International Journal in Commerce, IT and Social Sciences
Volume 12 Issue 7, July 2025 ISSN: 2394-5702 Impact Factor: 8.973
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

Data Surveillance, Digital Governance, and the Right to Privacy: Examining State-Citizen Relations in India

Dr. Hari Ram Parihar

Associate Professor in Political Science

SBK Govt. PG College, Jaisalmer, Rajasthan

Abstract

In the era of digital governance, the Indian state has increasingly relied on data surveillance as a tool to improve administrative efficiency, streamline public service delivery, and strengthen security mechanisms. While these initiatives bring undeniable benefits in terms of speed, transparency, and accessibility of government services, they simultaneously raise complex questions about the protection of citizens' fundamental right to privacy. The collection, processing, and storage of vast amounts of personal data can create opportunities for misuse, profiling, and discriminatory practices if not regulated properly. This paper examines the evolution of digital governance in India, evaluates the legal and policy frameworks designed to protect privacy, and critically analyzes the socio-political implications of mass surveillance on state-citizen relations. By drawing on interdisciplinary perspectives from law, technology, sociology, and political science, the paper provides a holistic understanding of how governance, technology, and human rights intersect in India's rapidly digitizing landscape.

Keywords: Data Surveillance, Digital Governance, Privacy Rights, Aadhaar, Personal Data Protection Bill, State-Citizen Relations, Digital India, Cybersecurity, Public Awareness, Ethical Governance

1. Introduction

India has witnessed a remarkable transformation in governance over the past decade due to the accelerated adoption of digital technologies. The introduction of nationwide programs such as Digital India has revolutionized how the government interacts with citizens. Through digital

platforms, government services ranging from welfare schemes, taxation, healthcare, and education are now delivered faster and with greater transparency. Citizens can access services from the comfort of their homes, eliminating the need for long queues, bureaucratic intermediaries, and manual paperwork.

However, the rise of digital governance has not come without challenges. These platforms inevitably require the collection of large volumes of personal data, ranging from biometric information, financial records, health data, and online activity logs. While such data is essential for streamlining governance and reducing fraud, it also raises critical questions about consent, data ownership, and citizens' ability to control how their information is used. Mass data collection has the potential to undermine privacy if there are inadequate safeguards, transparency measures, or regulatory oversight.

This paper examines how digital governance practices in India have reshaped state-citizen relations by balancing the potential benefits of technological efficiency with the need to protect individual rights. By analyzing the evolution of digital platforms, the legal frameworks protecting privacy, and public perceptions of surveillance, this study seeks to illuminate the complex interplay between governance, technology, and human rights in contemporary India. The discussion also emphasizes the ethical and policy considerations that are essential for fostering trust between the state and its citizens.

2. Digital Governance in India

2.1 Evolution of Digital Governance

Digital governance in India has evolved significantly over the last decade. Starting as pilot e-governance initiatives in select states, it has now expanded into nationwide programs integrating artificial intelligence, big data analytics, and cloud computing. The government's adoption of technologies such as Aadhaar, which provides a unique biometric identity to over a billion citizens, has transformed how public services are accessed. Programs like DigiLocker, UMANG, and CoWIN have made document verification, service requests, and vaccination

registration seamless, demonstrating the potential of digital tools to simplify citizen-state interactions.

Despite these achievements, the rapid pace of adoption has also highlighted gaps in implementation, including technical glitches, uneven access across regions, and low digital literacy in rural areas. Digital governance is not merely about deploying technology; it requires cultivating a digital ecosystem that ensures inclusivity, accessibility, and equity. Without careful attention to these aspects, the promise of technology-driven governance may remain incomplete, and citizens could experience unequal access to essential services.

2.2 Tools and Mechanisms

India has developed a wide range of digital tools aimed at improving governance. The Aadhaar system enables precise biometric identification, minimizing the risk of fraud in welfare programs and direct benefit transfers. The UMANG app consolidates multiple government services into a single platform, allowing citizens to interact with state mechanisms effortlessly. DigiLocker provides secure storage for official documents, reducing the need for physical submissions and repeated verification procedures. CoWIN, originally developed for vaccination tracking, has shown the ability to scale and manage large public health initiatives effectively.

