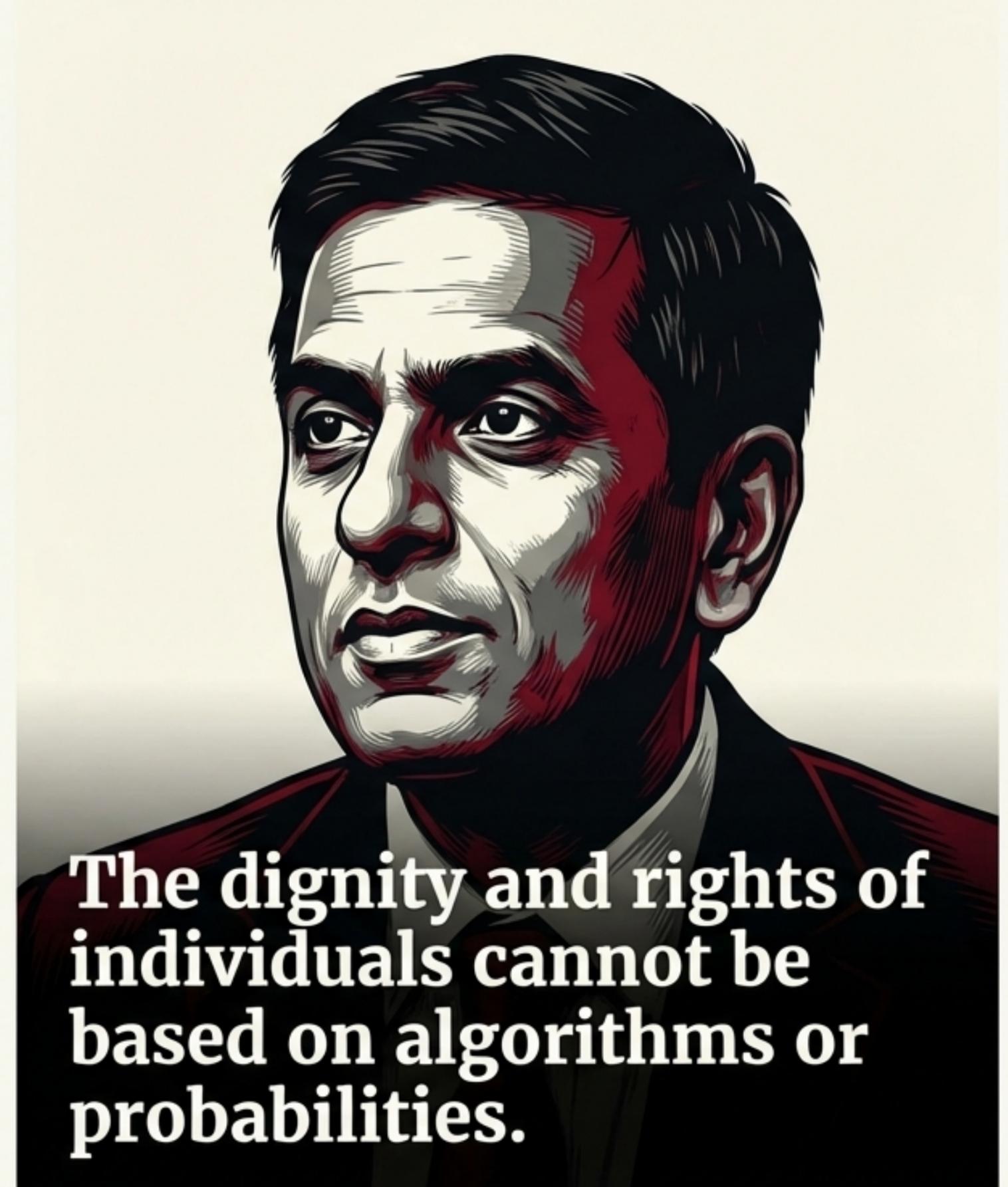
In the 2019 Supreme Court case (*K.S. Puttaswamy v. Union of India*), a 4-1 majority upheld the mandatory use of Aadhaar for welfare. Justice D.Y. Chandrachud was the sole dissenter.

Key Points from his Dissent:

- Held that the entire Aadhaar scheme was “pervasive, exclusionary, and violated the privacy judgment.”
- Warned that making constitutional entitlements dependent on biometric authentication was a violation of fundamental rights.

