



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 AADHAAR TO AI SURVEILLANCE: IS INDIA PREPARED FOR THE NEXT?

-Aradhya Singh

INTRODUCTION

Imagine standing in a queue at your local ration shop, handing over your Aadhaar card to claim subsidies. A simple act that's quietly evolved into something far bigger. Launched over a decade ago as India's answer to identity chaos, Aadhaar has ballooned into the world's largest biometric database, powering everything from bank accounts to welfare payouts. But as we race into AI surveillance facial recognition cameras scanning streets, predictive policing algorithms sifting through our data are we ready for the privacy trade-offs?¹

This blog dives into that journey, unpacking Aadhaar's roots, its fusion with cutting-edge AI and the looming constitutional clashes. From Supreme Court battles to regulatory gaps, we'll explore if India's ready for the next frontier or if it's time to hit pause.

AADHAAR: EFFICIENCY OR SURVEILLANCE?

The Aadhaar project, governed by the Aadhaar Act, 2016, is a digital tug-of-war between administrative efficiency and individual liberty. While the collection of biometric data (fingerprints and iris scans) was designed to prune "ghost beneficiaries" from welfare schemes, it sparked intense "mission creep" controversies.²

The debate peaked over mandatory linking requirements for bank accounts and SIM cards, which critics viewed as a blueprint for state surveillance. The judiciary intervened through two landmark decisions:

¹ Unique Identification Authority of India, *Aadhaar: Digital Identity Infrastructure*, UIDAI, <https://uidai.gov.in>

² The Aadhaar Act, 2016, No. 18, Acts of Parliament, 2016 (India)

1. **JUSTICE K.S. PUTTASWAMY (RETD.) V. UNION OF INDIA (2017):** A nine-judge bench declared the Right to Privacy a fundamental right under Article 21. It established the proportionality principle, mandating that any state intrusion must be legal, necessary, and the least restrictive option.³
2. **AADHAAR JUDGMENT (2018):** The Court upheld Aadhaar for welfare and PAN linking but struck down its mandatory use for bank accounts and SIM cards by private entities.⁴

Aadhaar is a valid tool for targeted subsidies, but the "Right to be Let Alone" remains the constitutional default.⁵

RISE OF SURVEILLANCE TECHNOLOGIES IN INDIA

India is witnessing a rapid expansion of surveillance technologies, transitioning from traditional policing to advanced digital oversight. Central to this shift is Facial Recognition Technology (FRT), notably the National Crime Records Bureau's (NCRB) proposed Automated Facial Recognition System (AFRS), aimed at identifying criminals across national databases.⁶ This is bolstered by massive CCTV expansion under the Smart Cities Mission, integrating public monitoring into urban infrastructure.⁷

The deployment of Drone surveillance has moved beyond border monitoring to active policing during protests, raising concerns regarding assembly rights. Simultaneously, the state utilizes social media tracking tools to monitor online speech, while predictive policing tools attempt to pre-empt crime through algorithmic analysis.⁸

These emerging systems pose significant risks. Without a robust data protection framework, there is high potential for profiling and discrimination against marginalized communities. Algorithmic biases often lead to wrongful targeting, threatening the "Right to be Let Alone" established in *Puttaswamy*.⁹ As surveillance becomes more pervasive, the proportionality of these measures remains a critical constitutional hurdle.

³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India)

⁴ *K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 S.C.C. 1 (India)

⁵ Id

⁶ National Crime Records Bureau, *Automated Facial Recognition System (AFRS) Project*, Ministry of Home Affairs, Government of India

⁷ Ministry of Housing and Urban Affairs, *Smart Cities Mission Guidelines*, Government of India

⁸ Apar Gupta, *Surveillance and Privacy in India: Legal Challenges in the Digital Age*, Internet Freedom Foundation

⁹ *Justice K.S. Puttaswamy (Retd.)*, (2017) 10 S.C.C. 1

AI-POWERED SURVEILLANCE: THE NEXT BIG CONCERN

AI has transformed surveillance from static observation into dynamic, real-time control. By integrating real-time facial recognition with behavioral tracking and crowd monitoring, these systems identify "anomalous" patterns to pre-emptively flag individuals. Predictive policing algorithms and automated risk scoring further attempt to forecast criminal activity, shifting the legal burden from action to intent.¹⁰

Globally, a regulatory schism has emerged:

- The China Model: Extensive state-led integration via "social credit" systems.¹¹
- The U.S. Debate: A patchwork of local bans on police facial recognition in cities like San Francisco.¹²
- The EU AI Act: A rigid framework strictly limiting biometric surveillance in public spaces.¹³

In India, projects like the AFRS are gaining momentum despite the lack of a surveillance-specific statute. Without legislative guardrails, these AI tools risk becoming instruments of automated profiling and discrimination, likely failing the proportionality test mandated by the Supreme Court.¹⁴

CONSTITUTIONAL CHALLENGES & LEGAL FRAMEWORK

India's surveillance expansion faces severe constitutional hurdles. Article 14 is threatened by algorithmic biases that institutionalize discrimination, while Article 19(1)(a) is undermined by a "chilling effect" on free speech. Crucially, under the *Puttaswamy* mandate, mass surveillance often fails the Article 21 proportionality test.¹⁵ Furthermore, a lack of transparency in automated systems denies citizens basic due process.

