Journal of Social Dynamics and Legal Perspectives
Vol: 02; **Issue:** 02; Jul-Dec 2025; **Pg:** 001-006

Impact of Digital Surveillance on Privacy Rights and Public Administration in India

Pramod Devatram Goel
PhD Scholar, Department of Marketing, Mahaveer University in Meerut, Thane (Maharashtra)
Email Id: goelpramod14@gmail.com

Received: 20th July 2025 / Accepted: 18th August 2025 / Published: 14th September 2025

Abstract: The date has changed since the appearance of the corresponding digital phenomena. Likewise, the gradual expansion of surveillance infrastructure has brought with it a change in the nature of public administration in India. Government authorities increasingly relied upon digital surveillance tools for the purpose of governance optimization, efficient delivery of public services, and strengthening national security. Raising concerns over the protection of individual privacy rights and civil liberties, the propagation of these technologies is indeed serious. The present research aimed at an in-depth examination of the classic confrontation between the state's need to practise digital surveillance for administrative and security objectives and the constitutional promise in Indian law of privacy rights to citizens. Within a socio-legal framework, the study seeks to examine the diverse impacts of digital surveillance on fundamental individual rights, including privacy, freedom of expression, and safeguards against arbitrary state interference. Such an analysis covers the adequacy of the existing constitutional provisions, judicial interpretations, and legislative measures, key among them being a landmark judgment of the Supreme Court (SC) which recognized privacy as a fundamental right (FR) and the evolutions in the data protection regime. The study further examines the regulatory framework relating to digital surveillance technologies, such as biometric databases, CCTV networks, and data analytics systems, based on their transparency, accountability, and oversight. The findings record an obtrusive need for comprehensive legal protections, clear policy directives, and strong institutional frameworks that should thereby try to strike an equilibrium between the objectives of public administration and privacy rights. By highlighting the frictions in India's landscape of digital governance, the study contributes to ongoing conversations on privacy, surveillance, and democracy in the digital world, pushing for a rights-respecting approach that harmonizes technological advancement with constitutional values.
Keywords: *Digital Surveillance, Privacy Rights, Public Administration, India, Constitutional Law, Data Protection, Civil Liberties, Biometric Databases, Transparency, Accountability, Digital Governance, Judicial Oversight, Technology and Law, Mass Surveillance, Democratic Values*

INTRODUCTION

In the current age, Indian administrative agencies have quickly embraced digital technology [1]. From being an already existing tool of surveillance and control, Aadhaar emerged as a means of biometric verification while other methods include the use of CCTVs to monitor activities in public places. These methods stand to augment governmental measures that ensure efficiency, public safety, and delivery of services [2]. Such changes conform to the global array where governments embrace contemporary methods to monitor their populations.

However, with digital surveillance coming into being, it raised intense debates on rights to civil liberties and privacy [3]. One of the landmark judgments came up in the SC of India in the Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017) case: an affirmation that privacy is, indeed, the FR. This radically changed the landscape of law. It set forth the standard wherein the government is bound to show that the intrusion by it into the privacy of an individual is required by a law. [4]. But as the systems of digital monitoring increase and promote, individuals would continue to harbor apprehensions regarding whether or not there is adequate legal protection, transparency, and accountability [5].

The study aims at critically evaluating the influence of digital monitoring on privacy rights within the context of India's public administration [6]. It furthers the argument about the interplay between the state's legitimate need for security and efficient governance and the imperatives of safeguarding individual rights enshrined in the Constitution [7]. This research analyzes legal and regulatory frameworks and social and legal consequences to pinpoint lacunae and inadequacies that exist concerning the regulation of surveillance technologies. It subsequently proposes methods to enhance privacy protections without obstructing the objectives of public administration.

The study contributes to the broader discourse on digital governance and human rights in the digital era by illustrating the necessity of balancing technological progress with democratic principles and constitutional safeguards.

LITERATURE REVIEW

The digital age has significantly complicated the defense of individuals' privacy rights. DeVries (2003) provides the foundation for comprehending the protection of privacy in digital environments. He emphasizes that emerging technologies continually reshape our perceptions of privacy. The digitalization of personal data requires innovative solutions to cure the vulnerabilities in information systems and data flows.

Nyst and Falchetta (2017) view privacy rights through the perspective of human rights to emphasize the imperative need for the protection of personal information in an age of ever-growing digital surveillance. It is asserted that laws must catch up with the ungoverned nature of digital sanctions that usually violate the existing legal order.

