KeAi
CHINESE ROOTS
GLOBAL IMPACT

Journal of Digital Economy

DIGITAL SURVEILLANCE AND THE ETHICS OF WELFARE ADMINISTRATION: LESSONS FROM INDIA'S AADHAAR-ENABLED STATE

Lt. Dr. Kongala Sukumar
Associate Professor of Public Administration
Dr. MCRHRD Institute of Telangana, Hyderabad.

Abstract

The Aadhaar biometric identification system in India is a contentious case study and a cross-section of digital surveillance, welfare management, and ethical governance, which is examined in this paper. Introduced in 2010, Aadhaar is now the largest biometric identification system in the world, with more than 1.3 billion citizens covered, and has radically changed the welfare delivery system structure in India. With the help of the analysis of empirical data, policy documents, and field studies, this study demonstrates a paradoxical system in which financial inclusion is encouraged. However, at the same time, new versions of digital exclusion are developed. This research concludes that failure rates to authenticate between 13 and 49 percent in various states have led to systematic denial of welfare benefits to the vulnerable groups, especially the elderly, women, and marginalized communities. The paper records how the shift to compulsory linking of access to basic services has established a surveillance infrastructure that has gone beyond the application of welfare service delivery to the utilization of surveillance in the private sector. The recent trends in 2025 that enable the infrastructure of Aadhaar to be accessed by private entities represent important issues of behavioral data mining, as well as the breach of privacy. The results indicate that even though Aadhaar has attained high levels of enrollment coverage (93% of the populace), its practice presents underlying conflicts between techno-efficient solutions and rights-based welfare delivery. The paper has concluded that the transformation of Aadhaar as a welfare instrument into a full-fledged surveillance machine provides important lessons to any digital identity implementation in the world and states that solid data protection policies, accountability provisions, and alternative authentication solutions to lock vulnerable groups out of essential services can help avoid the marginalization of vulnerable groups.

Keywords: biometric identification, digital surveillance, Aadhaar, welfare administration, social exclusion, privacy, India, digital identity.

Introduction

The introduction of digital technologies in the public administration has completely altered the relations between a state and its citizens, especially in the sphere of welfare provision. The Aadhaar system in India, introduced in 2010, is one of the most ambitious attempts at digitizing the welfare administration system with the use of biometric identification. Although it enrolls its residents, roughly 1.3 billion as of 2023, Aadhaar has been transformed since it began as a voluntary identification system to enhance the delivery of welfare. This new system is now a quasi-mandatory infrastructure layer mediating access to basic services, financial systems, and, increasingly, transactions in the private sector (Sadhya & Sahu, 2024).

ISSN:2773-0670

The name of the Aadhaar project, which translates to foundation or support in some of the languages used in India, was developed to address the endemic issues in the welfare system of India, such as corruption and leaks, as well as failure to provide services to undocumented residents of India. The system gives an identification number to every resident that is a unique 12-digit number that is associated with the biometric data of the person (fingerprints, iris scan, and a face photo) and their demographic data. This biometric database was seen as a process through which welfare benefits are more likely to go to the right people, even as those who have duplicated and defrauded the system will be weeded out.

Nevertheless, the adoption and spread of Aadhaar have cast deep concerns on the ethicality of digital surveillance as an instrument of welfare management. The development of the system is indicative of the larger global tendencies towards what scholars have described as the "regulatory state," whereby governance is being driven by technological systems of surveillance and regulation, rather than by direct service delivery or through forceful power (Walby, 1999). The change has specific consequences for developing nations, where digital identification systems are frequently advanced as a means to overcome the lack of capacity in states and may lead to the emergence of new exclusion and vulnerability.

The importance of research on Aadhaar has a bigger scope than India. With governments all over the world becoming more digitally inclined in their welfare administration benefits, the experience of India provides some of the most important insights into both the benefits and dangers of biometric governance. Aadhaar has received acclaim from the World Bank as the most advanced ID programme in the world, and India has been actively encouraging other countries to adopt similar systems through its Digital Public Infrastructure programmes. The ethical considerations and practical implications of Aadhaar are hence needed to inform international discourses regarding digital identity, surveillance, and social protection.

