International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 24-02-2026, Accepted: 27-03-2026, Published: 11-04-2026
Volume 12, Issue 2, 2026, Page No. 65-68

Social Media surveillance and privacy erosion in India: Legal Framework, Digital Rights, and citizen vulnerability

Rachana Gupta[1], Dr. Rajendra Prasad[2]
[1] Research Scholar, Drpartment of Law, Bundelkhand University, Jhansi, Uttar Pradesh, India
[2] Bundelkhand College, Jhansi Uttar Pradesh, India

Abstract
Social media has revolutionized the way people communicate and engage with the population in India, yet it has also increased the threats of surveillance, misuse of data, and invasion of privacy. Within the framework of this paper, a critical look at the way social media platforms are the strong data-collection ecosystems, which allow constant monitoring, profiling, and tracking of users behaviour will be provided. It sheds light on the growing susceptibility of Indian citizens because of lax consent procedures, obscure privacy policies, algorithmic surveillance, and the commercialization of personal data. The paper also examines the Indian jurisprudence of digital privacy, such as constitutional protection of Article 21, the influence of K.S. Puttaswamy v. Union of India, and the legislative policy of the Information Technology Act, 2000. The Digital Personal Data Protection Act, 2023, is given particular attention with a focus on how well this act can enhance privacy protection alongside pinpointing the issues of enforcement and exemptions. This paper claims that the breakneck pace at which social media surveillance is expanding is a significant threat to individual autonomy, democratic freedom and even the rights of digital citizens. It is concluded with the recommendations of greater regulatory responsibility, platform transparency requirements and better privacy regulation to ensure citizen protection in the digital changing India.

Keywords: Surveillance, social media, right to privacy, digital rights, IT Act 2000, K.S. Puttaswamy, DPDP Act 2023, data protection, citizen vulnerability

Introduction

Background and Context

The advent of online media has propelled social media to become a core component of personal communication, social interaction and information sharing in the world. As a result of this proliferation, social networking sites have created a digital ecosystem where user behaviour, preferences and interactions are continually tracked and monitored, through the generation of vast amounts of personal data. Studies have pointed to the fact that social media sites are involved in systematic data gathering and behavioural surveillance, frequently in the absence of any specific user authorization, casting grave doubt on the safety and confidentiality of information on the internet. Moreover, researchers note that the increase in online surveillance has significant consequences on the autonomy of a person and informational self-determination.

Social Media and Surveillance

Social media are structured in such a way that the maximum engagement is achieved by personalised content, which is greatly reliant on the need to monitor user activity, location data, and past interactions. This kind of data gathering can be used to perform algorithm-based profiling, targeted advertising, and predictive analytics, frequently without full understanding or user control. These activities are one of the new types of digital surveillance which are not limited to corporate interests, but they also affect the opinion and consumer behaviour of people and even their political involvement. Research on information privacy in social media points to the fact that information privacy among users is largely influenced by data collection methods and user behaviour, which implies that user actions on the internet usually put them at risk of unforeseen privacy invasion.

Privacy: A Fundamental Right in India

The case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) [8] in India marked a major change in legal status of privacy in the country. In this historical decision, a nine-judge Constitution Bench unanimously decided that the right to privacy was a basic right that was guaranteed by Article 21 of the Constitution, which included personal autonomy, informational privacy, and dignity. The ruling made by the Court reversed the previous jurisprudence and created the possibility that only a law that is legitimate, necessary, and proportionate can restrain privacy. This precedent now forms the basis of assessing the sufficiency of legal safeguards against surveillance and misuse of data in the digital era in India.

Objectives of The Study

The paper is based on the following objectives:

1. To investigate how social media surveillance is being born and developed in the digital era.
2. To examine how social media sites gather, crunch, and use personal data, which results in the erosion of privacy.
3. In order to examine the constitutional acknowledgment of the right to privacy in India, particularly, Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) [8].
4. To assess the current Indian legal system on social media monitoring and data protection, such as the Information Technology Act, 2000 and other regulations.
5. To determine the applicability and usefulness of the Digital Personal Data Protection Act, 2023 in dealing with privacy issues that crop up as a result of social media surveillance.