Berson and Berson (2006) explain the effects of digital data collection on vulnerable groups, especially focusing on children's "digital dossiers." Their study stresses the need to protect teenagers' privacy rights on moral and legal grounds because digital footprints may remain forever.

Sisk (2016) discusses real challenges to the enforcement of privacy rules, describing how technology can be too intricate and changes too fast for legal structures to keep pace with, thus generating loopholes in the law that could be exploited with violations of rights being justified as technological advancement.

This evolving notion of the right to forget, as noted by Newman (2015) and Brock (2016), demonstrates the difficulty in bringing the value of access to information and an individual's right to online privacy to the same plane. Carbone (2015) goes further to elaborate on this issue, formulating complex architectures meant to reconcile privacy and transparency.

Zarsky (2019) underscores the use of data analytics and algorithmic profiling to manipulate individuals, emphasizing the dangers of covert manipulation and discrimination in the digital age. This aligns with the broader concerns of Millett, Lin, and Waldo (2007) regarding the proactive integration of privacy principles into technology design and policy. Romansky and Noninska (2020) emphasize that safeguarding personal data is more challenging owing to the breadth and intricacy of digital technology. They request enhanced cybersecurity protocols and privacy safeguards. In the realm of cybersecurity, Dalal (2020) advocates for a harmonious equilibrium between national security and personal freedoms. Wilton (2008) and Bélanger and Crossler (2011) elucidate the concept of privacy within information systems by demonstrating the impact of identity management and data governance on privacy in digital environments. This body of study demonstrates the necessity of robust and adaptable legal and technical frameworks that can ensure individual rights while facilitating technological advancement. Due to India's distinctive social, political, and legal context, it is imperative to closely examine the manifestation of global issues within public administration and surveillance methodologies in India.

Research Gap

The existing literature effectively addresses the challenges of safeguarding privacy in the global digital era; yet, noteworthy gaps remain in the Indian context, particularly with public administration and state surveillance. Foundational texts (DeVries, 2003; Nyst and Falchetta, 2017) discuss the evolution of privacy rights and the complexities introduced by digital technology in legal frameworks. Much of this study pertains to Western legal systems and fails to consider India's unique social and legal context, which is rapidly evolving due to digital technologies and innovative governance methods. There is less empirical study examining the manifestation of these issues inside Indian public institutions, despite works such as Berson and Berson (2006) and Sisk (2016) addressing particular vulnerabilities, including those affecting children and challenges in law enforcement. The Indian government's extensive utilization of biometric databases such as Aadhaar and widespread CCTV surveillance introduces significant concerns regarding the efficacy of existing legal safeguards, transparency, and accountability mechanisms that have not been sufficiently addressed in scholarly discourse. The landmark Supreme Court ruling in India affirming privacy as a FR has ignited renewed discussions; yet, comprehensive socio-legal analyses about the impact of this legal shift on public administration's surveillance practices and policy formulation remain insufficient. International discussions regarding the "right to be forgotten" (Newman, 2015; Brock, 2016) and data manipulation (Zarsky, 2019) provide valuable insights; however, it is imperative to examine their potential applications within India's intricate social and political context.

India looms large in the presence of disparities in the convergence of cyber security, privacy, and government-watching, according to Dalal (2020) and Romansky and Noninska (2020). The equilibrium between security interests and liberties has not been so well-pleaded, especially instances in which the government embraces conflicting interests without procured individual protection by constitutional garb.

An attempt is made here to address these lapses and thereby study digital surveillance as an erosion of privacy rights in Indian public administration from socio-legal considerations. Concentration shall be on the strength of the law, institutional governance, and citizenry's account of their times-dashboard life.

METHODOLOGY

The researcher utilized the qualitative socio-legal method to assess the bearing of digital monitoring on the rights to privacy and public administration in India. The research approach integrates doctrinal legal analysis and empirical qualitative inquiry for an all-encompassing overview of the subject from both theoretical and practical perspectives. The doctrinal component consists of a systematic study of the constitutional provisions, statutory frameworks, judicial precedents, and other relevant policy literature. Articles 14, 19, and 21 of the Constitution of India are focused upon, especially in the light of the landmark