Literature Review

Theoretical Frameworks of Digital Surveillance and Welfare

Surveillance and welfare provision have a long history, not to mention that digital technologies have dramatically changed this order of things. The concept of governmentality by Foucault is a helpful model of approaching the way Aadhaar is a technology of governmentality that influences both the state power and the subjectivity of the citizens (Jacobsen, 2012). The system does not just work by direct coercion, but rather by creating what Rao and Nair (2019) refer to as a metonymy that goes beyond its literal context, which will automatically connect citizens to a holistic identification infrastructure.

More recent literature has paid even more attention to how digital identification systems establish novel kinds of "dataveillance" that are qualitatively different than the old surveillance systems. According to Masieri and Shakthi (2019), Aadhaar is a so-called datafier, which means that people are transformed into machine-readable data, and automated decision-making is carried out regarding the eligibility of benefits and access to services. This datafication process essentially changes the very essence of citizenship and the right to welfare, as it is made dependent on the successful authentication in the digital systems.

Digital Identity as a Post-Colonial Practice

A number of researchers have explored Aadhaar using post-colonial theoretical frameworks, and they have shown that the system replicates and strengthens previous categorization and control patterns. As Nair (2018) shows, Aadhaar unveils the instability of the social identities

ISSN:2773-0670

that the technology is designed to control and generate alternative methods of identity control, which are especially impactful on marginalized communities. It has been critiqued that the system focuses on biometric authentication as the main way of defining identity and assumes that identity functions in rather simplistic social and cultural environments in India.

The post-colonial analysis gains further relevance when it comes to discussing how Aadhaar has changed from a tool of inclusion to what critics term an instrument of exclusion. The strict parameters and technicalities of the system offer what Bhabha could call a hybrid space wherein citizens have to always balance their embodied and digitalized selves, with failure in doing so leading to their denial of critical services.

Privacy, Data Protection and Human Rights

Aadhaar has faced widespread debates in legal circles and academic literature with regard to its privacy implications. The 2017 Supreme Court ruling that privacy is a fundamental right was a watershed moment in the way data protection is viewed in India. However, the 2018 follow-up decision in support of the constitutionality of Aadhaar unveiled the contradictions between the protection of individual privacy and the goals of collective welfare (Sadhya and Sahu, 2024).

Comparisons between India and other parts of the world have found that India is operating very differently with regard to the biometric identification systems used in Europe and the United States, especially in data protection and consent. Unlike the European Union's General Data Protection Regulation (GDPR) framework, which emphasizes explicit consent and data minimization, Aadhaar's architecture enables extensive data sharing across government departments and, increasingly, with private sector entities (Huynh, 2025).

Methodology

This research employs a mixed-methods approach combining quantitative analysis of authentication data, policy document analysis, and synthesis of field studies conducted across multiple Indian states. The analysis draws on:

1. **Official Statistics**: Government data on Aadhaar enrollment, authentication rates, and welfare delivery outcomes from 2010-2024, obtained from the Unique Identification Authority of India (UIDAI), the Ministry of Electronics and Information Technology, and various state governments.
2. **Academic Studies:** Academic papers on digital governance and development studies published in the last 5 years (2012-2025) that have been found as a result of systematic searches on Google Scholar, Web of Science, and selected databases.
3. **Field Reports:** Reporting by civil society bodies, including the case studies of exclusion and authentication failures, which are gathered by the researchers and activists who work directly with the affected communities.
4. **Legal Contents:** The Supreme Court decisions, governmental announcements, and regulations on the use and implementation of Aadhaar.
5. **Media Reports:** The current news text reports on the implementation issues, security failures, and experiences of citizens with the system.

The critical interpretive approach is utilized in the analysis as it focuses on the objectives and official metrics of the Aadhaar system, as well as its unintended consequences and impacts on different groups of the population. Special consideration is given to the problem of exclusion,

ISSN:2773-0670

failure to authenticate, and broadening surveillance functions beyond the welfare-oriented scope of the system.

Results and Analysis

Aadhaar Implementation Scale and coverage.

The Aadhaar system has attained great magnitude in regard to enrollment, and there are great implications for the inclusion and the surveillance capacity. Table 1 shows the trend of Aadhaar enrollment and integration into the welfare programs.

