



Digital Surveillance in India: Constitutional Challenges and Implications for Civil Liberties

Jiya Bhatt ¹, Manthan Khopkar ²

¹ Student, Computer studies and Emerging Technology,
TransStadia University, Ahmedabad

² Assistant Professor, Computer studies and Emerging Technology,
TransStadia University, Ahmedabad

Abstract- Digital surveillance has emerged as an integral feature of governance in contemporary India. The desire for national security, prevention of crime, distribution of welfare services, and administrative efficiency has prompted the Indian state to increasingly adopt digital technologies in the areas of governance. The rapid expansion of digital technologies such as biometric technologies, facial recognition technologies, and extensive communication interception technologies has enabled the Indian state to increasingly use digital surveillance. The use of such technologies has not only provided efficiency in governance but has also posed significant challenges to civil liberties such as the right to privacy, freedom of expression, and the right to due process. The paper seeks to examine the evolution of digital surveillance in India, the constitutional basis of digital surveillance in India, and the implications of digital surveillance on civil liberties in India. The paper seeks to examine the implications of digital governance in India on the constitutional values of a democratic society. The paper seeks to examine the implications of digital governance in India on the constitutional values of a democratic society. The paper seeks to examine the implications of digital governance in India on the constitutional values of a democratic society.

Keywords- Digital Surveillance, Civil Liberties, Right to Privacy, Indian Constitution, Data Protection, State Accountability, Privacy Law, Governance

I.INTRODUCTION

India has rapidly evolved from an analog society to a digitally governed society. The Indian state has increasingly used digital technologies in the areas of governance over the past ten years. The use of digital technologies in the areas of governance has not only provided efficiency in governance but has also posed significant challenges to civil liberties such as the right to privacy, freedom of expression, and the right to due process.

In the case of India, the issue of surveillance is not new. The majority of the legislation in the sphere of surveillance,

especially in the sphere of the interception of communications, is colonial in origin and was introduced with the primary objective of maintaining administrative control over the population, not protecting the rights of citizens. The Indian Telegraph Act of 1885 is still in force in the digital age. The digitalization of the sphere of surveillance is enormous in scope; it enables the real-time tracking of citizens, the storage of data over time, and the creation of detailed profiles of citizens. The question is whether the Indian system is capable of regulating such extensive powers of surveillance.



II. RESEARCH OBJECTIVES

To examine the evolution of the methods of digital surveillance in India.

To examine the legal and constitutional framework that governs the practices of surveillance in the country.

To examine the impact of digital surveillance on civil liberties in the country.

To examine the reforms that can be introduced in the sphere of surveillance.

III. RESEARCH QUESTIONS

How has the sphere of digital surveillance expanded in the recent past in the Indian context?

Are the current legislative mechanisms adequate in regulating the sphere of digital surveillance in the country?

What is the impact of digital surveillance on civil liberties in the Indian context?

What reforms can be introduced in the sphere of digital surveillance?

IV. RESEARCH METHODOLOGY

The present study undertakes a qualitative approach to understand the legal and constitutional ramifications of digital surveillance in India. The methodology for this study is based on secondary research, relying on various legal provisions, judicial pronouncements, government policies, academic literature, and reports from civil society organizations. The study undertakes a comparative approach to assess the viability of digital surveillance in India in relation to international human rights standards and democratic governance. The methodology is based on legal interpretation, policy analysis, and critical evaluation, as opposed to data collection.

V. LITERATURE REVIEW

The literature on digital surveillance reveals the increasing concerns regarding the erosion of democratic freedoms owing to excessive state surveillance. The literature reveals that there exists a significant threat to civil liberties in India owing to the increasing surveillance infrastructure. The literature on smart city surveillance projects reveals that there exists a significant threat to social equality owing to the implementation of large-scale surveillance projects. Moreover, there exists a significant threat to civil liberties owing to continuous surveillance without proper consent or transparency.

The literature on government surveillance reveals significant concerns regarding democratic freedoms owing to excessive state surveillance. Moreover, there exists a significant threat to democratic freedoms owing to the continuous surveillance of citizens. The literature reveals that there exists a significant threat owing to the development of a surveillance state, wherein there exists a significant threat owing to the collection and processing of personal data.