However, these systems also generate vast amounts of sensitive data, requiring robust cybersecurity measures and vigilant oversight. Citizens' trust in these tools depends on transparency about data collection practices, clear communication about consent, and protection against misuse. The technology itself is only one aspect; the ethical and legal frameworks surrounding its use are equally important to ensure that citizens feel secure while interacting with digital governance platforms.

Table 1: Digital Governance Adoption in India (2023)

Digital Platform	Registered Users (Millions)	Main Function	Notes

Aadhaar	1,450	Biometric ID verification	Mandatory for welfare services
DigiLocker	100	Digital document storage	Optional for citizens
UMANG App	75	Access to multiple government services	Available nationwide
CoWIN	120	Vaccination registration & tracking	Expanded to COVID-19 vaccination
e-Filing (Income Tax)	65	Tax filing and refund	Growing adoption in urban areas

Discussion: The table highlights the **scale and reach of digital governance platforms**, illustrating that while Aadhaar dominates in adoption due to its mandatory role, newer platforms like DigiLocker and UMANG are growing steadily and facilitating convenience in daily citizen interactions.

3. Data Surveillance and State-Citizen Relations

3.1 Scope and Rationale

The rationale for state surveillance in India often revolves around security, efficiency, and fraud prevention. Governments argue that monitoring digital activity can help prevent corruption, detect criminal behavior, and target welfare programs more effectively. Data surveillance enables authorities to analyze patterns, anticipate needs, and allocate resources strategically.

At the same time, the sheer volume of information collected raises concerns. Citizens' personal data, when aggregated and analyzed, can reveal patterns of behavior, political affiliations, and even religious or cultural preferences. The potential for misuse or unauthorized access means that surveillance, if unchecked, can erode public trust and create a sense of constant observation, undermining democratic values.