Table 1: Aadhaar Enrollment and Coverage Statistics (2011-2023)

Year	Total Enrollments (millions)	Population Coverage (%)	Welfare Schemes Linked	Authentication Transactions (billions)
2011	10	0.8	0	-
2014	600	48.0	15	0.1
2017	1,123	87.3	189	8.8
2020	1,257	92.1	312	53.7
2023	1,380	93.4	325	150.0

Source: Unique Identification Authority of India (2023); Ministry of Electronics and Information Technology (2024)

The data reveals that Aadhaar has achieved near-universal coverage of India's adult population, with 93.4% enrollment as of 2023. However, this aggregate figure masks significant variations in actual accessibility and usage. The exponential growth in authentication transactions—from 100 million in 2014 to 150 billion in 2023—indicates the system's deep integration into daily life, extending far beyond its original welfare delivery mandate.

Authentication Failures and Exclusion Patterns

Despite high enrollment rates, authentication failures represent a critical challenge in Aadhaar-enabled welfare delivery. Analysis of authentication data reveals systematic patterns of exclusion that disproportionately affect vulnerable populations.

Table 2: Authentication Failure Rates by State and Context (2018-2024)

State/Region	Failure Rate (%)	Primary Affected Groups	Main Causes
Jharkhand	49	Tribal populations, elderly	Poor connectivity, worn fingerprints
Rajasthan	37	Rural women, agricultural workers	Biometric changes, technical errors
Kerala	9-45*	Elderly pensioners	Age-related biometric degradation
Andhra Pradesh	22	Rural populations	Network issues, seeding errors
National Average	13-66**	Elderly manual laborers	Multiple factors

ISSN:2773-0670

*9% complete denial, 45% faced at least one failure **13% final failure rate after multiple attempts, 66% initial failure rate *Source: State government reports; Bansal (2018); Yadav (2024)*

The data reveals that while UIDAI reports a 13% authentication failure rate, this figure represents only final failures after multiple attempts. Field studies indicate that initial failure rates can reach 66%, forcing beneficiaries to make multiple trips to access their entitlements. This discrepancy between official statistics and ground reality highlights the hidden costs of digital authentication systems.

Gendered Dimensions of Digital Exclusion

Aadhaar implementation has demonstrated that there are gross gender gaps in the attainment of welfare benefits. The women have specific difficulties in using the digital infrastructure on which they have to be authenticated.

Table 3: Gender-Differentiated Impacts of Aadhaar Implementation

Dimension	Impact on Women	Statistical Evidence
Mobile Phone Access	Lower ownership rates affect authentication	37% of women vs. 71% of men own phones
Digital Literacy	Limited ability to navigate systems	29% of women vs. 47% of men are digitally literate
Biometric Degradation	Higher rates due to manual labor	67% of women agricultural workers report issues
Documentation Gaps	Name mismatches after marriage	23% face seeding errors
Autonomy in Access	Dependence on male relatives	45% require assistance for authentication

Source: IT for Change (2023); National Family Health Survey-5 (2021)

These gendered impacts reveal how seemingly neutral technological systems can reproduce and amplify existing social inequalities. The necessity of a mobile phone connection, e.g., cannot include many women, as they do not have independent access to mobile devices or cannot buy frequent recharges.

Welfare Tool to Surveillance Infrastructure

The growth of Aadhaar in more than just welfare provision is a major change in its role and purpose. This evolution and its implications for surveillance are recorded in Table 4.

Table 4: Expansion of Aadhaar Applications (2010-2025)

Period	Primary Applications	Surveillance Capabilities	Privacy Safeguards
2010-2013	Voluntary ID, limited welfare pilots	Basic identity verification	Minimal regulation
2014-2016	Subsidy delivery (LPG, MGNREGA)	Transaction tracking	Administrative guidelines
2017-2018	Mandatory linking (banking, telecom)	Cross-database integration	Supreme Court intervention

ISSN:2773-0670

2019-2023	Comprehensive welfare integration	Behavioral pattern analysis	Aadhaar Act provisions
2024-2025	Private sector access	AI-enabled profiling	Pending data protection law

Source: UIDAI notifications; Supreme Court judgments; Huynh (2025)

The table presents an obvious roadmap between the desired welfare usage and an all-encompassing surveillance system. A particularly important advancement is the 2025 move to make the authentication services of Aadhaar available to the private companies, which made it possible to extract the behavioral data on a scale never observed before.

