

The Right to Privacy in Social Media Platforms: Legal and Regulatory Challenges in India

Ms. Dev Kaur¹, Prof. (Dr.) Amar Nath²

¹Research Scholar, Faculty of law, Agra college, Agra, Dr. Bhim Rao Ambedkar University, Agra (UP)

²Professor, Faculty of Law, Agra college, Agra, Dr. Bhim Rao Ambedkar University, Agra (UP)

Abstract

In India the hasty evolution of social media platforms has renovated E-commerce, communication and social connections, although at the same time growing complex apprehensions in relation with right to privacy. Although in case of “Justice K.S. Puttaswamy vs. Union of India (2017)” the Hon’ble Supreme Court of India recognized right to privacy as a fundamental right. Social media platforms gather, process and transmit huge amount of individual’s personal data frequently without any proper consent mechanisms, that leads to revealing individual’s data to surveillance, profiling and abuse of information. This research paper scrutinizes the legal and supervisory challenges regarding protection of privacy on social media platforms in India through focusing on Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023 and the other legal frameworks and guidelines. The paper also examines the loop holes regarding execution, jurisdictional complications, and the absence of vigorous accountability mechanisms for the organizations related to technology. The paper deals with the existing legal frameworks which provide a base, but they remain unsatisfactory while addressing the vigorous risks that evolve through technologies, algorithmic governance and cross-border data transfer. Reinforcing supervisory oversight, increasing public awareness and arrange Indian laws with worldwide standards such as the GDPR which are very important for guaranteeing significant protection of privacy rights in this digital era.

Keywords: Right to Privacy, Social Media Platforms, Cyber laws in India

1. Introduction

In past decades, India has observed a digital revolution along with more than 800 million (approximate) internet users and a speedily growing format for social media users. Social media platforms have a focused point on politics, commerce, entertainment and individual expressions. Though the nature of these social media platforms was constructed regarding data collection, advertisement, programmatic profiling that leads to creates a high risk in context to individual privacy.

In the landmark case of “Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017)” the Hon’ble Supreme Court of India legally recognized the Right to Privacy as a fundamental right under Article 21 of the Constitution of India. Not like out-dated privacy concerns, digital privacy is not only vulnerable by state surveillance but also through the private organizations that work with enormous power and have a limited liability.

In India, the data protection related to social media platforms and individual consent is mainly governed

by Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules). The IT Act delivers a comprehensive framework related to the protection of personal data and requires organizations to collect and process data to acquire individual's consent. On the other hand, the SPDI Rules provides particular guidelines in context to gather, store, process and protection of sensitive personal data or information (Sheetal Ramesh Nikam, 2024) [1].

The perception of social media is erroneous in India; due to this our legal system faces dual of protecting digital independence and creating liability. The Information Technology Act, 2000 and its succeeding amendments target to control cyber activities, but the growth in cybercrimes incidents discloses significant loopholes. This paper scrutinizes the legal framework related to cybercrime, estimates the accountabilities of social media intermediaries, and suggested measures to enhance answerability while maintain a balance between individual's rights and privacy (Dr. Saman Devgan, 2024) [2].

This research paper scrutinizes that how Indian legislative framework deals with the privacy issues and challenges in context with social media, the supervisory contests of implementing responsibility in case of worldwide technical organizations, and the proper enforcement of newly legislated Digital Personal Data Protection Act, 2023 (DPDP Act) (Aaditya Bhatt, et al., 2024) [3].

2. Historical Background

In human history the concept of privacy was deeply embedded, growing along with societal customs, technological improvements and legislative frameworks. Starting from the ancient developments the inviolability of home to the arrival of laws regarding the privacy in modern time period, the concept of privacy has experienced a philosophical conversion over the times. For instance, in prehistoric Rome, the word "domus" not only included the physical space of the household but also includes the unfringeable dominion of private autonomy and family integrity.

Likewise, the word "Hurma" in Islamic jurisprudence explained regions of privacy and humility, protecting individual self- respect and social accord. In 15th century the beginning of printing press indicated a new age of mass communication, stimulating old-dated ideas of privacy and redefining public discourse. With the growth of newspaper, magazines, and pamphlet's, individual is stuck with the pressure between the Freedom of Expression and the Right to Privacy placing the foundation for future considerations.