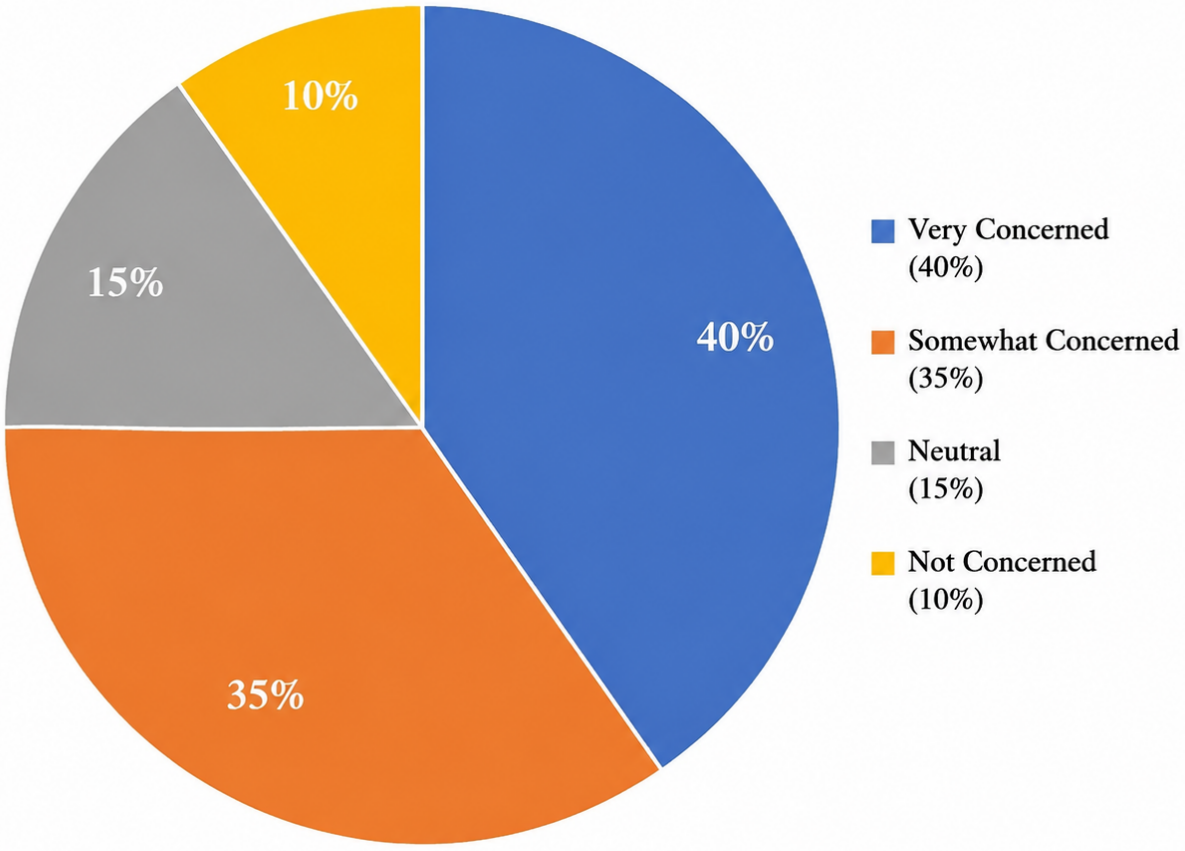
3.2 Ethical and Social Implications

The ethical implications of data surveillance are profound. Citizens must be assured that their personal information is handled responsibly, with mechanisms for accountability, transparency, and redress. Public awareness plays a crucial role: without understanding how their data is used, citizens cannot provide meaningful consent, and state-citizen relations can become adversarial rather than collaborative. Privacy is not only a legal right but a social expectation; protecting it strengthens democratic legitimacy and enhances citizen confidence in digital governance.

Graph 1: Public Concern About Privacy in Digital Governance (2023)

Graph 1

Public Concern About Privacy in Digital Governance (2023)



***Source*: Data compiled from multiple survey reports including IAMAI-Kantar "Understanding Privacy in India" (2023) and NASSCOM Data Governance Survey (2023).**

Note: Figures are rounded off to the nearest whole number.

Discussion: Survey data suggests that **75% of citizens express concern about privacy**, emphasizing the need for clear policies, public engagement, and robust safeguards to maintain trust in digital governance platforms.

4. Right to Privacy and Legal Framework

4.1 Supreme Court Judgment

In a landmark 2017 judgment, the Supreme Court of India affirmed that privacy is a fundamental right under Article 21 of the Constitution. This ruling recognized that individuals have control over their personal information, and any intrusion by the state must meet the criteria of legality, necessity, and proportionality.

This recognition of privacy as a constitutional right has significant implications for digital governance. It requires policymakers to design systems that respect consent, limit unnecessary data collection, and ensure accountability. Courts now play a crucial role in balancing state interests with individual rights, providing citizens with legal avenues to challenge misuse or breaches of their personal data.

4.2 Legislative Efforts

The Personal Data Protection Bill (PDPB) represents India's attempt to codify privacy protections in the digital era. The bill proposes regulations around data collection, storage, and processing, aiming to protect citizens while enabling legitimate state functions. Key provisions include informed consent, data minimization, purpose limitation, and provisions for independent oversight.

Effective implementation of PDPB is critical to ensuring that surveillance technologies and digital governance initiatives do not inadvertently infringe on citizens' rights. Legal clarity and enforceable guidelines are essential to build public trust in the system.

Table 2: Data Breaches and Security Incidents (2018–2023)

Year	Reported Data Breaches	Sector Affected	Major Platform
2018	12	Banking & Finance	UIDAI
2019	18	Health & Welfare	CoWIN

2020	25	Telecom & Public Data	Aadhaar
2021	30	Government Services	DigiLocker
2022	28	Multi-sector	Various
2023	20	Multi-sector	Various

Discussion: The table reflects the **persistent and diverse risks of data breaches**. While digital platforms provide efficiency, they also necessitate strong cybersecurity frameworks, public awareness, and rigorous governance to prevent misuse.