Legacy:

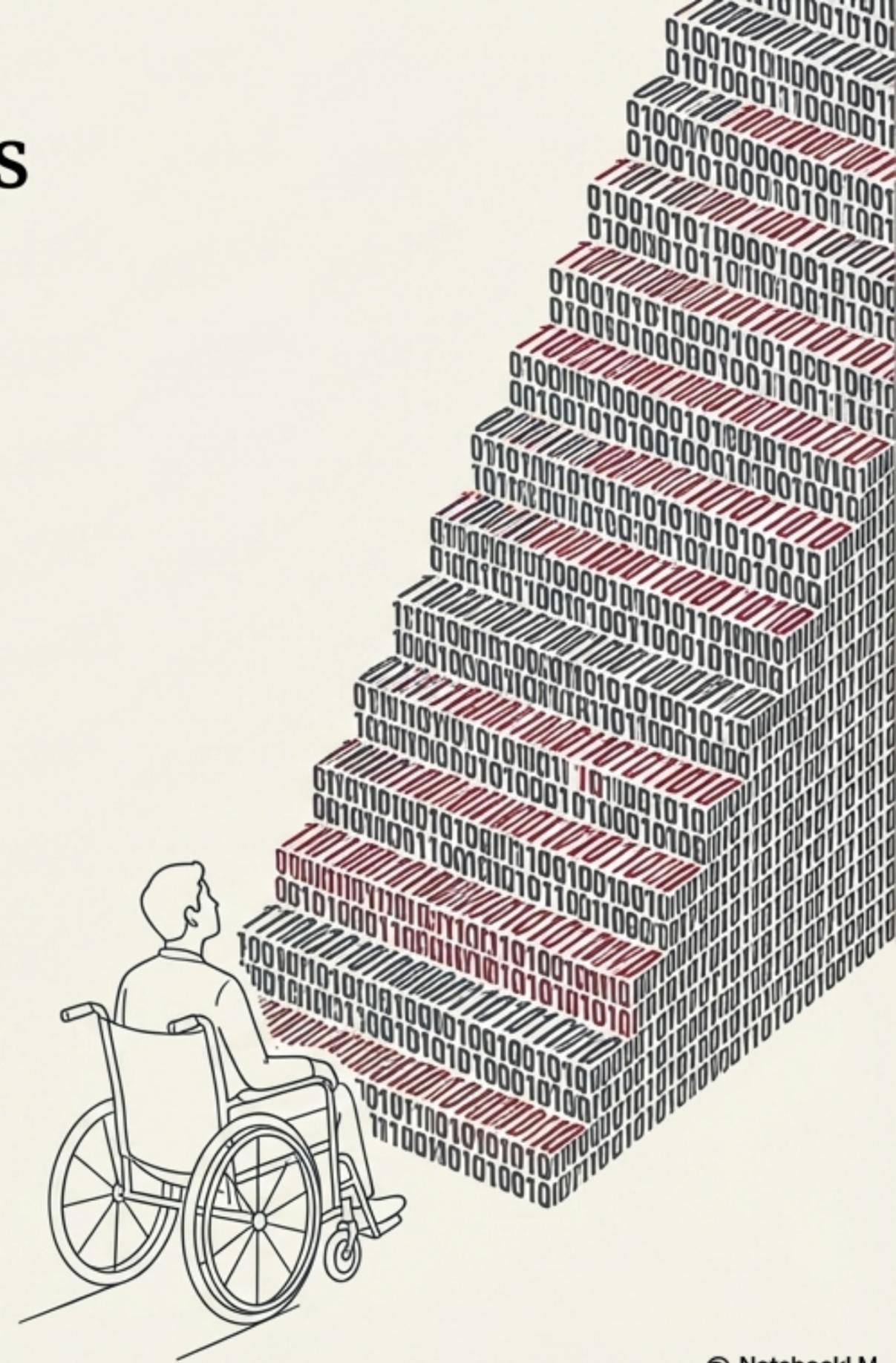
His dissent provided the foundational legal and ethical argument against the coercive nature of the project, an argument now validated by years of on-the-ground evidence.



The dignity and rights of individuals cannot be based on algorithms or probabilities.

The architecture of exclusion extends beyond rations to the very fabric of digital citizenship.