6. To bring out the insecurities of the Indian citizens in the face of digital watch and misappropriation of personal information.
7. To recommend legal and policy actions to enhance privacy protection and accountability of social media in India.

Conceptual Framework

1. Meaning of Social Media Surveillance

Social media surveillance is the process of collecting, monitoring and analyzing user information systematically by the platform with the aim of either commercial, behavioural or security purposes. This involves monitoring online behaviours, content interactions as well as individual features to create rich user profiles that can be applied to do targeted advertising or behavioural forecasting.

2. Digital Privacy and Informational Self-Determination

Digital privacy is about the control that an individual has of personal information online. Informational self-determination is the right to choose on the way the data about the person is gathered and processed. In the case of social media, users seldom make a truly informed consent as a result of unclear policies and large-scale data processing.

3. Data Monetization and Surveillance Capitalism

Surveillance capitalism refers to an economic model in which individual information is commercialized and transformed into revenue by constantly monitoring, tracking and algorithmically analyzing. Studies underscore the manner in which large technology platforms capture and commercialize user data to deliver advertisements and manipulate behaviour.

4. Digital Vulnerability and Exposure of citizens

Identity theft, manipulation of behaviour and abuse of data are some of the dangers that users face when exposed to massive surveillance ecosystem. In the online realm, the personal autonomy and civil liberties of citizens are undermined in the absence of sufficient protection.

Review of Literature

1. Global Literature on Social Media Surveillance

International literature demonstrates that surveillance is not restricted to corporate applications but it is also used to manipulate the behaviour of the masses, changing the perception of privacy and autonomy.

2. Privacy and user behaviour studies

Researchers discover that users tend to underrate data surveillance and have poor comprehension of privacy regulations.

3. Indian Law on privacy rights

In Indian literature after Puttaswamy, the constitutional position of privacy and the necessity of its detailed legal safeguards is emphasized.

4. Government Surveillance and State Power Studies

Research on state surveillance demonstrates a conflict between the demands of security and privacy rights, particularly in the arena of digital governance.

5. Research Gap

Although theory is abundant, not much has been done to connect legal protections and real world societal surveillance activities that affect citizens.

Indian Laws on Privacy and Surveillance

1. Protection of Privacy as a Constitutional Right

The right to privacy is under Article 21 of the Constitution of India, which guarantees the right to life and personal liberty. In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) [8], a nine-judge Constitution Bench unanimously declared the right to privacy a fundamental right in Article 21 and must not be infringed, unless through a fair, just and reasonable process, that has been laid down under law. This ruling reversed previous rulings and acknowledged the informational privacy as a vital component of individual freedom in the digital era. The Court has pointed out that the privacy of personal information is an important aspect that involves autonomy, dignity and control over information.

2. Information Technology Act, 2000

In India, digital activities are regulated by the Information Technology Act, 2000 (IT Act), which has restricted protection of privacy.

- Section 43A holds companies responsible in cases of non-protection of sensitive personal data when the companies are supposed to adopt reasonable security measures. In practice, however, there has been laxity in enforcement.
- Section 69 and section 69A will provide the state with authority to intercept, monitor or block digital information in the name of the state order or state sovereignty or state security, invoking controversy around the question of whether surveillance authority strikes a balance with the privacy interest.
- Section 72 and Section 72A punish unauthorized disclosure of information by government officials or intermediaries and it is a criminal offence to disclose personal information without permission where the information is harmful.

3. Intermediary Guidelines Rules, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 require social media intermediaries to adopt measures such as grievance redressal mechanisms and appoint compliance officers. There are also clauses in the Rules on traceability of messages to prevent abuse, although critics claim that traceability requirements can be incompatible with user privacy and encryption protections.

4. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the first independent data protection regime in India governing the processes of digital personal data processing and highlighting such principles of ethical data processing as consent, transparency, limitation of purposes and security protection. Some of the rights granted to data principals by the Act include access, correction, erasure and withdrawal of consent. Nevertheless, it also contains exemptions of government agencies under specific situations and gradual implementation of major provisions still poses implementation problems.

Research Methodology

1. Research Design

The current research is based on a doctrinal and analytical research design. The legal principles of privacy and surveillance in India are analyzed through the doctrinal approach, whereas the critique of the efficiency of the current laws in the area of social media surveillance and privacy loss is discussed using the analytical method.

