Anusandhanvallari
Vol 2025, No.1s
January 2025
ISSN 2229-3388

Privacy in the Age of Social Media Challenges for Indian Law and Society

1stDr S. Udayakumar, 2ndP Sowjanya, 3rdDr Pamarthi Satyanarayana,

[1]Assistant Professor, School of Law, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai.

[2]Research Scholar, Dept of Law, Sri Padmavati Mahila Visvavidyalayam (Women's University), Tirupati, Andhra Pradesh, India.

[3]Assistant Professor, School of Law, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai.

Abstract: The fast growth of social media sites has completely changed the boundaries of privacy in India with vexed legal and social issues. Personal data is now a lucrative commodity and a potential victim since millions of people are using digital platforms every day. Privacy being declared as a basic right in K.S. Puttaswamy v. Union of India was a landmark constitutional achievement but the practice of exercising this right in social media is still fraught with difficulties. This paper is a critical reflection on the changing concept of privacy in relation to user-generated content, the practice of data sharing, and algorithmic surveillance. It examines the sufficiency of the current legal frameworks, specifically the Digital Personal Data Protection Act, 2023, to tackle the new threats, including data misuse, identity theft, and online harassment. The paper also examines the conflict between the freedom of expression and privacy rights and the role of intermediaries and accountability. Within the socio-legal framework, the paper highlights the effects of digital illiteracy, consent fatigue, and an unequal access to the legal solutions. It concludes by recommending an equal opportunity approach to regulation that incorporates strong legal protection, technological remedies, and social education to allow a significant degree of privacy protection in the fast-growing digital world of India.

Keywords: Digital Privacy, Social Media Regulation, Data Protection Law, Right to Privacy, Cyber Law in India.

1. Introduction

The introduction of social media has completely changed how people communicate, interact and express themselves in the modern society. Facebook, Instagram, X (previously Twitter) and WhatsApp are the platforms that have built up a dynamic digital ecosystem where the personal information is shared, stored, and analyzed constantly. Social media use has become so ingrained in daily lives in India, where internet penetration has increased exponentially over the past ten years. On the one hand, these platforms provide a whole new level of connectivity and expression; on the other hand, they are a real threat to the privacy of the individuals. The information on personal data, which previously was kept in a narrow circle, is currently being revealed in cyberspace on a regular basis, often without a clear understanding of the repercussions.

The concept of privacy in the social media age is no longer confined to the usual perception of confidentiality or secrecy. Rather it includes informational privacy, data autonomy and the right to manage ones digital identity. Users willingly provide photos, views, and positioning information, and preferences, which undergo intricate algorithms to generate targeted advertisement and behavioral profiling. This commodity-like sale of personal information has brought forth the question of how much people are in control of their data. This is compounded by unclear privacy policies and terms of service agreements which users accept without any substantial consent. Consequently, the concept of informed consent can be cast doubt on in practice.

Social media privacy is an issue that is compounded by digital illiteracy, socio-economic differences, and lack of awareness of data rights in India. The nature of data collection, sharing, and even monetization is unknown to

many users, which exposes them to exploitation. Cases of data breaches, identity theft, cyberstalking and online harassment have become more frequent than ever, and the legal and regulatory systems have become weaker than ever. Furthermore, social media sites are cross-border which makes them difficult to enforce, because the data is frequently stored and processed in jurisdictions other than India.

The conflict between the rights of individuals and collective interests is another important aspect of privacy in the social media environment. The social media is the platform of public conversation, political activism and social movements thus involving the right to express oneself. Nevertheless, misinformation, hate speech, and intrusive surveillance practices can also be spread via the same platforms. This poses a fine line between maintaining privacy and maintaining democracy.

Moreover, the emergence of technological innovations like artificial intelligence, facial recognition, and analytics of big data has escalated privacy issues. Such technologies allow gathering and analyzing data at unprecedented levels, and the analysis is often conducted without the express permission of the users. The resulting surveillance economy pits the conventional law system in difficulties, which finds it hard to keep up with the pace of change in technology. In this regard, privacy should be redefined to not just a passive right but an active and enforced right that needs constant protection.