Economic and Administrative Outcomes

Advocates of Aadhaar point out its contribution to curbing corruption and improving the delivery of welfare. According to government statistics, the removal of duplicate beneficiaries and leakage will save much money.

Table 5: Reported Economic Impact of Aadhaar Implementation

Metric	Pre-Aadhaar	Post-Aadhaar	Change
Duplicate Beneficiaries (millions)	44.5	4.7	-89.4%
Annual Savings (billion INR)	-	900	-
Direct Benefit Transfer Volume (billion INR)	740 (2013)	6,200 (2023)	+738%
Transaction Cost per Transfer (INR)	125	22	-82.4%
Beneficiary Complaints (%)	34	47	+38.2%

Source: Ministry of Finance (2024); CAG Report (2023)

Nevertheless, the benefits in efficiency should be contrasted with the expenses of being locked out. Critics believe the so-called savings by the government are, in fact, a denial of benefits to legitimate beneficiaries who cannot pass the authentication tests, and not the eradication of fraud. The rise in complaints by beneficiaries, even with the better metrics, is an indication of continued challenges with implementation.

Discussion

The Paradox of Inclusion Through Exclusion

The Aadhaar system is a paradox that is inherent in the modern welfare management system: a technology intended to achieve inclusiveness has become the system of exclusion of the most vulnerable members of society. This paradox indicates more profound contradictions in technocratic methods of social policy, in the fact that pursuing efficiency and fraud prevention may compromise the very essence of welfare provision, i.e., basic social protection of the entire population.

The rates of authentication failure recorded in this research demonstrate that technical solutions are inadequate to deal with the social reality of poverty and marginalization, which is complex. Elderly citizens whose fingerprints have deteriorated over the decades of manual labor, women without personal access to mobile phones, and rural inhabitants of locations with a weak internet connection are all subjected to systematic disadvantages in accessing their legal rights using Aadhaar-enabled systems. Such exceptions are not just the technical bugs but include the decisions on the design level, which select one or the other of the forms of legibility and authentication.

ISSN:2773-0670

The 2018 ruling by the Supreme Court that recognizes these exclusions and reinstates the constitutional validity of the Aadhaar card demonstrates that it is not easy to maintain a balance between collective welfare goals and the rights of an individual. The rationale of the court that the system cannot be crucified on the untested plea of exclusion when it has a much greater end actually places the utilitarian efficiency in a position of priority over the rights of the people who go outside the system. This judicial legitimization has helped the further growth of Aadhaar, even with reported cases of systematic exclusion.

From Welfare Delivery to Surveillance Capitalism

This development of Aadhaar as a form of welfare delivery system to a form of all-inclusive surveillance infrastructure has brought up some very important concerns regarding the nature of the relationship between social protection and state power. The recent introduction of Aadhaar to applications by the private sector is considered a qualitative change of what Zuboff (2019) describes as a form of surveillance capitalism to a hybrid form in which the state infrastructure facilitates the extraction of behavioral information by the private sector.

This has been achieved by the mission creep process, wherein the exceptional measures used to justify welfare delivery have become the norm and have been extended into other arenas. What was originally a system of biometric authentication to receive subsidies has transformed into a system that can track financial transactions, communication, patterns of movement, and, over time, into a behavioral analytics system based on AI-enabled processing. Facial recognition technology combined with the creation of real-time authentication dashboards presents features of population monitoring that are way beyond the mandate of the system.

Such surveillance infrastructure has very worrying implications in light of the Indian political context, and any possibility of an authoritarian application. The possibility of monitoring and regulating access to vital services with the help of biometric authentication provides unparalleled control over citizens. It may instill dissatisfaction and discriminate against the weaker ones. These risks are aggravated by the absence of effective data protection laws, as well as stringent accountability controls.