The 20th century observed the beginning of modern privacy laws and constitutional safeguards in response to the creation of innovative technologies and mass media. Right to privacy as an essential aspect of specific sovereignty is being observed in the landmark cases of "Griswold vs. Connecticut" and "Roe vs. Wade" along with leaving the way for further legal developments. In this digital era, the increasing growth in the social media platforms has presented new complications in context with privacy landscape, concealing the bridge between public and private sphere. While finding the historical development of privacy, from the ancient age to the modern digital age, we experienced important perceptions between the personal autonomy, societal standards, and technological evolution. The historical perception enlightens our knowledge regarding the modern challenges facing mass media and the right to privacy, emphasizing the requirement for a robust and interdisciplinary approach and legal frameworks while dealing with these intricate issues (Dr. Rekha Rani Sharma, 2023) [4].

3. Laws regarding to privacy and Social Media [3]

3.1 Digital Personal Data Protection ACT, 2023

In year 2023, the Indian Legislation has enacted a “Digital Personal Data Protection, Act” for the protection of fundamental right to privacy which is acknowledged by the Hon’ble Supreme Court of India. The said Act addresses the risks which is arising from the quick digitalization, and substitutes the out-dated provisions of the Information Technology Act, 2000. The objective of the DPDP Act is to regulate the gathering, storing and processing of individual’s personal data, it also protects citizens in case of data abuse and data violation, guaranteeing the rights to the individual regarding their data, and line up India’s legal framework with worldwide standards such as GDPR. The Act also creates a digital trust, guarantees liability of private organizations and government bodies, and also support India’s digital economy along with international co-operation.

4. Rights of Data Principles under Data Protection Laws

4.1 Right to Access

Under this right, Data Principals have an absolute right to acquire a clear and concise summary of their personal data which is being processed. They also have the right to request information regarding the data processing activities, for which purpose the said data is being processed, along with the information of all Data Fiduciaries and Data Processors with whom their personal data is being shared.

4.2 Right to Alter and Erasure

Data Principals have the right to request for the correction of erroneous or obsolete personal data. They have also the right to request for the deletion or erasure of their personal data, particularly in case when the said data is no more important and not fulfilling the purpose for which it was collected or when the Data Principal withdraws their consent.

4.3 Right to Complaint Redressal

The DPDP Act directs all the Data Fiduciaries to create an effective digital mechanism for the Data Principals to file a complaint or objection. Having an effective redressal mechanism, it is very easy for the users to file a complaint and get a solution within a reasonable timeframe. In case the Data Principal is not satisfied from the response of the Data Fiduciary, he can further approach its complaint to the Data Protection Board of India.

4.4 Right to appoint nominee

A Data Principal has the right to nominate another person on behalf of him to exercise their rights under the Act, in case when the Data Principal is being died or having incapable to exercise its right.

4.5 Right to withdrawal of consent

Under the Act, the Data Principal shall also have a right to withdraw consent anytime, but the condition is this that the consent shall be “free, definite, unconditional, informed and unambiguous”. The Act also states that, it must be very easy for the principal to withdraw consent same as when to give it. Once the consent is being withdrawn by the Data Principal, the Data Fiduciary instantly ceases to process their personal data except in cases where the processing is mandatory for some purpose or according to the law.

5. Obligations of Data Fiduciaries in context to Social Media Platforms

According to DPDP Act, social media platforms, the Data Fiduciaries are being obligated to safeguard individual’s data and sustain the rights of Data Principles. The prime duty of the Data Fiduciary includes

procure free and specific consent from the Data Principals before processing their personal data, guaranteeing data correctness, and executing strong security measures to avoid data breach. They are also obliged to maintain a clear and manageable grievance redressal mechanism and mandatory to delete data in case the specific purpose of processing has been achieved or when the Data Principal withdraws consent.