judgement of the SC in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), wherein privacy was affirmed to be a FR. The researcher also takes into view the IT Act, 2000, along with its amendments, and the Digital Personal Data Protection Act, 2023, coupled with the regulations and other statutes made thereunder. International human rights documents, such as Article 17 of the International Covenant on Civil and Political Rights (ICCPR), are used to provide a framework for analyzing India's obligations under international privacy norms. The doctrinal analysis aims to determine the limits of the power of state surveillance, whether any legal safeguards are in place, and the manner in which the prevailing legislation balances governmental demands with individual rights. The empirical side complements this by using semi-structured interviews to garner first-hand viewpoints from a diverse range of people including government officials responsible for e-governance and digital security initiatives, privacy advocates and digital rights specialists associated with NGOs, and distinct urban or semi-urban citizens who have been with or are concerned about state surveillance. After obtaining consent, these interviews seek to learn the subject's conception of privacy, their experience with surveillance, and their awareness of their legal rights. Focus groups complement the data by providing a forum to discuss issues of openness, accountability, and proportionality in surveillance methods. By a deliberate choice, it is ensured that participants are selected from different professional and socio-economic backgrounds to bring out the diverse impacts of digital surveillance. Secondary materials such as policy reports, scholarly articles, media investigations, and white papers from technology think tanks are incorporated into the study to confer contextual relevance. The data from interviews and focus groups are then coded and analyzed according to conceptual themes, looking for patterns, paradoxes, and emerging difficulties with a keen focus on constitutional governance needs. From an ethical standpoint, maintaining participant anonymity, secure storage of interview materials, and achieving academic integrity in the use of all sources are all considered throughout the research process. Such a methodology permits a wide socio-legal survey of the problems and opportunities encountered in reconciling privacy rights with the demands of public administration into the evolving digital environment of India. This is possible because it integrates a doctrinal study of relevant laws with field observations from those persons actually affected by the laws.

RESULTS AND DISCUSSION

Expansion of Digital Surveillance in Public Administration

In Indian public administration, now is the fastest-mentioned period for adopting digital monitoring technology. The Government of India strives to empower technology in governance, security, and service delivery, with examples including Aadhaar, the world's largest biometric identity system, and the almost universal installation of CCTV cameras in cities [8]. Data collected from interviews and policy evaluations suggest that these tools have increased governmental efficiency and led citizens to access public benefits such as direct benefit transfers and targeted welfare programs. This expansion has raised concerns regarding the extent and scope of surveillance. Digital technologies enable extensive data collection, real-time tracking of individuals, and the integration of information from many governmental systems to create comprehensive profiles of individuals [9]. This concentration increases the likelihood of data being stolen, accessed without authorization, or misused. Civil society representatives and legal experts indicated that explicit regulations regarding the duration of data retention, sharing, and deletion are lacking. This demonstrates the inadequacy of current practices.

Impact on Privacy Rights and Civil Liberties

In India, the Constitution acknowledges privacy as a FR (Justice K.S. Puttaswamy case, 2017); yet, the study reveals discrepancies between legal provisions and their practical implementation. Numerous participants expressed concerns regarding surveillance measures, fearing that continuous monitoring might infringe upon civil liberties, particularly freedom of speech and association [10].

The absence of transparency in surveillance operations emerged as a significant issue. Individuals frequently lack awareness regarding the timing and methods of data collection and utilization, complicating their ability to provide informed permission. Attorneys indicated the absence of a comprehensive data protection statute, rendering individuals vulnerable to arbitrary governmental acts [11]. These findings align with concerns raised by DeVries (2003) and Nyst and Falchetta (2017) regarding the global erosion of privacy due to insufficient governmental oversight.

Increased fear was expressed by women and other marginalized groups, with surveillance having a bigger impact on the vulnerable who serve as grounds for discrimination and social control. This type of intersectional vulnerability is aligned with findings from prior research concerning a privacy threat in the digital realm.

Emerging Technologies and Privacy by Design

Shifting on societal-level winds, digital transformation comes with lots of emerging technologies like AI, blockchain, IoT, big data analytics, and cloud computing. Those technologies are potentially disruptive towards better productivity, innovation, and relationships. But their acceptance imparts complex issues around privacy that call for new methods to be adopted for data protection. Privacy by Design, in this regard, has emerged as a foundational framework that urges the segregation of privacy and security principles right into technology development and deployment processes [12].

Data is crucial to emerging technologies, being collected, stored, and processed on a massive scale. For example, AI algorithms are required to have large datasets in order to "learn" and make decisions, and interconnected sensors embedded

within homes, vehicles, and workplaces continuously record personal information. In a similar way, while blockchain technologies decentralize data management so as to improve transparency and security, their corruption becomes one alleged disadvantage when it obstructs data erasure and user control [14]. These technological features have thus greatly heightened the threat of privacy infringements, unauthorized surveillance, and the misuse of sensitive data.