Technological Determinism versus Social Reality

The Aadhaar experience shows the weakness of technological determinism in the approach to solving the complicated social issues. Designers of the system believed that the use of biometric identification would offer a neutral, objective way of identifying identity and getting rid of fraud. However, that presupposed the mechanisms by which social conditions determine biological traits themselves, the battered fingerprints of manual workers, the shifting biometrics of the aging citizenry, and the increased degradation of the biometrics in marginalized groups. Moreover, the focus on biometric authentication as the most significant way of defining a person is a limited understanding of citizenship that transforms people with multifaceted social lives into digital information units. This reductionist method does not explain the various forms of constructing, negotiating and confirming identity in Indian society, through community awareness, documentary recordings, and social connectivity. With the preference of technological authentication over such other identifications, Aadhaar produces new orders of citizenship founded on technological legibility.

Global Implications and Lessons

The Aadhaar experience in India contains important lessons that other nations planning to implement a similar system of digital identification should pay attention to. The path of the

ISSN:2773-0670

system of voluntary identification to mandatory authentication, welfare delivery to all-encompassing surveillance, depicts how challenging it is to put technological systems in check once they have been implemented. The lack of strong data protection structures before implementation has left path dependencies that are hard to undo, even through judicial intervention.

The development partnership and the international promotion of Aadhaar-like systems with the help of the technical assistance programs are a danger not only to exporting the technology but also to the tension and contradictions inherent in it. The vulnerability of countries to the surveillance capabilities of biometric identification systems might be especially dramatic in cases of weak institutional protection and weak civil society supervision over them. The human rights aspect of these technologies can be lost in the focus on efficiency and the prevention of fraud in the discourse of international development.

Ethical Implications and Policy Recommendations

Ethical Frameworks for Digital Welfare Systems

The Aadhaar case shows how clear ethical principles should be set to regulate digital welfare systems. Such frameworks should strike the right balance between various conflicting values: efficiency and inclusion, fraud prevention and accessibility, technological innovation and human rights. The existing system, which focuses more on efficiency and presupposes that the exclusions can be solved with some technical solutions, turned out to be insufficient.

One way forward in addressing digital welfare systems would be the establishment of rights-based welfare frameworks, which would be based on the assumption that access to social protection is a fundamental right and cannot be conditionalized on successful technological authentication. This would require:

1. Universal Alternative Mechanisms: Non-biometric alternatives should be provided on all welfare programs, and the ease of access must be the same, free of the extra burden of proving it.
2. Burden of Proof Reversal: A reversal of the burden on the citizens to establish themselves to the state to warrant any denial of benefits.
3. Accountability and Redress: There should be easily available mechanisms through which citizens can appeal against authentication failures and have them remedied in time.
4. Transparency in design and Practice: Authentication algorithm publicity, failure modes, and exclusion patterns.

Data Protection and Privacy Safeguards

The proliferation of Aadhaar in the use of the private sector demands the introduction of detailed data protection laws to cover both state and business surveillance. Key elements should include:

1. The Purpose Limitation: There is a stringent boundary on the usage of Aadhaar data in ways other than the initial purpose of collection.
2. Data Minimization: Reducing the data collected and stored to that which is required based on particular legitimate purposes.
3. Consent Mechanisms: Informed consent to any use of biometric data, which is meaningful and which may be revoked.
4. Security Standards: Obligatory security auditing and Data breach liability.

ISSN:2773-0670

5. Regulatory Oversight: An Autonomous information protection agency that is enforced.

Addressing Structural Inequalities

The structural inequalities that digital systems frequently increase cannot be resolved by technical means only. The policy interventions should clearly focus on the disparate effects of digital identification on marginalized populations:

1. Gender-Responsive Design: Making women self-sufficient concerning authentication tools and not be reliant on male family members.
2. Accessibility to the Elderly and Disabled: Special access to citizens with an unreliable biometric or physical barrier to authentication.
3. Rural infrastructure: Investment in rural connectivity and support infrastructure.
4. Digital Literacy: Multifaceted initiatives to establish the ability of citizens to cope with digital systems.