2. Sources of Data

The study is based on both primary and secondary sources of data. Constitutional provisions, including Article 21, statutory laws, including the Information Technology Act, 2000, Intermediary Guidelines Rules, 2021, the Digital Personal Data Protection Act, 2023, and landmark judicial cases, including Justice K.S. Puttaswamy v. Union of India. The secondary sources will be books, research articles, journals, government reports, policy documents, and published online materials on privacy, surveillance and digital rights.

3. Method of Analysis

The study uses the comparative analysis as a method to review the Indian privacy legislation against the international privacy standards and frameworks. The practical interpretation of the powers of surveillance and the lack of laws to protect the digital privacy of citizens are evaluated by means of a critical analysis.

4. Limitations of the Study

It is restricted to doctrinal analysis, and lacks an empirical fieldwork. It dwells primarily on Indian law and judicial events concerning social media surveillance.

Findings

1. Social Media Surveillance Processes

The study concludes that social media is by its very nature designed to capture and track online activity of users. These platforms also collect active (e.g., posts, messages) and passive data (e.g., location, device identifiers, browsing traces), which are used to create detailed user profiles, and in many cases users are not aware of the scope of such data collection. This constant surveillance of user behaviour is in line with the principle of dataveillance, meaning widespread surveillance of data and metadata in online networks and social networks, which is not only used to customize content, but also to make predictions and share this data with third parties, subjecting users to multifaceted privacy risks.

2. Consent and Data Exploitation

One significant result is that social media user consent mechanisms tend to be superficial. Users are also normally made to agree to long privacy policies without clear understanding, which enables platforms to process, distribute and monetize personal data. Such consent practices do not constitute an actual informational self-determination and as such, impairs the control that users have over their personal data. A more recent empirical study brings to light the role of privacy issues in shaping user behaviour and how lack of transparency in data practices contribute to vulnerability to privacy violations.

3. Legal Loopholes and Enforcement Problems

The research also reveals that there are major loopholes in the legal framework of India. Although privacy has been constitutionally acknowledged in the wake of Puttaswamy, the measures to put the control methods in place against social media surveillance are at variance with technological realities. Laws, such as the Information Technology Act and more recent legislation on data protection, offer principles but have been criticized as being difficult to enforce and insufficiently policing the issue of data abuse and surveillance, placing users in a vulnerable position regarding their lack of protection against data misuse and surveillance.

Discussion

1. Privacy Risk and Vulnerability of Citizen

The results indicate that deep data gathering, profiling and surveillance by the social media platforms exposes citizens to high levels of privacy risk. The data-oriented model provided by social media exposes users to identity theft, data abuse and manipulation of behavioural patterns because of the dark-web approach to consent and constant monitoring of personal data. The studies stress that in the absence of explicit and binding protection, people cannot have a meaningful control over the processing and sharing of their data. Lack of privacy in a user-centered design makes it worse in terms of susceptibility to cyber-attacks and unauthorized use of personal data.

2. State Surveillance and Fundamental Rights

Although India acknowledges the right to privacy as a basic one, the legal exceptions and sweeping surveillance authority by the current legislation make one question excessive government surveillance. Critics contend that certain elements of the Digital Personal Data Protection Act, 2023 and its Rules might permit interpretations that diminish transparency and grant more access by the state without sufficient checks and balances, which may erode individualized privacy protection. The conflict between national security and privacy rights depicts the long-standing constitutional dilemmas of ensuring the protection of individual autonomy by an intrusive approach in the digital environment, by the state.

3. International Standards and Indian Position

Comparative views show that international standards such as the General Data Protection Regulation (GDPR) focus on greater and more robust individual rights, accountability and enforcement procedures over the Indian system, which focuses on compliance with low penalties and gradual implementation. Such international norms can offer practical templates to enhance the privacy regime in India and balance between technological advancements and strong civil liberties.

Recommendations

1. Strengthening Privacy Laws

The Indian legal system should transform beyond initial legislation to deal with privacy erosion in social media. The Digital Personal Data Protection Act, 2023 must be complemented with more substantial enforcement mechanisms, a more detailed consent management procedure, and a decrease in the exemptions that may be misapplied to have a way to avoid privacy protection. Based on the best practices identified internationally assists in organizing the legal requirements that would strike a balance between innovation and individual rights.