The current legal landscape is fragmented and outdated. While the DPDP Act, 2023, establishes data standards, its extensive government exemptions leave state power unchecked.¹⁶ Legacy laws like the Telegraph Act, 1885, and IT Act, 2000, along with the IT Rules, 2021, lack the

¹⁰ Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard Univ. Press 2018)

¹¹ Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019)

¹² San Francisco, Cal., Police Code art. 29 (2019)

¹³ Regulation (EU) 2024/1689, Artificial Intelligence Act

¹⁴ *Justice K.S. Puttaswamy (Retd.)*, (2017) 10 S.C.C. 1

¹⁵ Constitution of India arts. 14, 19, 21; *Puttaswamy*, (2017) 10 S.C.C. 1

¹⁶ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India)

precision needed for the AI era.¹⁷ Without a unified, rights-based law, pervasive monitoring risks eroding democratic accountability.

ETHICAL CONCERNS

The integration of AI into state oversight introduces profound ethical challenges that test the limits of constitutional safeguards:

- **Bias and Discrimination:** AI systems often inherit the prejudices of their training data, leading to algorithmic bias that results in the minority targeting of vulnerable communities.¹⁸
- **Informed Consent:** Surveillance is frequently deployed in public spaces without informed consent, depriving individuals of their agency and the "right to be let alone."¹⁹
- **Profiling and Function Creep:** Mass profiling transforms citizens into data points. Furthermore, function creep—where data collected for one purpose (e.g., subsidies) is used for another (e.g., policing)—erodes public trust.²⁰
- **Security Risks:** Centralized biometric and behavioral databases are high-value targets. Frequent data breaches risk permanent identity compromise, as biometrics cannot be reset like passwords.²¹

These ethical failures suggest that technological "efficiency" often comes at the cost of human dignity and systemic fairness.

COMPARATIVE PERSPECTIVE

Global regulatory approaches to surveillance are divided into three distinct models:

- **European Union (Rights-Centric):** The EU AI Act employs a "risk-based" strategy, banning high-risk systems like social scoring and strictly limiting real-time biometric tracking in public.²²

¹⁷ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); Indian Telegraph Act, 1885

¹⁸ UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021)

¹⁹ *Puttaswamy*, (2017) 10 S.C.C. 1.

²⁰ Daniel J. Solove, *Understanding Privacy* (Harvard Univ. Press 2008)

²¹ Digital Personal Data Protection Act, 2023.

²² Regulation (EU) 2024/1689, Artificial Intelligence Act

- United States (Fragmented): Lacking federal privacy legislation, the U.S. relies on a patchwork of state laws and local bans on facial recognition in cities like San Francisco to check police power.²³
- China (State-Centric): This model integrates AI into governance via the "Social Credit System," using mass surveillance as a tool for proactive social engineering.²⁴

The Indian Dilemma: India remains at a crossroads. While the *Puttaswamy* ruling aligns with the EU's rights-centric values, broad government exemptions in recent laws suggest a drift toward the Chinese model's pervasive oversight.²⁵ Without a unified framework, India risks deploying advanced technology without the necessary democratic safeguards.

THE WAY FORWARD

To secure constitutional liberties, India must transition to an accountable oversight model. Essential reforms include establishing an independent oversight authority, requiring judicial authorization for interceptions, and mandating algorithm audits to eliminate bias. Furthermore, narrowing DPDP Act exemptions and publishing transparency reports will ensure state power remains proportionate and publicly accountable.²⁶

CONCLUSION

The evolution of India's digital landscape presents a stark paradox. While the state aims for administrative precision, the lack of a comprehensive regulatory framework for emerging technologies threatens to transform a tool for empowerment into a mechanism for pervasive oversight. Aadhaar promised inclusion through digital identity. But if India moves toward AI-powered surveillance without robust safeguards, could convenience come at the cost of constitutional freedoms?²⁷

²³ Kashmir Hill, *Your Face Belongs to Us* (W.W. Norton 2023)

²⁴ Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019)

²⁵ *Puttaswamy*, (2017) 10 S.C.C. 1.

²⁶ Digital Personal Data Protection Act, 2023; Information Technology Rules, 2021.

²⁷ Constitution of India arts. 14, 19, 21.