The literature on international surveillance reveals significant concerns regarding democratic freedoms owing to excessive state surveillance. Moreover, there exists a significant threat owing to the development of a surveillance state in many countries within the European Union.

Despite significant literature on surveillance and civil liberties, there exists a lack of focus on the gap between constitutional law and practice in India. This research aims to bridge the gap between constitutional law and practice in India. This research aims to critically analyze the effectiveness of the current regulatory framework in providing institutional accountability.



VI. PROBLEM STATEMENT

The development of digital surveillance mechanisms in India has been accompanied by an absence of robust legal frameworks and mechanisms. While the right to privacy is recognized as a fundamental right by the Indian Constitution, the practice of surveillance is still based on old legal frameworks and broad executive powers. Citizens are not aware of the extent to which their personal information is being collected, processed, and monitored. This is due to the absence of clear authorization mechanisms and judicial review, which can easily lead to the misuse and potential political surveillance of citizens.

VII. DIGITAL SURVEILLANCE MECHANISMS IN INDIA

Aadhaar and Biometric Surveillance

The Aadhaar project is the world's largest biometric identification project. This project collects fingerprints, iris scans, and other demographic information to provide a unique identity number to Indian citizens. While the Aadhaar project has been very effective in improving government efficiencies and delivering welfare services to citizens, concerns have been raised about data security issues, unauthorized information authentication, and potential surveillance through database convergence.

Communication Interception and Internet Monitoring

Government authorities derive their powers to intercept communication and the internet from the Indian Telegraph Act of 1885 and the Information Technology Act of 2000. Surveillance mechanisms like the Central Monitoring System (CMS) and Network Traffic Analysis (NETRA) allow the government to monitor large numbers of phone calls, emails, and internet usage. These mechanisms are not very transparent and have very limited judicial review. This

is a potential threat to the Indian Constitution and the right to privacy.

Facial Recognition and CCTV Surveillance

Facial recognition and extensive CCTV surveillance have become very popular mechanisms to control and police crowds and to maintain public order. While these mechanisms have been very useful to law enforcement agencies, the absence of clear and comprehensive legal frameworks to regulate their use is a potential threat to the right to privacy and the potential misuse of personal information. While citizens are being monitored, this is likely to create a culture of surveillance and reduce anonymity.

VIII. LEGAL AND CONSTITUTIONAL FRAMEWORK

Right to Privacy

The establishment of the right to privacy as a fundamental right under Article 21 of the Indian Constitution marked a milestone in the development of Indian constitutional law. The Supreme Court has established the principles of legality, necessity, and proportionality as the essential requirements for state action affecting the privacy of individuals. However, the application of the principles has been inconsistent in the context of emerging surveillance technologies.

Data Protection Regime

The Indian data protection regime has been in a state of development with the implementation of the Digital Personal Data Protection Act, 2023. While the new act marks a milestone in the development of a data protection regime in India, the new act has also been criticized for providing broad exemptions to the government authorities



on the pretext of national security and maintaining public order.

Case Study: Pegasus Surveillance Controversy

One of the most notable instances of digital surveillance in India relates to the Pegasus surveillance controversy. According to the reports, the Indian government was accused of using the Pegasus surveillance software to access the private communications of journalists, activists, and politicians. Such instances have raised significant concerns regarding the use of surveillance technologies and the need for stronger legal frameworks.

IX. CHALLENGES

Regulating digital surveillance in India faces several challenges. These challenges include the lack of updated laws on surveillance in India, the changing nature of technology in the digital age, the lack of regulatory bodies in India to deal with the issue of digital surveillance, and the lack of transparency in decision-making. National security has become the main factor in dealing with the issue of digital surveillance in India. Therefore, it has become difficult to strike the right balance between national security and the right to freedom.

Policy Recommendations

The government must establish an independent body comprising judicial personnel to authorize the practice of digital surveillance in India.

The government must bring updates to the existing laws on surveillance in India.