2. Regulating Platform Accountability

Social media platforms must be expected to a greater level of transparency and accountability, such as requiring data practices to be disclosed, consent notices to be clear, breach notification schedules to be strict and regular, and audits to be conducted by independent entities. Some of the aspects that India can adopt in its privacy legislation include the provision of better rights to the data subject and dedicated supervision as in the case of the GDPR and other international frameworks to make sure that the platforms meet their data protection commitments at all times.

3. Improving Digital Awareness

Enhancing legal specifications should be accompanied by software education that informs users of their rights, data protection principles and consent impacts. Education of citizens through public education, privacy-by-design norms and industry best practices will enable citizens to responsibly manage personal data and hold digital service providers accountable.

Conclusion

1. Summary of Key Findings

This paper concludes that social media surveillance systems, poor consent culture, and legal laxity are all factors that have led to the erosion of privacy among the Indian citizens. Privacy is a constitutionally guaranteed right after Puttaswamy, but the Digital Personal Data Protection Act, 2023 and associated regulations cause real-life privacy to be reduced as a means to protect against data surveillance, profiling and abuse.

2. Concluding Observations

The only way to balance between digital innovation and privacy rights is to have a strong legal and regulatory ecosystem that considers technological realities. The integration of the privacy regulations in India with the international privacy laws such as the GDPR can serve as a measure to strengthen the privacy of Indian citizens without undermining the advantages of online platforms. The policy measures must raise accountability, imposing explicit data rights and lessening legal uncertainties that can facilitate unjustified surveillance.

3. Future Legal Scope

The areas of future studies and legislative efforts ought to be the closing of enforcement loopholes, broadening the rights of data subjects, improving the consent process, and enhancing institutional accountability. Increased international collaboration and alignment with the international privacy systems will further strengthen the role of India in defending digital rights and civil liberties.

References

1. Abrol C. ‘The Key Aspects of India’s Data Protection Act’, 2024. (online).
2. Belapurkar R. ‘Information Privacy Concerns and Surveillance in Social Media’, 2018, 1(5). International Journal of Law Management and Humanities (IJLMH) (online).
3. Bonfils N. ‘An Empirical Inquiry into Surveillance Capitalism: Web Tracking’, 2025. arXiv (online).
4. ‘Dataveillance’ Wikipedia (online).
5. Kaur D. ‘The Right to Privacy in Social Media Platforms: Legal and Regulatory Challenges in India’, 2025, 7(5) International Journal for Multidisciplinary Research (IJFMR) https://doi.org/10.36948/ijfmr.2025.v07i05.57047.
6. Gour H. ‘India’s New Digital Personal Data Protection Rules, 2025 – A Detailed Reading’, 2025 (online).
7. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
8. Justice K.S. Puttaswamy (Retd.) v Union of India,2017:10 SCC 1 (SC).
9. Kumar S, Punam S. Right to Privacy in the Age of Social Media: An Analysis of Indian Jurisprudence (ResearchGate 2025) (online).
10. Singh V, Singh S. Privacy and Surveillance in Digital Era: A Case for India (ResearchGate 2025) (online).
11. Digital Personal Data Protection Act, 2023. (Act 22 of 2023).
12. ‘Privacy Concern Behaviour on Social Media Sites’, 2022 SAGE Journals (online).
13. Supreme Court Observer. ‘Fundamental Right to Privacy’, 2025. (online).
14. ‘The Evolution of Right to Privacy: From K.S. Puttaswamy to Aadhaar’, 2025. International Journal for Multidisciplinary Research (IJFMR) (online).
15. Gupta V, Srivastava S. ‘Right to Privacy and Data Protection Regime in India: A Critical Analysis’ (IILM University, Greater Noida, 2025.
16. Yadav V. ‘Crossing Borders: Comparative Perspectives on Data Protection Laws in India, the EU and the US’, 2025.
17. Drishti IAS. ‘Towards a Robust Digital Data Protection Regime in India’ (online).
18. INDIA CONST art 21.