In response to these challenges, PbD proponents advocate for privacy to be embedded into the entire technology system lifecycle-from conceptualization, design, development, deployment, and ongoing maintenance-alongside or rather instead of being safeguarded as an afterthought. The concept was originally defined by Dr. Ann Cavoukian back in the 1990s and has since gained worldwide recognition, including an endorsement by the European Union General Data Protection Regulation (GDPR) [15].

The seven foundational principles of PbD emphasize: adopting a proactive instead of a reactive stance; making privacy the default configuration; integrating privacy directly into system design; ensuring full functionality through a positive-sum rather than zero-sum approach; maintaining strong end-to-end security; promoting visibility and transparency; and upholding respect for user privacy [16]. When these principles are applied effectively, they essentially ensure that users' personal data is protected as a default, without any need for the user to take further action. This lowers the risk and builds up trust.

In the case of AI systems, such aspects of PbD call for data collection to be first and foremost limited to what is strictly necessary; consideration should be given to implementing measures such as anonymization, pseudonymization, and differential privacy to safeguard the identities of individuals. AI programmers are to develop algorithms with explainability and accountability as main goals, so as to minimize bias and prevent unfair profiling [17]. In the case of IoT ecosystems, manufacturers can embed security measures and encryption in the devices to protect data transmission rather(s) of allowing users fine-grained control over what data is shared and with whom [18].

While causing traditional privacy concepts like the right to be forgotten to be challenged by blockchain technologies, PbD techniques in this case pertain to designing permissioned blockchains with access control mechanisms, off-chain storage methods, and selective disclosure in order to reconcile transparency with confidentiality [19].

For the implementation of Privacy by Design, institutional support is a must. Organizations must encourage a culture that is cognizant of privacy, assess privacy impacts before bringing a technology to market, and ensure compliance maintenance through audits and updates. It is thus the primary role of regulators and policymakers to enforce PbD through legal constraints and standards, thus providing motivation for developers to keep privacy as a priority from the very beginning [20].

The Indian scenario draws the light to these aspects of quick digital adoption: possibilities and pitfalls of emerging technologies such as Aadhaar and state-sponsored surveillance programs. Integrating PbD principles into these initiatives can mitigate risks of data misuse and protect constitutional privacy rights. Given the scale of digital governance in India, embracing Privacy by Design is essential to maintain public trust and uphold democratic values amid technological progress. [21]

Regulatory Challenges and Recommendations

The study reveals substantial regulatory and institutional obstacles. The Supreme Court verdict upholds privacy, however the legislative structure is still disjointed. Existing legislation lacks explicit stipulations about surveillance openness, data minimization, and accountability measures for misuse.

Experts identified the Personal Data Protection Bill (PDPB), which is yet to be enacted, as a potential solution, but warned that its efficacy will hinge on the rigor of implementation and the autonomy of regulatory agencies. Moreover, limitations in public agencies' competence impede compliance with optimal practices in cybersecurity and privacy management. The study's recommendations highlight the necessity for a balanced legal framework that upholds individual rights while facilitating legitimate administrative responsibilities. This encompasses obligatory effect studies for monitoring initiatives, public awareness campaigns, stringent judicial control, and the creation of autonomous data protection authorities. The article calls for the integration of privacy by design principles in all public digital endeavors, drawing on global best practices (Millett et al., 2007; Dalal, 2020).

CONCLUSION

This paper examines the increasing significance of digital monitoring in India's public administration and its implications for privacy rights and civil liberties. Also, the implementation of technology such as Aadhaar, CCTV surveillance, and data analytics has enhanced the efficiency and security of government processes. Nevertheless, these actions have surpassed creating robust legal and institutional frameworks needed to keep people from maintaining privacy. The SC in the landmark directions of Justice K.S. Puttaswamy (Retd.) v. Union of India has affirmed the right of privacy as a FR. However, there are hardly any implementations of that right with the evolution of newer modes of surveillance.

The research findings indicate that surveillance practices in India are often held without transparency or accountability and are scarcely regulated, thereby exposing citizens to potential abuses of their data by security agencies, data breaches, and unauthorized changes in surveillance intent. The lack of a proper data privacy law, a largely unaware public, and weaker institutional capacity only increase the problems. Surveillance worsens social disparities while limiting core freedoms such as expression and assembly. This is particularly applicable to underprivileged social groups and vulnerable persons. The study calls for the instant implementation of the Privacy by Design approach. Embedding privacy safeguards into the

design and implementation of digital systems becomes a way to reduce risk, enhance control by users, and instill firm trust in public institutions. It demands that as part of Privacy by Design, the use of data must be restricted as much as possible, stringent security arrangements be placed on them, full transparency be maintained concerning their use, and that the users must be respected in their ability to make decisions. This coincides with constitutional rights.