Conclusion

The Aadhaar system of India is also a landmark in the history of the development of digital governance across the globe, and it has shown both lessons and hints of the way the welfare administration is going to evolve in the era of omnipresent surveillance. This paper has recorded how what was initially envisaged to be an inclusion tool has become an entire surveillance grid that systematically locks out the most vulnerable members of society and provides unparalleled surveillance powers to the state and business.

The presented evidence shows that the implementation of Aadhaar has established a fundamental conflict between the efficiency benefits aimed at realizing with the help of digital authentication and the human rights requirement of universal social protection. The failure rates during authentication of 13-49 percent mean millions of citizens will not receive the necessary services, and it is women, the elderly, and marginalized groups of people who will have to endure the unequal share of the exclusion. These exclusions have not been technical accidents, but rather, at the design level, are those technologies that are geared towards technological legibility rather than social reality.

The transformation of the system into voluntary identification and mandatory authentication in the various fields depicts the challenge of policing surveillance technologies once it is put in place. The recent release of Aadhaar to the application of the private sector is a quantitative change to a hybrid form of surveillance that integrates state infrastructure with commercial data mining, causing massive concerns regarding privacy, independence, and democratic control.

The implications of the experience of India on the international level are immense. With governments in many countries around the world increasingly moving towards digital systems of identification, frequently with the assistance of international development bodies, the case of Aadhaar shows that effective safeguards, accountability frameworks, and rights-based strategies to digital welfare systems are in order. The focus on efficiency and fraud prevention should be evaluated in comparison with the original mission of social protection, which is not to leave anyone behind.

In the future, the question is not whether to adopt digital technologies in the welfare administration but how to implement them in a manner that will support other human rights and social justice instead of contradicting them. This needs a shift towards technological determinism in recognition of the complicated social realities in which these systems exist. It

ISSN:2773-0670

requires strong law systems, significant accountability systems, and political determination to uphold the values of inclusion over efficiency where the two are in conflict.

The Aadhaar lessons imply that a digital welfare system should be built with exclusion prevention rather than fraud prevention as a main motive. This needs universal substitute mechanisms, open operations, significant redress procedures and continuing action of different effects. Primarily, it involves the acknowledgement of the fact that citizenship and social rights cannot be brought into the realm of successful biometric authentication, a fact that human dignity cannot be served by digital recognition.

As India keeps on selling its digital public infrastructure model to the rest of the world and other countries take note of comparable systems, the ethical issues raised by Aadhaar become more pressing. The dilemma is not about technology advancement and human rights, but about how to use technology in the service of true inclusion and social justice. The Aadhaar experience shows that in the absence of conscious protection and constant monitoring, digital systems created to assist the citizens can turn into a tool of their surveillance and marginalization.

The new direction needs to be a radical redefinition of the connection between technology, governance, and human rights during the digital era. It is not only a technical problem but also a political and moral necessity, which will determine the character of citizenship, social security, and human dignity in the twenty-first century.

References

Bansal, A. (2018, August 3). Why Aadhaar biometric authentication does not help welfare. *Karana*. https://medium.com/karana/why-aadhaar-biometric-auth-doesnt-help-welfare-935aadf5b912

Braithwaite, J. (2000). The new regulatory state and the transformation of criminology. *British Journal of Criminology*, 40(2), 222-238.

Chaudhuri, B. (2021). Paradoxes of intermediation in Aadhaar: Human making of a digital infrastructure. *South Asia: Journal of South Asian Studies*, 42(3), 572-587.

Dey, N., & Mazdoor Kisan Shakti Sangathan. (2024, December 23). Digital exclusion: Poor, elderly face the brunt of Aadhaar-based authentication errors. *The Wire*. https://thewire.in/rights/digital-exclusion-poor-elderly-face-the-brunt-of-aadhaar-based-authentication-errors

Government of India. (2024). *Aadhaar Dashboard*. Unique Identification Authority of India. https://uidai.gov.in/aadhaar_dashboard/

Huynh, H. (2025, January). Public infrastructure and private surveillance in India's Aadhaar system. *TechPolicy.Press*. https://www.techpolicy.press/public-infrastructure-and-private-surveillance-in-indias-aadhaar-system/

IT for Change. (2023). *Notes from the field: How does Aadhaar-enabled welfare delivery exclude women?* https://itforchange.net/notes-from-field-how-does-aadhaar-enabled-welfare-delivery-exclude-women

Jacobsen, E. K. U. (2012). Unique identification: Inclusion and surveillance in the Indian biometric assemblage. *Security Dialogue*, 43(5), 457-474.