For main platforms “Significant Data Fiduciary” has been elected and performs such duties such as, appointing Data Protection Officer (resident of India), accompanying regular Data Protection Impact Assessments, and the most important employing an independent data auditor. The DPDP Act, also inflicts some stringent provisions on social media platforms regarding the data of children, eliminated targeted advertising and other detrimental practices regarding the children’s and users.

6. Landmark Privacy Judgments: The K.S. Puttaswamy judgements and its implications

In the landmark judgment of K.S. Puttaswamy (Retd.) vs. Union of India (2017) the Hon’ble Supreme Court of India necessarily renovates the purview of privacy in India. The said judgment established a statutory framework for dealing privacy concerns in this digital era through recognizing right to privacy as a fundamental right guaranteed under Article 21 of the Constitution of India.

The judgment also deeply affected social media regulations. It recognized that any violation of privacy must be considered after the triple test i.e. Legality, Necessity and Proportionality. This framework necessitates social media regulations to be reasonable and justified not only through the law but also through the perceptible need and judicious scope.

The Court’s legally recognition of informational privacy as a fundamental right has specifically important for social media platforms. It imposes the execution of severe data protection measures and impacts how these platforms gather, store, process and transmit individual’s information.

7. State Surveillance vs. Privacy Rights

In this digital era, it is very challenging to make a balance between individual privacy rights with reasonable state surveillance. The landmark judgment of Justice K.S. Puttaswamy case provides a legal framework for assessing surveillance measures, necessitating them to abide complex constitutional principles.

Law enforcement agencies while pursuing access to social media data for the purpose of investigation, they must fulfil these constitutional requirements. The consequences of this were the expansion of more complex procedures for the government to gain access of individual data, giving importance on necessity and proportionality.

The judgment also aimed the on-going dispute related to data encryption and to take access of personal communication on social media platforms by the government.

Case Law: Rajagopal v. State of Tamil Nadu, 1995 AIR 264

In the landmark case of Rajagopal vs. State of Tamil Nadu, 1995 the Hon’ble Supreme Court of India held that, the Right to Privacy is a crucial component of the Right to Life and Personal Liberty under the Constitution of India. The case highlighted the necessity of an accountable press that admire the privacy of every individual [2].

8. Constitutional Framework prevailing Social Media

8.1 Right to Privacy in the Social Media Era

In our Indian Constitution, the Right to Privacy is not been explicitly mentioned but through some judicial interpretation the said right has been recognized as a fundamental right under Article 21 of the Constitution of India. The landmark case of Justice K.S. Puttaswamy vs. Union of India (2017) has a specific importance regarding social media governance. The said judgment consider privacy as a fundamental right, including informational privacy, which directly controls how social media platforms gather, store, handle and process individual's data.

The recognition of informational privacy under the K.S. Puttaswamy case has evolved numerous complications regarding social media platforms:

The right regarding the sharing of personal information on social media platforms has been considered as an essential aspect of an individual privacy. Individuals have a significant control over their data which includes the right to delete or modify information which had been previously shared on social media platforms. The judgment also highlights the requirement of transparent data collection procedures and individual consent for processing of data.

Regarding social media platforms it is very essential to apply severe data protection measures to protect individual's privacy. It includes protection in case of illegal access, data violations, and illegal use of personal information. The statutory right to privacy creates compulsions on both public as well as private organizations to safeguard individual's data [3].

9. Constitutional and Legal Frameworks in India

9.1 The Information Technology Act, 2000

Section 66: Section 66 of the Information Technology Act, 2000 says that, if any individual person with dishonest or fraud intention does any act which damages the computer, computer system or computer network of any other person without the consent of that person. The guilty person will be awarded an imprisonment of maximum three years or with fine of five lakh rupees or with both.

Section 66 A: Section 66 A of the Information Technology Act, 2000 says that, if any individual person sends offensive message through the means of computer resources or communication devices. The guilty person will be awarded an imprisonment of maximum three years and with fine.

Section 66 B: Section 66 B of the IT Act, 2000 prescribe that, any individual person who with dishonest intention receives or retain any computer resource or communication device which he knows to be stolen. The accused person shall be punished with a maximum imprisonment of three years or with fine of one lakh rupees or with both.