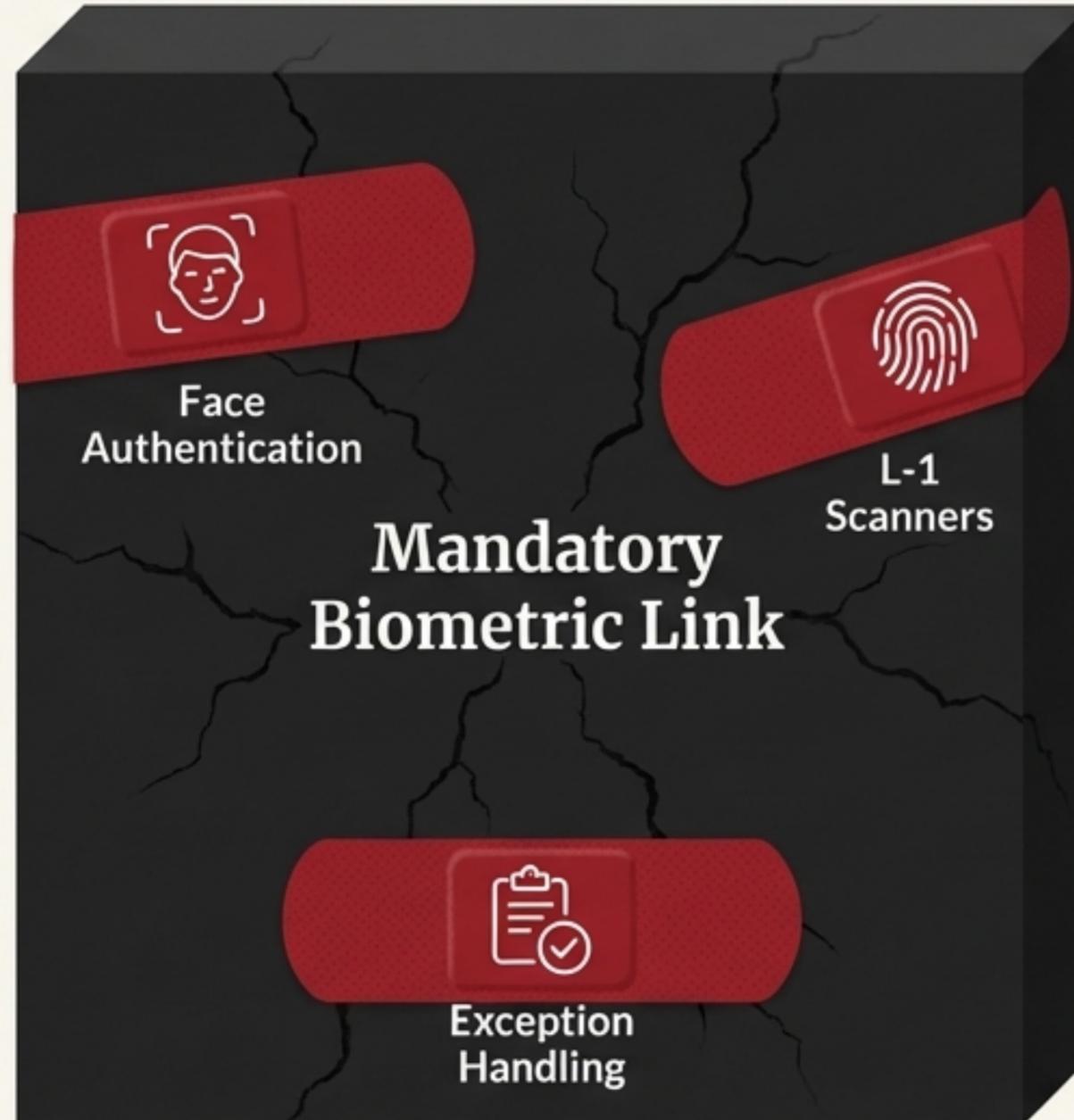
- **Landmark Judgment:** *Pragya Prasun & Ors. v. Union of India* (April 2025).
- **The Problem:** Digital KYC (Know Your Customer) procedures for banking and mobile services were inaccessible to persons with disabilities. Petitioners with visual impairments or facial disfigurements from acid attacks were excluded by requirements like blinking for a live-photo or aligning their face with a template.
- **The Ruling:** The Supreme Court held that these exclusions violated the rights to life, equality, and dignity. It declared a 'fundamental right to inclusive and meaningful digital access.'
- **Broader Implication:** The judgment affirms that digital systems must adapt to human diversity, not the other way around. It treats inaccessibility as a 'system-level failure,' not an individual's problem.



Are technological fixes enough to remedy a flawed foundation?

Corrective Measures Implemented:

- **Face Authentication:** Introduced by UIDAI in 2018 as an additional authentication method.
- **L-1 Scanners:** New devices that authenticate fingerprints only if there is live blood flow.
- **Exception Handling:** Official policies state benefits should be provided via alternate IDs if authentication fails.



The Lingering Question:

While these measures address specific technical failures, they do not change the mandatory, coercive nature of the system. The burden of proof remains on the citizen, and robust, easily accessible non-digital alternatives are still lacking.

Is the state patching the symptoms while ignoring the disease?

The path forward requires a return to first principles: a system built for human dignity, not algorithmic probability.

The experience of Aadhaar demonstrates a critical lesson for digital governance. Efficiency and fraud prevention are valid goals, but they cannot come at the cost of constitutional guarantees. When a system designed for inclusion creates new hierarchies of exclusion—the digitally invisible, the biometrically illegible—it betrays its core purpose. The ultimate measure of a public welfare system is not its technical sophistication, but its unwavering commitment to the last person in line.

The ultimate measure of a public welfare system is not its technical sophistication, but its unwavering commitment to the last person in line.

“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.”

- John Simte, Legal Researcher