2. Privacy in India: constitutional foundations

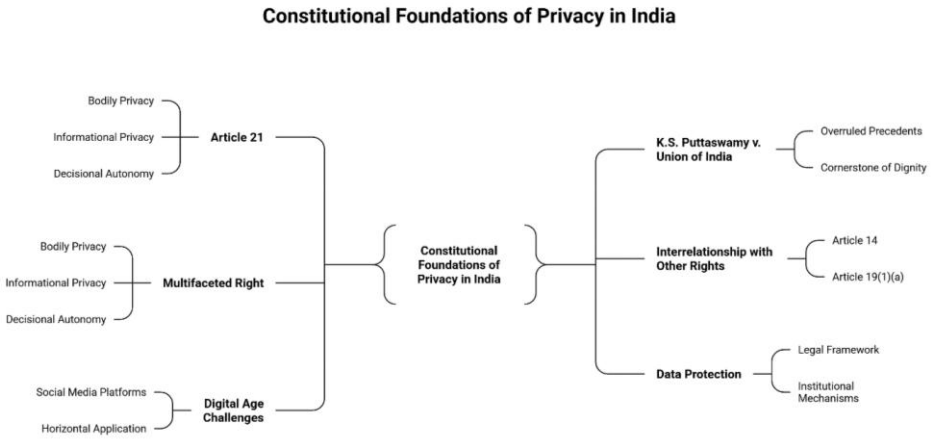

Fig: Constitutional Foundations of Privacy in India

The acknowledgment of the right to privacy in the Indian constitution is a paradigm shift in the history of the development of the fundamental rights jurisprudence. Privacy is not a direct right that is stated in the Constitution of India, but the judiciary has interpreted it as an inseparable right to the right to life and personal liberty in Article 21. This conception culminated in the landmark decision of ***K.S. Puttaswamy v. Union of India*** in which a nine-judge court led by the Supreme Court judges confirmed beyond a reasonable doubt that privacy is a constitutional right. The case was not just a repeal of previous precedents, but it also made privacy a fundamental part of the dignity, autonomy, and freedom of individuals.

The conceptualization of privacy in the Puttaswamy judgment viewed privacy as a complex right that includes bodily privacy, informational privacy and autonomy in decision making. The informational privacy, more specifically, has become highly relevant recently in the framework of social media, where personal information is being constantly generated and processed. The Court stressed that people need to possess their personal data and that any violation should meet the criteria of legality, necessity, and proportionality. This framework has taken the form of the guiding principle to assess state actions that could be a violation of privacy rights.

The constitutional base of privacy is further enforced by the fact that it is interrelated to other rights that are fundamental like equality in Article 14 and freedom of speech and expression in Article 19(1)(a). Privacy is a measure of protection against arbitrary power of the state and a guarantee that people are not interfered with in their exercise of freedoms. Concurrently, the Court recognized that privacy was not an absolute right and could be limited under reasonable restrictions in the name of national security, public order and other valid state interests.

The applicability of constitutional principles in the context of social media in the digital era poses challenging issues. In contrast to the conventional state actors, social media platforms are privately owned and possess a great influence on the information of users and discourse. It has resulted in arguments about the horizontal extension of basic rights and to what degree constitutional protections are applicable against private corporations. Whereas the traditional focus of Indian jurisprudence has been on vertical relations between the state and individuals, it is increasingly being realized that there is the need to consider the role of the private in bringing about privacy outcomes.

The Puttaswamy case also emphasized on the role of data protection as a vital aspect of privacy. It demanded the creation of a strong legal system to govern the process of gathering, storing and processing of personal information. This law has shaped the future of legislation and the introduction of new comprehensive laws on data protection. Nevertheless, constitutional privacy rights can be effectively implemented only through legal provisions as well as institutional mechanisms and enforcement practices.