Section 66 E: Section 66 E of the Information Technology Act, 2000 says that any individual person intentionally or knowingly taking, storing, publishing or transmitting the image of any person in his private area without his/her consent. The guilty person will be awarded an imprisonment of three years or two lakh rupees fine or with both.

Section 67: Section 67 of the Information Technology Act, 2000 says that any individual person having guilty intention publishes or transmits any material which is obscene in its nature. The guilty person in its first conviction shall be punished with an imprisonment of three years and with fine of five lakh rupees in second or subsequent conviction the imprisonment of five years and with ten lakh rupees fine.

Although, in the landmark case of Shreya Singhal vs. Union of India, 2015 Section 66A of the IT Act which criminalized illegal offensive messages online was struck down. It was a debate regarding freedom of speech versus regulation.

9.2 It Rules, 2021 (Intermediary Guidelines and Digital Media Ethics Code)

The IT Act, 2021 were introduced according to Section 79 of the IT Act, 2000 to increase intermediary responsibility. The said rules directed that:

- To safely and accurately handle individual's complaint, appointment of Grievance Officers.
- Deletion of illegal content within 36 hours after receiving of court's order or direction of the government.
- Positioning of mechanically programmed tools which helps in identification and removal of harmful content easily.

9.3 Bhartiya Nyaya Sanhita, 2023 (BNS)

The Indian Penal Code (now, Bhartiya Nyaya Sanhita, 2023) deals with various offences which is gradually being committed through social media platforms. The offences are:

- Defamation (section 499 IPC / section 356 BNS)
- Criminal Intimidation (section 503 IPC / section 351 BNS)
- Promoting enmity between different groups (section 153A IPC / section 196 BNS)
- Stalking (section 354D IPC / section 78 BNS)

These are some provisions which aim to control the misuse of online platforms in context of illegal activities [2].

10. Challenges in Safeguarding Privacy on Social Media

10.1 Legal and Technical Challenges

After the application of Aadhaar – social media linkage, various technical or procedural challenges have also arisen. The concern issues are related to data security, illegal access and the complications regarding managing cross-platform verification systems.

Legal concerns related to compulsory linkage have highlighted the probable violation of right to privacy and the principle of proportionality recognized in the K.S. Puttaswamy case. Judiciary must estimate that, whether such actions constitute a reasonable restriction on right to privacy [3].

10.2 Future recommendations and challenges

The growing arena of privacy laws and social media leads to create new challenges and chances. When "Personal Data Protection Bill" was enforced, it will require substantial modifications from both social media platforms and individuals.

Social media platforms must include advanced compliance requirements while preserving individual's experience and invention. The advanced compliance requirement includes new measures for data protection, individual's consent management, and protection of privacy.

The amalgamation of growing technologies such as Artificial Intelligence and Face Recognition on social media portals will evolve new privacy concerns which require cautious consideration under the legal framework [3].

10.3 Express Informed Consent

Press media or reporters should require clear informed consent before publishing or broadcasting personal information regarding the individuals. The consent includes full permission regarding full disclosure about the intentional use of personal information.

10.4 Cross-Border Data Storage: International Jurisdictional Issues

A huge segment of injurious content initiates from the beyond Indian jurisdiction, that creates difficulty for enforcement agencies and regulations in context to domestic laws.

10.5 Government Monitoring: According to Indian Telegraph Act and Information Technology Act, 2000 extensive intervention powers, that traces that mandates end-to-end encryption.

10.6 Weak Execution Process: Deficiency of resources by the regulatory authorities liable international organizations answerable, leads to an absence of proper action remedies.

10.7 Struggle between Rights: Creates conflicts between the privacy under defamation and free speech, revenge pornography and cases related to doxxing and also between the national security vs. privacy under misinformation and cyber terrorism cases.