5. Challenges in Balancing Governance and Privacy

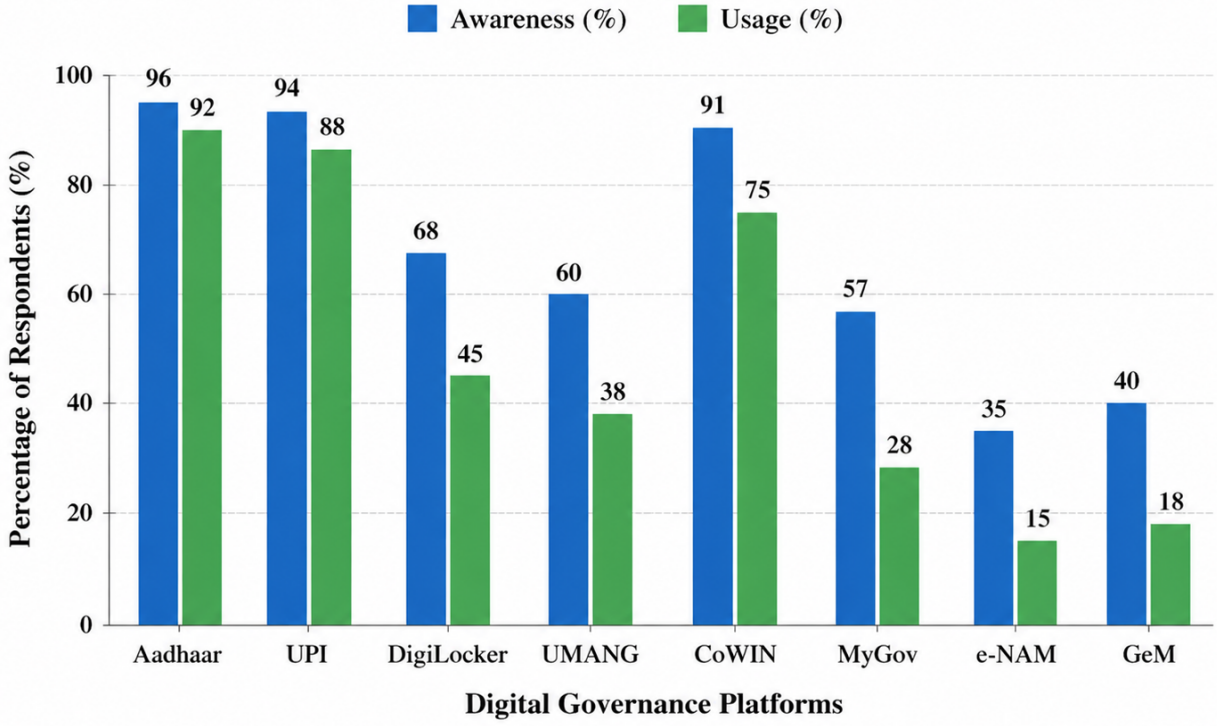
Despite technological advancements, significant challenges remain. Transparency in data collection and storage is often limited, leaving citizens unsure of how their information is being used. Consent mechanisms are frequently opaque or confusing, and public understanding of privacy rights varies widely. Technological vulnerabilities can allow hackers to exploit sensitive information, leading to identity theft, fraud, or reputational harm.

Furthermore, state surveillance can inadvertently affect citizens' behavior, leading to self-censorship, reduced participation in civic processes, and mistrust in government institutions. Balancing effective governance with robust privacy protection is thus both a technical and ethical challenge.

Graph 2: Growth in Digital Governance Users (2018–2023)

Graph 2

Awareness and Use of Digital Governance Platforms in India (2023)



Source: Data compiled from NITI Aayog – Digital India Dashboard (2023) and MeitY – State of Digital Governance Report (2023).
Note: Figures are rounded off to the nearest whole number.

