Virtual Bharat: The Sociological Impact of E-Governance, Aadhaar, and Digital Surveillance

Nikhil Srivastava[1], Shweta Sachan[2], Abhinav Kumar[3]
[1]*Personal Assistant, ANDUAT, Kumarganj, Ayodhya*
[2]*Assistant Professor, CoCS, ANDUAT, Kumarganj, Ayodhya*
[3]*Assistant Professor, CoA, ANDUAT, Kumarganj, Ayodhya*

Abstract- **India's digital revolution, championed by transformative policies like Digital India and instruments like Aadhaar, has restructured citizen–state relationships in ways both empowering and precarious. The promise of inclusion, efficiency, and transparency has often clashed with the lived realities of exclusion, surveillance, and digital marginalization. This paper reviews the sociological ramifications of e-governance and digital surveillance in India, critically examining the implications of Aadhaar, UPI, FRT (Facial Recognition Technology), and related platforms. Drawing on empirical data, government reports, academic literature, and theoretical perspectives—especially those of Foucault, Scott, and Latour—this paper explores the dual nature of technology as both liberating and oppressive in the Indian sociopolitical context. The paper ends with policy recommendations to align digital governance with constitutional ideals of justice and equality.**

Index Terms- **Digital India, Aadhaar, Surveillance, Sociology, Digital Exclusion, Data Justice, Foucault, UPI, FRT**

I. INTRODUCTION

India's digital architecture has seen a rapid transformation in the last decade, with initiatives like the Aadhaar program, JAM trinity (Jan Dhan–Aadhaar–Mobile), Digital India, and the proliferation of platforms like Digi Locker, BHIM, and UMANG. These innovations, while designed to enhance efficiency and bridge access gaps, often reinforce pre-existing social inequalities.

According to UIDAI (2023), over 1.3 billion Indians are enrolled in Aadhaar, making it the largest biometric database globally. Simultaneously, the proliferation of surveillance technologies, such as facial recognition, has raised alarm about privacy, autonomy, and democratic rights. This paper argues that India's digital trajectory, while progressive on the surface, is deeply embedded in structures of surveillance capitalism, digital exclusion, and algorithmic governance.

II. THEORETICAL FRAMEWORK

This analysis is grounded in several sociological frameworks:

1. Michel Foucault's concept of Biopower and Panopticons explains how surveillance technologies like Aadhaar and CCTV turn citizens into data subjects, governed by unseen yet omnipresent mechanisms of control.
2. James C. Scott's idea of "legibility" posits that states simplify complex social realities to make populations easier to manage, a process mirrored in the digitization of welfare and identity.
3. Langdon Winner's theory of technological politics reminds us that technologies are not neutral—they encode values, privileges, and institutional biases.

III. AADHAAR: THE BIOMETRIC BACKBONE OF THE STATE

While Aadhaar was introduced to facilitate welfare distribution and curb leakages, studies reveal a darker side:

1. Jean Drèze and Reetika Khera's 2019 study in Jharkhand found that 12% of ration beneficiaries were denied food due to biometric mismatches. These errors disproportionately affect the elderly, tribal communities, and the disabled.
2. Aadhaar has become a gatekeeping tool, making access to PDS, pensions, and MGNREGA wages contingent on biometric authentication—even in areas with poor connectivity.

3. The absence of robust grievance redressal has made it hard for the excluded to re-enter the system.

IV. DIGITAL GOVERNANCE AND PROCEDURAL EXCLUSION

Government portals like e-gram swaraj, UMANG, and Digi Locker aim to streamline citizen services. However:

1. Only 33% of rural women have access to the internet (NFHS-5, 2021–22), limiting their ability to engage with digital services.
2. Digitally illiterate citizens often become dependent on intermediaries, leading to potential exploitation.
3. Procedural opacity—e.g., auto-rejection of applications due to software bugs—alienates the digitally vulnerable.

V. SURVEILLANCE INFRASTRUCTURE: CITIES OF CONTROL

India is rapidly embracing surveillance technologies under the guise of "smart governance":

1. Over 152 cities have adopted Facial Recognition Technology (Compatriotic, 2023).
2. Programs like CCTNS (Crime and Criminal Tracking Network System) and NATGRID centralize and analyse citizens' data without adequate oversight.
3. The Data Protection Act (2023) exempts government agencies from key provisions, raising concerns about unchecked surveillance.