11. Comparative Study

11.1 European union (GDPR) (Sanjeev Kumar, et al., 2025) [5].

Indian privacy framework has evolved in a worldwide environment that is subjugated by extensive regulatory organizations in context to digital privacy. European's Union, GDPR (General Data Protection Regulation) had a surging effect on the legal developments in India. The report of Srikrishna Committee strengthened the draft related to data protection legislation in India, clearly recognized its support on GDPR, including the concept related to data minimization and specific limitation also the rights related to Data Portability. The impact of the GDPR was clearly ostensible in the landmark case of K.S. Puttaswamy, in which Justice Chandrachud while interpreting the principles of informational privacy raised European privacy legal framework such as in case of Google Spain SL vs. AEPD (2014).

- Strong rights for individuals: access, rectification, erasure ('right to be forgotten').
- Heavy penalties for violations (up to 4% of global turnover).
- Independent supervisory authorities with enforcement powers.

11.2 United Kingdom (UK)

The UK and India both have a different data protection framework even though both countries are inclined to global standards. The United Kingdom works under the UK GDPR and the Data Protection Act, 2018, a system which is directly influenced by the EU's comprehensive data privacy laws. The legal framework of the UK is comparatively more flexible.

Personal Data Protection Law: UK

In context to data privacy, the United Kingdom has the most vigorous personal data privacy legal framework, specifically when it separated from the European Union. Even though the GDPR not legally bind the UK, because the UK separately enacted his version known as UK GDPR together with Data Protection Act, 2018.

GDPR and Data Protection Act 2018: UK

The UK based GDPR looks like EU's GDPR, containing most of the similar legal provisions in context to data subject's rights, data consent, and data processing, along with punishments in case of non-compliance of the provisions. Some important provisions are:

Rights related to Data Subject: The UK GDPR provides rights of Data Subjects which are equivalent to EU GDPR provisions through providing the access rights and the power to alter and remove such data.

Accountability: According to UK GDPR, Data Controllers must have to comply the statute through clearly revealing their data processing operations.

International Data Transfers: As per the UK GDPR, they have adopted a mechanism which allows them to transfer personal data outside the country, bound by certain protections such as Standard Contractual Clauses (SCCs).

Penalties for Non-compliance: If any organization fails to comply with the UK GDPR they will get a fine up to £17.5 million or 4% of their global turnover, whichever is higher.

The Data Protection Act, 2018 enhances the UK GDPR through dealing with UK specific areas, such as the handling and processing of criminal conviction data and the role of the Information Commissioner's Office (ICO) i.e. the UK's data protection authority.

11.3 India

In spite of these influences, Indian courts have tended to adopt instead of follow the European approach. In the landmark case of Internet Democracy Project vs. Union of India (2022), High Court of Delhi acknowledge that, "even though there are various international frameworks are there that provides valuable and informative guidance, privacy is considered as a circumstantial right which cannot be applied consistently across changing social contexts" [5].

DPDP Act is comparatively weaker in context to broad exemptions and limited enforcement than GDPR because DPDP Act limited towards starting framework.

Due to the rapid & continuous digital developments, Indian legislation has been continuously placing its efforts to confront the challenges coming its way. In past few years, Indian legislations passed some statutes to regulate social media in India. The Information Technology Act, 2000 controlled the way and was tailed by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Wide range of guidelines has been provided by these rules for the intermediaries. In context to these rules, the social media platforms have been obligated to continuous monitoring on the content being posted by the individuals and also have the power to remove the content which is considered to be harmful such as defamatory statements, obscene materials, illicit publications, hatred speech and ingredients related to child sexual abuse etc.

The recent legal statute was passed is Digital Personal Data Protection Act, 2023 have an objective to control the processing of digital personal data of the individual who are involving in such online activities. The Act also deals with the concept of free speech in various essential ways, specifically when to create a balance between protecting personal data and permitting open communications on the internet. Indian legal framework is much more obstructive in nature showing its distinctive legal and social context (Akriti Shashank, et al., 2025) [6].