The connection of constitutional privacy to human dignity is another important element of constitutional privacy. The Court pointed out that privacy is what helps people to form their own personalities, make their own choices, and preserve personal relationships without interference of others. When social media is used to reveal information about people and their personal lives, the safeguarding of dignity is especially. The psychological and social effects of the abuse of personal data, Internet harassment, and unauthorized surveillance may be far-reaching, thus subverting the meaning of constitutional rights.

3. Laws and regulations of social media and data protection

Law and policy provisions in the regulation of privacy in social media in India is a combination of statutory provisions, subordinate legislation and developing policy frameworks. Traditionally, the most significant law used to regulate digital activities was the Information Technology Act, 2000, which offered the fundamental legal framework of electronic governance and cyber crimes. The Section 43A and the rules on reasonable security practices were some of the provisions that attempted to make corporations that dealt with sensitive personal data accountable. These provisions were however not comprehensive enough and did not offer the multifaceted methodology that is needed to accommodate the intricacies of contemporary data-driven ecosystems.

Acknowledging these shortcomings, India has adopted the Digital Personal Data Protection Act, 2023, which is a serious move towards creating a specific data protection regime. The lawful processing, purpose limitation, data minimization, and accountability are some of the key principles introduced by the Act. It establishes the responsibilities of data fiduciaries and data principal, thus establishing a detailed system of data governance. Notably, the Act focuses on consent as the main premise of data processing, which must be free, informed, specific, and clear. It is especially applicable to the case of social media, where the data about users are gathered and processed in large amounts and used in different ways.

The Act further offers the formation of a Data Protection Board to monitor compliance and make decisions on contention. It sets responsibilities on the entities to introduce a reasonable security protection and requires the reporting of the data breach. It also adds children data protection provisions, as children are more vulnerable in the online space. Regardless of these developments, there are still fears about the efficiency of enforcement tools, the extent of waivers to the state and the possibility of over-regulation.

Besides the data protection framework, social media platforms regulation is affected by the intermediary liability provisions of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These regulations also place due diligence on the intermediaries whereby there is a need to delete illegal content and trace messages under specific circumstances. Although these steps are taken to increase accountability and prevent abuse, they also become a major privacy concern, especially in terms of end-to-end encryption and anonymity of the users.

The cross-border movement of data is another important concern. Social media sites are frequently global in nature, and the data is saved and processed across various jurisdictions. The lack of clear and consistent regulations of data localization and transfers on the national and international levels complicates the enforcement of regulations and leads to issues concerning the data sovereignty. The Digital Personal Data Protection Act is an effort to curb this problem by permitting cross-border transfers to the countries that are notified, yet the standards of such notifications are still.

Moreover, such novel issues as artificial intelligence, algorithmic profiling, and targeted advertising have to be addressed by the legal framework. Through these technologies, much personal information can be gathered and processed even without the direct knowledge of the users. The current laws do not cope with the subtleties of such practices, and it is essential to keep legal changes. Regulatory agencies, judicial checks and balances, and self-regulation in the industry become critical in making sure that technological innovation is not at the expense of privacy.

4. New Issues: Online Abuse of Data, Surveillance, and Online Abuse

The fast growth of the social media sites has brought about a multifaceted array of challenges that jeopardize the privacy of individuals and the well being of the society. The abuse of personal data is among the most significant issues. Social media organizations gather immense amounts of user data, such as preferences, behavioral patterns, geographic location data, and communication history. This information is frequently sold via targeted advertising and it is distributed to third parties, at times without the knowledge or premeditated approval of users. The resulting data economy poses serious questions of ownership, control and accountability. Cases of information intrusion and unauthorized entry have also put users at risk of identity theft, financial fraud and damages to reputation.

Raising levels of surveillance, both state and non-state, is another important issue. Surveillance by governments can be based on the grounds of national security, civil order or preventing crime. Nonetheless, the unrestrained surveillance may cause the decay of civil liberties and produce the chilling effect on free speech. Facial recognition, biometric identification, and artificial intelligence are just some examples of technologies that allow constant surveillance of people with little or no protection or transparency. The issues of proportionality and need of such surveillance measures have been brought up in the Indian context especially in the wake of constitutional safeguards that have been identified in K.S. Puttaswamy v. Union of India. The lack of detailed control systems contributes to increasing the risk of abuse even more.