This infrastructure disproportionately targets certain populations—e.g., minorities during protests—leading to what scholars' term function creep.

VI. FINANCIAL INCLUSION OR ALGORITHMIC EXPLOITATION?

The rise of digital payment platforms like UPI has been remarkable:

- Over 10 billion UPI transactions occurred in May 2023 (NPCI).
- Yet, 190 million Indians remain unbanked (World Bank Findex, 2022), especially women and rural populations.
- Gig workers (estimated at 7.7 million by NITI Aayog) remain excluded from formal protections despite being digitally visible.

Fintech platforms often algorithmically nudge users toward loans, credit scoring, and risk profiling—raising issues around digital predation.

VII. INTERNET SHUTDOWNS: GOVERNANCE BY BLACKOUT

India leads the world in internet shutdowns:

- 84 shutdowns were recorded in 2022 (Access Now).
- These affect students, telemedicine users, traders, and even emergency services—especially in Kashmir, Rajasthan, and North-East states.

Shutdowns reflect a paradox: the same state promoting digital governance restricts access to it when dissent arises.

VIII. CASTE, GENDER, AND THE DIGITAL DIVIDE

Digital platforms reproduce real-world inequities:

1. Dalit and Adivasi communities face infrastructural, linguistic, and cultural barriers to accessing digital services.
2. Women, especially in rural and conservative households, experience gendered surveillance—family control over device use.
3. The lack of regional language support and inclusive design further alienates marginalized groups.

IX. CONSENT, DATA SOVEREIGNTY, AND THE RIGHT TO BE FORGOTTEN

The principle of informed digital consent remains underdeveloped in the Indian context. Despite the growing digitalization of state–citizen interactions, users often engage with platforms like Aadhaar without a comprehensive understanding of the implications of data sharing. Aadhaar enrolment, in many instances, has been conducted without adequately communicating its long-term consequences, particularly among marginalized communities.

The recently enacted *Digital Personal Data Protection (DPDP) Act, 2023* marks a significant step toward data regulation; however, it has been critiqued for lacking robust mechanisms to ensure meaningful user consent, effective grievance redressal, and enforceable rights to data deletion. The Act does not mandate strong accountability structures for state or corporate actors handling sensitive personal data.

Additionally, citizen data is increasingly commodified—monetized for commercial gain, used for algorithmic profiling, or repurposed for political microtargeting. These practices challenge the foundational principles of data sovereignty and the individual's autonomy over their digital identity. The absence of a strong “right to be forgotten” further exacerbates the risk of perpetual digital surveillance and social profiling, raising serious ethical and constitutional concerns.

The idea of informed digital consent remains weak in India:

1. Aadhaar enrolment often occurs without clear understanding.
2. The DPDP Act (2023) lacks strong protections for user consent, grievance redressal, and data deletion rights.
3. Citizen data is increasingly being monetized, algorithmically profiled, or used for political microtargeting.

X. PICTOGRAPHIC SUMMARY OF KEY INDICATORS

Indicator	Stat	Source
Aadhaar Coverage	1.3 billion+ individuals	UIDAI (2023)
Rural Women with Internet Access	33%	NFHS-5 (2021–22)
Facial Recognition Cities	152+ cities	compatriotic (2023)
Aadhaar PDS Exclusion (Jharkhand)	12% denial rate	Jean Drèze Study (2019)
UPI Transactions (May 2023)	10+ billion	NPCI (2023)
Internet Shutdowns (2022)	84	Access Now (2022)
Gig Workers in India	7.7 million	NITI Aayog Report (2022)
Unbanked Adults	190 million	World Bank Findex (2022)
Data Protection Legislation	Enacted, with state exemption	DPDP Act (2023)

XI. GOVERNMENT INTERVENTIONS AND THE NEED FOR INCLUSIVE DIGITAL JUSTICE

India has made significant progress in digitizing governance, but this transformation has not been without challenges. Several flagship initiatives—such as the Digital India Mission, the Data Protection Act, and e-SHRAM—highlight both the promise and pitfalls of digital governance.