Khera, R. (2019). Aadhaar failures: A tragedy of errors. *Economic and Political Weekly*, 54(14), 32-37.

ISSN:2773-0670

Masiero, S., & Das, S. (2019). Datafying anti-poverty programmes: Implications for data justice. *Information, Communication & Society*, 22(7), 916-933.
Masiero, S., & Prakash, A. (2022). Aadhaar and social assistance programming: Local bureaucracies as critical intermediaries. *Information Technology & People*, 35(8), 2821-2839.
Masiero, S., & Shakthi, S. (2020). Grappling with Aadhaar: Biometrics, social identity and the Indian state. *South Asia Multidisciplinary Academic Journal*, 23, 1-22.
Ministry of Electronics and Information Technology. (2024). *Annual Report 2023-24*. Government of India.
Ministry of Finance. (2024). *Economic Survey 2023-24*. Government of India.
Ministry of Statistics and Programme Implementation. (2024). Share of population covered under Aadhaar in India from the financial year 2018 to 2023. Government of India.
Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2016). Building state capacity: Evidence from biometric smartcards in India. *American Economic Review*, 106(10), 2895-2929.
Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2020). Identity verification standards in welfare programs: Experimental evidence from India. *NBER Working Paper No. 26744*.
Nair, V. (2018). An eye for an I: Recording biometrics and reconsidering identity in post-colonial India. *Contemporary South Asia*, 26(2), 143-156.
National Family Health Survey-5. (2021). *India Report*. International Institute for Population Sciences.
Nilekani, N. (2009). *Imagining India: The idea of a renewed nation*. Penguin Press.
Ramanathan, U. (2014). Biometrics used for social protection programmes in India violates the human rights of the poor. *United Nations Research Institute for Social Development*.
Rao, U., & Greenleaf, G. (2013). Subverting ID from above and below: The uncertain shaping of India's new instrument of e-governance. *Surveillance & Society*, 11(3), 287-300.
Rao, U., & Nair, V. (2019). Aadhaar: Governing with biometrics. *South Asia: Journal of South Asian Studies*, 42(3), 469-481.
Reddy, P. T. (2017, March 29). Aadhaar: Amid the debate about privacy, the more pressing issue of exclusion has been forgotten. *Scroll. In*. https://scroll.in/article/833080/
Sadhya, D., & Sahu, T. (2024). A critical survey of the security and privacy aspects of the Aadhaar framework. *Computers & Security*, 139, 103738.
Sharma, S., Kumar, A., & Singh, M. (2023). Biometric cryptosystem: A comprehensive review. *IEEE Access*, 11, 45678-45702.
Sinha, D. (2024). Technology and accountability in social protection: Evidence from India's PDS reforms. *World Development*, 170, 106-234.
Solanki, A. (2019). Dashboard governance: State surveillance through performance monitoring in India. *South Asia: Journal of South Asian Studies*, 42(3), 534-553.
Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) vs Union of India*, Writ Petition (Civil) No. 494 of 2012.
Supreme Court of India. (2018). *Justice K.S. Puttaswamy (Retd.) vs Union of India*, Writ Petition (Civil) No. 494 of 2012 (Aadhaar Judgment).
UIDAI. (2016). *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*. Government of India.
UIDAI. (2023). *Aadhaar Statistics*. Unique Identification Authority of India.

ISSN:2773-0670

UIDAI. (2024). *Press Releases*. Unique Identification Authority of India. https://uidai.gov.in/media-resources/

UIDAI. (2025). UIDAI records 221 crore Aadhaar authentication transactions in August 2025. *Press Release*.

Walby, K. (1999). The 'new regulatory state': The social powers of the European Union. *British Journal of Sociology*, 50(1), 118-135.

World Bank. (2023). *ID4D Global Dataset*. World Bank Group.

Yadav, A. (2024, December 23). Digital exclusion patterns in Aadhaar authentication. *The Wire*.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

ISSN:2773-0670