Another important facet of the privacy debate is online harm. The social media platforms have turned into a place where people become targets of cyberbullying, harassment, trolling, doxxing, and non-consent sharing of intimate material. These harms are disproportionately experienced by women, children, and marginalized communities, thus creating issues of digital inequality and discrimination. The psychological effects of these harms might be drastic as a result of which anxiety, depression, and social isolation emerge. Although there are legal redresses, the law is not properly enforced and victims are usually subjected to procedural barriers to access justice.

Misinformation and disinformation are also phenomena that overlap privacy issues. Manipulated or false content may be exploited to attack individuals, intrude on their privacy, and ruin their reputation. Furthermore, the spread

of content determined by algorithms tends to boost sensational or harmful content, which generates a situation in which the breach of privacy may propagate fast and uncontrollably. The extent to which social media platforms moderate such content has been a matter of argument and questions arise of whether they are accountable and responsible.

Furthermore, the phenomenon of consent fatigue has become one of the significant issues of the digital age. Consumers are often asked to accept long and complicated privacy policies, which they often do without a full comprehension of the consequences of such agreements. This is the sabotage of the principles of consent-based data protection systems and the questioning of the efficiency of the legal protection that is already in place.

5. Privacy vs. Freedom of Expression

The correlation between the right to privacy and the right to freedom of expression is one of the complex problems in current constitutional and digital language. Both the rights are fundamental to a democratic society and are guaranteed by the Indian Constitution- privacy by Article 21 and freedom of speech and expression by Article 19(1) (a). But in the case of social media, these rights tend to clash, and a delicate and context-sensitive balance strategy has to be taken.

Social media sites have become important avenues of social communication where people can express their views, engage in political discussions and organise towards social agendas. Democratization of information has enabled the voices that are marginalized and enhances participatory governance. But with this growth of freedom of expression have also come occasions where speech can violate the privacy and dignity of others. To illustrate, sharing of personal information, defamatory statements as well as intrusive commentary can infringe on the right of privacy of an individual without the permission of the individual being discussed. The difficulty in this situation is the definition of the boundaries of what can be allowed to be expressed.

The judiciary has been pivotal in balancing this. The Supreme Court declared in the case of Shreya Singhal v. Union of India that the freedom of expression was infringed by Section 66A of the Information Technology Act, 2000. Meanwhile, the Court recognized that reasonable restrictions can be applied to avoid harm, such as the privacy protection. This two-faceted acknowledgment highlights the proportionality and necessity of regulation of online speech.

The entry of intermediaries, including social media platforms, is one of the main concerns in balancing these rights. These organizations are the gatekeepers of online communication and have the responsibility of censoring content. Nevertheless, their choices are usually questioned regarding transparency, accountability, and a possible bias. Excessive regulation can result in censorship and repression of legitimate expression, and conversely, the lack of regulation can result in the spread of harmful material. It is necessary to find the optimal balance, which would be achieved through clear-cut guidelines and efficient supervision mechanisms.

The other critical area is the difference between the public interest and the harm in the privacy. Although freedom of expression safeguards the sharing of information about issues of societal interest, it does not cover the infringement of the privacy of individuals without reasonable cause. It is at this point that the principle of reasonable expectation of privacy comes into play, especially when the personal lives of individuals are disclosed without their approval. Courts should pay close attention to the purpose of the disclosure of information, i.e. whether it is related to an honest purpose of the public or an intrusion into autonomy in private.

This balance is also complicated by technological reasons. Social media content is viral, so the consequences of the privacy breach can be very far-reaching and irreversible. When the information is posted online, it becomes hard to control the spread of information and it is important to use preventive measures as opposed to using post-facto solutions. Meanwhile, the shortcoming of technological solutions is that automated content moderation systems can easily censor legitimate speech.