1. Digital Personal Data Protection Act (2023): This Act marks India's first formal legal framework to safeguard individual data. While it establishes mechanisms for user consent and data fiduciaries, critics highlight that exemptions granted to state agencies compromise privacy, especially in the absence of independent oversight.
2. Expansion of the Aadhaar Ecosystem: Mandatory Aadhaar linkage for welfare schemes has improved targeting in many cases, but studies like those conducted in Jharkhand reveal how biometric mismatches and authentication failures have led to 12% ration denials—especially among the elderly and tribal populations.
3. National Digital Health Mission (NDHM): Introduced under Ayushman Bharat, this mission digitizes health records linked to Aadhaar. However, the lack of strong data consent frameworks risks compromising sensitive health data, particularly among marginalized groups.
4. PM-WANI and Bharat Net Initiatives: These programs aim to increase last-mile connectivity through public Wi-Fi and optical fiber in villages. However, their slow rollout and underutilization in states like Bihar and Uttar Pradesh indicate persistent regional disparities.
5. Digital Payment Ecosystem via UPI: With more than 10 billion transactions in May 2023, UPI has revolutionized cashless commerce. Yet, over 190 million unbanked adults, predominantly from rural and low-literacy backgrounds, remain excluded from this growth story.

6. Kerala's 'Right to Internet' Model: Declaring internet access a human right, Kerala is pioneering a bottom-up approach to digital empowerment. This can be replicated nationwide with state subsidies and public-private partnerships.

XII. POLICY RECOMMENDATIONS FOR AN INCLUSIVE VIRTUAL BHARAT:

1. Localized Grievance Redressal Systems: Every Aadhaar-linked public service should have a physical and human fallback system. Biometric mismatch must never lead to exclusion from entitlements.
2. Digital Literacy Drives for Women and Marginalized Groups: Tailored training programs must be introduced under the Skill India Mission. Community digital ambassadors could help bridge the gender divide in internet usage (currently at 33% among rural women, NFHS-5).
3. Independent Data Oversight Mechanism: Establish a constitutional body to regulate surveillance, data privacy, and digital rights. Parliamentary scrutiny must be mandatory for state-wide use of facial recognition systems.
4. Algorithmic Accountability in the Gig Economy: Platform workers—numbering 7.7 million—must be protected from algorithmic wage discrimination and integrated into schemes like PM-SYM and Ayushman Bharat using e-SHRAM.
5. Transparent Internet Shutdown Protocols: Judicial authorization and post-event reporting should be made compulsory. India's 84 shutdowns in 2022 were the highest globally, impacting civil liberties and education.
6. Digital Infrastructure in Regional Languages: All e-governance portals must be accessible in local dialects, with speech and visual support for differently-abled citizens. Only then can we truly democratize access.

XIII. CONCLUSION

Virtual Bharat is not separate from real Bharat; it reflects and often intensifies the fractures of caste, class, gender, and geography. While digital governance in India has the potential to democratize service delivery, unchecked digitization can erode constitutional rights. As India moves towards becoming a "Digital Republic," it must choose between surveillance and empowerment, exclusion and inclusion, opacity and accountability. Technology must remain a servant to the people, not a silent weapon of control.

REFERENCES

[1]. UIDAI. (2023). *Aadhaar Dashboard*. https://uidai.gov.in

[2]. NFHS-5. (2021–22). *National Family Health Survey*. Ministry of Health & Family Welfare.

[3]. Comparitech. (2023). *Facial Recognition Cities Index*.

[4]. Jean Drèze & Reetika Khera. (2019). *Aadhaar and Food Security*. Economic & Political Weekly.

[5]. NPCI. (2023). *Unified Payments Interface (UPI) Statistics*. https://www.npci.org.in

[6]. AccessNow. (2022). *Internet Shutdowns in India*.

[7]. NITI Aayog. (2022). *India's Booming Gig and Platform Economy*.

[8]. World Bank. (2022). *Findex Database: Global Financial Inclusion*.

[9]. Government of India. (2023). *Digital Personal Data Protection Act*. Ministry of Electronics & IT.

[10]. Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Vintage Books.

[11]. James C. Scott. *Seeing Like a State*. Yale University Press.

[12]. Langdon Winner. *Do Artifacts Have Politics?*. Daedalus.