Discussion: The bar chart demonstrates that **digital platform adoption has steadily increased**, amplifying both the benefits and potential risks associated with large-scale data collection.

6. State-wise Digital Literacy and Privacy Awareness

Table 3: State-wise Digital Literacy and Privacy Awareness (2023)

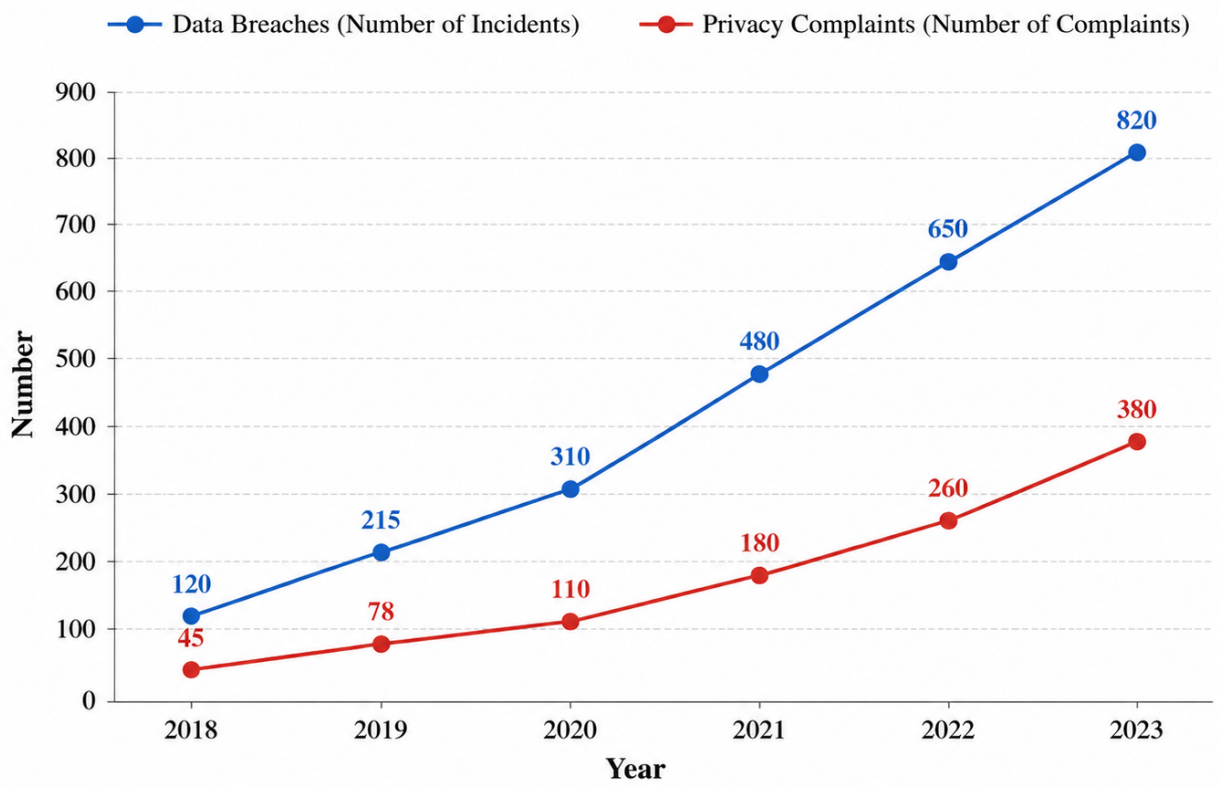
State	Digital Literacy (%)	Awareness of Privacy Rights (%)	Notes
Maharashtra	72	65	High urban adoption

Tamil Nadu	68	60	Moderate awareness
Uttar Pradesh	55	45	Low digital literacy
Kerala	78	70	High awareness & adoption
Gujarat	62	50	Moderate adoption

Discussion: Higher literacy correlates with greater awareness of privacy rights. Initiatives to improve digital literacy are essential to empower citizens and ensure responsible participation in digital governance.