After all, it is going to need a subtle and dynamic balance between privacy and freedom of expression. It requires a mix of legal clarity, judicial prudence, platform responsibility, and user awareness. It is only within the framework of this comprehensive approach that the competing interests will be balanced to some extent in order to respect the democratic principles and protect the rights of individuals.

6. Conclusion

The convergence between privacy and social media in India is a dynamic and changing area of the law that has both opportunities and challenges. The establishment of the right to privacy as a basic right in K.S. Puttaswamy v. Union of India has provided a solid constitutional base but the actual implementation of the right in the digital age is not comprehensive. With the rapid development of technologies and spread of social media networks, issues related to the misuse of data, surveillance, and the internet harm have been escalated. Simultaneously, the necessity to maintain freedom of expression as a principal of democracy makes the regulatory action difficult.

Going ahead, an all-encompassing and dynamic privacy protection is in urgent demand. Laws like the Digital Personal Data Protection Act, 2023 need to be properly enforced and they should prioritize transparency, accountability and empowering users. Institutional strengthening would be necessary to enforce the regulations on time and be effective through the stricter institutional mechanisms such as regulatory bodies and grievance redressal systems. Also, privacy-by-design and strong encryption are among technological solutions that need to be promoted to improve the security of data.

The role of digital literacy and public awareness is also very important. It is necessary to provide users with the knowledge and tools to make informed decisions regarding their data and online actions. Social media as one of the stakeholders have to embrace ethical practices and become more transparent in their operations.

References

[1] Jindal, T. (2024). Right to Privacy as a Fundamental Right in India: Evolution, Challenges, and the Impact of Digitalization. *International Journal For Multidisciplinary Research*, *6*(6). https://doi.org/10.36948/ijfmr.2024.v06i06.31832

[2] Grover, D. J., & Singh, R. (2024). The law of right to privacy in india: protecting privacy in the digital era: challenges. *ShodhKosh Journal of Visual and Performing Arts*, *5*(1). https://doi.org/10.29121/shodhkosh.v5.i1.2024.3498

[3] Tiwari, S. K., & Mishra, K. G. (2024). A case study on right to privacy. *ShodhKosh Journal of Visual and Performing Arts*, *5*(5). https://doi.org/10.29121/shodhkosh.v5.i5.2024.2967

[4] Prashanth, S. K., & Devaiah, N. G. (2024). *Privacy on New Media Platforms*. https://doi.org/10.20944/preprints202405.0497.v1

[5] Mittal, S., & Sharma, P. (2017). *A Study of the Privacy Attitudes of the Users of the Social Network(ing) Sites and Their Expectations from the Law in India* (pp. 1038–1051). Springer, Cham. https://doi.org/10.1007/978-3-319-76348-4_100

[6] Ansari, M. B., & Haque, I. (2024). Privacy Rights and Social Media. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2024.58023

[7] Uppaluri, U., & Shivanagowda, V. (2015). Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating Toward a Privacy Right in India. *Social Science Research Network*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2660569

[8] Satapathy, A. (2024). *The use of social media as evidence according to indian law*. https://doi.org/10.5281/zenodo.11115757

[9] Siwal, A. (2021). *Social Media Platform Regulation in India – A Special Reference to The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (pp. 215–232). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748929789-215

[10] Basu, S. (2012). Privacy Protection: A Tale of Two Cultures. *Masaryk University Journal of Law and Technology*, *6*(1), 1–34. https://journals.muni.cz/mujlt/article/download/2593/2157

[11] Bhandari, V., & Sane, R. (2018). Protecting Citizens From the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018. *Social Science Research Network*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3251982

[12] Ardhapurkar, S. B., Srivastava, T., Sharma, S., Chaurasiya, V. K., & Vaish, A. (2010). Privacy and Data Protection in Cyberspace in Indian Environment. *International Journal of Engineering Science and Technology*, *2*(5), 942–951.