12. Policy recommendations

- Establishment of purely self-regulating data protection authority along with financial and functional autonomy.
- Constricted the scope of government exemptions under DPDP Act to avoid misuse.
- Obligate transparency reports by the social media organization in relation to data usage and government requests.
- Encourage privacy in context to platform architecture.
- Bring together digital literacy programs to aware citizens.
- Prescribe effective remedies, which include class actions and retributory damages.
- Support data localization with the protection against foreign abuse of data, while ignoring unnecessary control of the state.

13. Conclusion

In India, the recognition of right to privacy as a fundamental right has placed the basis for robust digital rights. But, the authenticities of mass surveillance, weak enforcement and the domination of worldwide social media platforms continue to weaken active privacy protection. The DPDP Act, 2023 signifies growth but rests unsatisfactory without strong enforcement and judicial inaccuracy. Over the next few years, India was aimed to maintain a balance between inspiring digital invention and defending citizen's fundamental rights. Firming up privacy protections regarding social media is not only a legal necessity but also an independent imperative to safeguard dignity, autonomy, and independence in the digital age.

This connection of privacy laws and social media signifies a crucial area of legal and technological developments. The achievement of India's privacy framework will be interdependent on discover the balance between safeguarding individual's privacy rights and allowing the valuable features of social media platforms [3].

References

1. Sheetal R.N., "User Consent and Data Protection: Legal Challenges on Social Media Platforms", International Journal of Research Publication and Reviews, September 2024, 5 (9), 1421-1427. <https://ijrpr.com/uploads/V5ISSUE9/IJRPR33198.pdf>
2. Dr. Saman D., "Cybercrime and social media platforms: Legal accountability in the Indian context", International Journal of Law, Justice and Jurisprudence, November 2024, 4 (2), 325-327. <https://www.lawjournal.info/article/159/5-1-7-835.pdf>
3. Aaditya B., Chandni J., "BOOKLET ON SOCIAL MEDIA REGULATIONS IN INDIA", Bhatt & Joshi Associates, 2024, 1-107. <https://bhattandjoshiassociates.s3.ap-south-1.amazonaws.com/booklets+%26+publications/Social+Media+Laws+in+India+-+Compliance+%26+Cybercrime+Prevention.pdf>
4. Dr. Rekha R. S., "Media and the Right to Privacy, the Incursion of Social Media", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), December 2023, 3 (1), 693-699. <https://www.ijarsct.co.in/A14100B.pdf>
5. <https://www.drishtias.com/daily-updates/daily-news-analysis/sc-calls-for-regulating-social-media?hl=en-US#:~:text=Cross%2DBorder%20Jurisdictional%20Issues%3A%20A,regulation%20difficult%20under%20domestic%20law>
6. Sanjeev K., Prof Shashi P., "Right to Privacy in the Age of Social Media: An Analysis of Indian Jurisprudence", Journal of Legal Studies, international Refereed Peer-Reviewed Journal, August 2025, 13(1), 1-10. https://www.researchgate.net/publication/394520562_Right_to_Privacy_in_the_Age_of_Social_Media_An_Analysis_of_Indian_Jurisprudence
7. Akriti S., Prof. Dr. Monika R., Sweksha B., "Social Media And The Right To Free Speech In India: Constitutional Challenges, Legal Boundaries, And The Role Of Judicial Oversight In The Digital Era", International Journal of Creative Research Thoughts (IJCRT), April 2025, 13 (4), 926-932. <https://ijcrt.org/papers/IJCRT2504458.pdf>
8. "Personal Data Privacy Laws In USA, UK & India" (Blog) <https://thelegalschool.in/blog/personal-data-privacy-laws?hl=en-US>

9. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. <https://lawlex.org/lex-bulletin/case-summary-k-s-puttaswamy-retd-v-s-union-of-india-2017/18929>
10. The Information Technology Act, 2000. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
11. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. <https://mib.gov.in/sites/default/files/2024-02/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf>
12. The Digital Personal Data Protection Act, 2023. <https://indiankanoon.org/doc/3510545/>
13. European Union General Data Protection Regulation (GDPR), 2016. <https://gdpr-info.eu/#:~:text=Here%20you%20can%20find%20the%20official%20PDF%20of,of%20the%20GDPR%20are%20linked%20with%20suitable%20recitals.>