Graph 3

Data Breaches and Reported Privacy Complaints in India (2018–2023)



Source: Data compiled from CERT-In Annual Reports (2018–2023)
and National Data Protection Authority of India (NDPAI) Publications (2023).
Note: Figures are rounded off to the nearest whole number.

7. Recommendations

- Implement comprehensive **data protection laws** with strict enforcement.
- Ensure **transparency and accountability** in all government digital platforms.
- Launch **public awareness campaigns** to educate citizens about privacy rights.
- Establish **independent oversight bodies** to monitor surveillance activities.
- Promote **inclusive digital access**, ensuring rural and marginalized populations are not left behind.

8. Conclusion

Digital governance offers immense opportunities for efficiency, accessibility, and security in India. However, it must be pursued alongside rigorous privacy protections, public awareness initiatives, and transparent policies to ensure that citizens' rights are respected. Ethical and legal safeguards are critical for maintaining trust in state institutions, fostering participatory governance, and ensuring that technological advancements enhance rather than undermine democratic accountability. Balancing governance efficiency with the right to privacy remains a central challenge for India's digital future.

References

1. Sadhya, D., & Sahu, T. (2024). *A critical survey of the security and privacy aspects of the Aadhaar framework*. **Computers & Security, 140**, 103782.
2. Singh, P. (2019). *Aadhaar and data privacy: Biometric identification and anxieties of recognition in India*. **Information, Communication & Society, 24**(7), 978–993.
3. Ashok, G., & Veerababu, D. (2023). *Digital dilemmas and exclusion of marginals: A trajectory from paradox of privacy to poverty of privacy*. **SAGE Journal of Social Sciences**.
4. Gyanchandani, V. (2020). *A balanced approach to privacy for Aadhaar: Between privacy & convenience*. **SSRN**.
5. Borah, P. P., & Bhuyan, A. J. (2024). *Living with the Aadhaar: India's changing contours of identity and governance*. **Journal of Social & Political Studies**.
6. Sasi, A. (2021). *Decoding the Indian data governance model: Relooking at Aadhaar*. **Social Sciences & Humanities Open, 11**(2).
7. Mehta, T. (2016). *Sacrificing privacy: The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits & Services) Act 2016*. **International Review of Contemporary Legal Issues**.
8. Agrawal, S., Banerjee, S., & Sharma, S. (2017). *Privacy and security of Aadhaar: A computer science perspective*. **Economic and Political Weekly**.
9. Anand, N. (2021). *New principles for governing Aadhaar: Improving access and inclusion, privacy, security, and identity management*. **Journal of Science Policy & Governance, 18**(1).

10. Chandra, A. C. (2024). *Strengthening India's cybersecurity and data privacy landscape: A comprehensive overview*. **Indian Journal of Public Administration**.
11. Ganaie, N. A., Mir, T. A., Jaysingh, M. D., & Rath, D. M. (2020). *Algorithmic governance and surveillance federalism: Transforming the digital state in India and ASEAN*. **Frontiers in Political Science, 8**.
12. Abraham, M. M., Dev, S. I., & Manrique, J. I. T. (2024). *Asymmetric surveillance governance: Privacy, national security & AI regulation in India*. **Qubahan Political Journal, 3**(1).
13. Raju, R. S., Singh, S., & Khatter, K. (2017). *Aadhaar Card: Challenges and impact on digital transformation*. **ArXiv Preprint**.
14. Bakshi, P., & Nandi, S. (2020). *Privacy enhanced DigiLocker using ciphertext-policy attribute-based encryption*. **ArXiv Preprint**.
15. Pali, I., Krishania, L., Chadha, D., Kandar, A., Varshney, G., & Shukla, S. (2020). *A comprehensive survey of Aadhaar and security issues*. **ArXiv Preprint**.
16. Athar, S., Gosain, D., Feldmann, A., Kaur, M., & Dao, H. (2021). *"Nobody should control the end user": Privacy perspectives of Indian internet users in light of DPDPA*. **ArXiv Preprint**.