The government must incorporate the element of procedure in dealing with the issue of digital surveillance in India.

The government must increase parliamentary oversight in dealing with the issue of digital surveillance in India.

The government must increase public awareness about the issue of digital surveillance in India.

Future Scope

Future studies may be carried out in the following areas. The studies may focus on the impact of digital surveillance on the lives of journalists, activists, and marginalized communities. The government may compare the situation in India with the situation in other democratic countries. The use of artificial intelligence in the practice of digital surveillance in India may be studied from the academic point of view

X. CONCLUSION

Digital surveillance in India has become an important phenomenon in the Indian context. The practice of digital surveillance in India has both negative and positive effects. The negative effects of the practice of digital surveillance in India include the threat to the right to freedom. The practice of digital surveillance in India has become necessary to maintain law and order in the country. Therefore, the government must be careful in dealing with the issue of digital surveillance in India.

REFERENCES

India-Specific Surveillance and Civil Liberties

1. Mahapatra, S. (2021). Digital Surveillance and the Threat to Civil Liberties in India. *Journal of Asian Public Policy*.
2. Bhatia, G. (2019). *Privacy and the Constitution of India: A Doctrinal and Comparative Analysis*. Oxford University Press.



3. Ramanathan, U. (2014). Aadhaar: From Welfare to Surveillance. *Economic and Political Weekly*.
4. Greenleaf, G. (2023). India's Digital Personal Data Protection Act: A Comparative Analysis. *Privacy Laws & Business International Report*.
5. Abraham, S., & Prakash, P. (2019). State Surveillance in India: Legal and Constitutional Issues. *Internet Freedom Foundation Report*.
6. Singh, P. (2020). Facial Recognition Technology and Privacy Concerns in India. *Indian Journal of Law and Technology*.
7. Narayan, R. (2022). Digital Surveillance and Democratic Accountability in India. *Journal of Constitutional Studies*.

Global Surveillance and Privacy Theory

8. Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Polity Press.
9. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
10. Solove, D. J. (2021). *Understanding Privacy*. Harvard University Press.
11. Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. Vintage Books.
12. Marx, G. T. (2016). *Windows into the Soul: Surveillance and Society in an Age of High Technology*. University of Chicago Press.
13. Ball, K., Haggerty, K., & Lyon, D. (2012). *The Routledge Handbook of Surveillance Studies*. Routledge.

International Human Rights and Legal Frameworks

14. United Nations. (2018). *The Right to Privacy in the Digital Age*. UN Office of the High Commissioner for Human Rights.
15. European Union. (2016). *General Data Protection Regulation (GDPR)*.
16. Council of Europe. (2021). *Guidelines on Facial Recognition Technology and Human Rights*.
17. United Nations Special Rapporteur. (2019). *Surveillance and Human Rights Report*.

IV. Key Legal Cases

18. Justice K.S. Puttaswamy v. Union of India Supreme Court of India (2017)
19. People's Union for Civil Liberties v. Union of India Supreme Court of India (1997)
20. Anuradha Bhasin v. Union of India Supreme Court of India (2020)
21. Maneka Gandhi v. Union of India Supreme Court of India (1978)

Government and Policy Reports

22. Government of India. (2023). *Digital Personal Data Protection Act*.
23. Ministry of Home Affairs. (2021). *Central Monitoring System (CMS) Framework Report*.
24. NITI Aayog. (2022). *Data Governance and Privacy Framework in India*.
25. Reserve Bank of India. (2021). *Guidelines on Data Protection and Cybersecurity*.

Emerging Technology and Surveillance

26. Kitchin, R. (2020). *The Data Revolution: Big Data, Open Data, Data Infrastructures*. Sage Publications.
27. Smith, G. (2020). *Artificial Intelligence and Surveillance: Ethical and Legal Challenges*. *Technology and Society Journal*.
28. Taylor, L., Floridi, L., & Van der Sloot, B. (2017). *Group Privacy: New Challenges of Data Technologies*. Springer.
29. Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness*. Duke University Press.
30. OECD. (2022). *Digital Security and Privacy Framework*.