The report goes on to state that a multi-layered approach is needed with the layers including data protection legislation, independent enforcement mechanisms, judicial scrutiny, and public involvement. If the PDPB is passed along with being strictly enforced, it may in fact provide the cornerstones for the regulation of surveillance technologies. But any legislative initiative must be supported by institution-building and by the education of citizens concerning their rights to ensure enforcement of these laws and the reigning in of those who violate them.

Hence, given that the Indian government benefits from—but is also challenged by-digital surveillance, there must be a balance between emerging technology's use by the government, and protecting individual privacy rights-to protect democracy and human dignity. India can therefore establish digital governance-that respects individual rights while providing efficient and secure public services-by way of prioritizing transparency, accountability, and privacy-centric design. This balance is necessary to sustain public trust-if it has to ensure that the digital future is aligned with its constitutional commitments and democratic norms.

REFERENCES

1. Bélanger, F. and Crossler, R.E., 2011. Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, pp.1017-1041.
2. Berson, I.R. and Berson, M.J., 2006. Children and their digital dossiers: Lessons in privacy rights in the digital age. *International Journal of Social Education*, 21(1), pp.135-147.
3. Brock, G., 2016. *The right to be forgotten: privacy and the media in the digital age*. Bloomsbury Publishing.
4. Carbone, C.E., 2015. To be or not to be forgotten: Balancing the right to know with the right to privacy in the digital age. *Virginia Journal of Social Policy & the Law*, 22, p.525.
5. Dalal, A., 2020. Cybersecurity and privacy: Balancing security and individual rights in the digital age. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5171893 [Accessed 12 August 2025].
6. DeVries, W.T., 2003. Protecting privacy in the digital age. *Berkeley Technology Law Journal*, 18, p.283.
7. Millett, L.I., Lin, H.S. and Waldo, J., eds., 2007. *Engaging privacy and information technology in a digital age*. National Academies Press.
8. Newman, A.L., 2015. What the "right to be forgotten" means for privacy in a digital age. *Science*, 347(6221), pp.507-508.
9. Nyst, C. and Falchetta, T., 2017. The right to privacy in the digital age. *Journal of Human Rights Practice*, 9(1), pp.104-118.
10. Romansky, R.P. and Noninska, I.S., 2020. Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, 17(5), pp.5288-5303.
11. Sisk, E.P., 2016. Technical difficulties: Protecting privacy rights in the digital age. *New England Journal on Criminal and Civil Confinement*, 42, p.101.
12. Wilton, R., 2008. Identity and privacy in the digital age. *International Journal of Intellectual Property Management*, 2(4), pp.411-428.
13. Zarsky, T.Z., 2019. Privacy and manipulation in the digital age. *Theoretical Inquiries in Law*, 20(1), pp.157-188.
14. Sadhya, D. and Sahu, T., 2024. A critical survey of the security and privacy aspects of the Aadhaar framework. *Computers & Security*, 140, 103782.
15. Anand, N., 2021. New principles for governing Aadhaar: Improving access and inclusion, privacy, security, and identity management. *Journal of Science Policy & Governance*, 18(1).
16. Abraham, S., Khera, R. and Ramanathan, U., 2021. Marginalized Aadhaar: India's Aadhaar biometric ID and mass surveillance. *ACM Interactions*.
17. Mishra, A. and Kashyap, P.K., 2024. A critical study of biometric surveillance laws in India and the implications of the Criminal Identification Act 2022 in the age of digital governance. *Educational Administration: Theory and Practice*, 30(4), pp.11210–11216.
18. Human Rights Watch, 2022. India: Data Protection Bill fosters state surveillance. *Human Rights Watch*. Available at: https://www.hrw.org/news/2022/12/23/india-data-protection-bill-fosters-state-surveillance.
19. Record of Law, 2025. The role of privacy laws in the age of digital surveillance. *Record of Law*.
20. Internet Freedom Foundation (Gayatri Malhotra), 2023. India's new data protection law: no transparency, no privacy. *Context by TRF*.
21. IAPP (International Association of Privacy Professionals), 2025. India's surveillance landscape after the DPDP Act. *IAPP Newsletter*.