European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

The Impact of Social Media on Privacy Rights: A Legal Evaluation

Garima[1*]
[1]Research Scholar Department of School of Law, Sushant University, Gurugram, India
*Corresponding Email: garimasingh.nidhi02@gmail.com

Dr. Shreya[2]
[2]Assistant Professor, Department of School of Law, Sushant University, Gurugram, India
Email: Shreya@sushantuniversity.edu.in

ABSTRACT

This study investigates the implications of social media facilities for people's privacy rights in India, adjusting its lens to the legal, policy and regulatory perspectives. In a society heavily dependent on digital platforms for communication, commerce, and social engagement, widespread collection, processing, and sharing of personal information pose serious threats to privacy. The paper will look at existing legal data protection and privacy frameworks in India currently governing data (the Information Technology Act, 2000, the IT Rules, 2021 and the Digital Personal Data Protection Act, 2023). But it evaluates the extent to which these laws effectively address escalating threats from private sector data practices and government surveillance. The article concludes with legal and policy recommendations to enhance privacy safeguards and to secure a balanced and rights-respecting digital milieu in India.

Keywords: *Privacy Rights, Social Media, Data Protection, Digital Surveillance and Information Technology Act*

INTRODUCTION

The digital revolution has brought about transformational change in various forms of interacting, communicating, sharing knowledge, and participating in social, political, and economic life[1]. At the heart of this transformation, is the saturation of social media platforms that have become geographically-specific everyday destinations. Nowhere is the impact of social media more profound than in India, where a significant and increasing part of the population is connected digitally. And far from just being tools of social interaction, these platforms — which include Facebook, Instagram, WhatsApp, Twitter and YouTube — have turned into gravitational forces in the world of information, politics, marketing and even civic involvement. Yet for all the wonderful contributions social media has made and continues to make, serious questions are being raised — currently and in the future — about fast weakening national privacy protections and correspondingly quickly weakening public respect for privacy[2].

Background and problem of the study

Impact of social media in India is huge and it has revolutionized the way we communicate, express ourselves and share information Like the rest of the world, Indian social media users are hooked on to services like Facebook, Instagram, WhatsApp and Twitter – all day, every day. But along with this digital change, we have also witnessed growing fears of privacy rights erosion. Personal data is gathered, saved, processed, and frequently misused without informed permission of users. Given the digital divide in a populous and diverse country, the low digital literacy and developing legal approach, privacy of people's digital identity is more and more difficult to protect. In this digital world, social media has turned into a strong means of communication and information dissemination, however it also raises background privacy concerns. In India, an evolving environment in which there is no robust, enforceable law to protect data and increased digital surveillance and opaque data-handling practices by social media companies leaves a legal and ethical vacuum[3]. The current legal

framework is a patchwork and is not equipped to deal with the rapidly evolving technology landscape and the transnational character of data flows.

Objective of the study

1. To critically examine the existing legal and constitutional framework governing privacy rights in India in the context of social media usage, with a focus on the effectiveness and adequacy of current laws such as the Information Technology Act, 2000, the IT Rules 2021, and the Digital Personal Data Protection Act, 2023.
2. To analyze the impact of social media platforms on individual privacy rights in India by evaluating judicial interpretations, state surveillance practices, and corporate data policies, and to propose legal and policy reforms to enhance privacy protection in the digital age.

RESEARCH METHODOLOGY

This paper follows the doctrinal approach of legal research to analyse existing statutory provisions, policy structures, academic discussions and regulation framework pertaining to privacy rights and social media in India. Secondary sources such as journal articles, government reports and international legal instruments are discussed to explore the development and limitations of PHIA legal protections as they exist now. The research is qualitative in nature and is an attempt to analyse the suitability of the Indian laws with respect to privacy concerns in Digital era.

The Legal and Constitutional Framework Governing Privacy Rights in India in the Context of Social Media Usage

In the age of digital privacy has become one of the most debated and critical human rights, all the more so with the mushroom growth of social media platforms that create, collect and deal with masses of user data every day[4]. In India, the convergence of rights to privacy with social media use has seriously questioned the adequacy of the already existing legal and constitutional mandates to safeguard personal information and uphold autonomy online. India's current regulatory framework is anchored in the Information Technology Act, 2000[5], the IT Rules, 2021 and the Digital Personal Data Protection Act, 2023[6].

The Constitutional Backdrop: Recognizing Privacy as a Fundamental Right

The right to privacy has not always been explicitly subsumed by the Indian constitution. Courts have moved slowly but inexorably to recognize this as an integral part of the guarantee in Article 21 itself, which gives the right to life and personal liberty. The landmark Supreme Court judgment of the Justice K.S. Puttaswamy (Retd.) vs Union of India (2017)[7], the Supreme Court held that right to privacy is a fundamental right guaranteed under the Indian Constitution.

The Information Technology Act, 2000: An Outdated Framework in a New Digital Reality

The IT Act– the first serious step the Indian government took to regulate cyberspace in the country– came into effect on 17 October 2000[8]. The IT Act, which was primarily aimed at encouraging e-commerce and deterring cybercrime, has only few provisions on privacy. Section 43A requires organizations handling any sensitive personal information to implement such security practices as are reasonable, whereas Section 72A punishes unauthorized disclosure of "personal information". "But those measures are not sufficient, and they do not adequately address the larger issue of how to protect user data in the day of Facebook."

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

The IT Rules, 2021: A Controversial Attempt at Accountability

In an effort to plug some of these lacunae in the IT Act, the Ministry of Electronics and Information Technology issued the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[9]. These guidelines have been framed to regulate the operations of intermediaries such as social media intermediaries, digital news and OTT Platforms. They also impose on social media intermediaries the obligation of due diligence, hiring of grievance officers and take down of content requests within specified period.
The IT Rules also enable the government to order platforms to take down content that it believes undermines national security, public order or decency, all without the need for independent judicial oversight. This creates the possibility for abuse and endangers the data and speech of users. While the rules aim to check the power of big tech companies, they also raise questions about surveillance, censorship and the loss of privacy. These rules are costly for both platforms and users to comply with, and yet they provide few, if any, rights-based safeguards, and little transparency, regarding state surveillance in the context of social media.

Digital Personal Data Protection Act, 2023[10]: Promise and Pitfalls

A landmark addition to the privacy jurisprudence of India is the Digital Personal Data Protection Act (DPDP) 2023. This law is designed to put each of India privacy standards on par with global data protection norms by enunciating the data protection principles and creating a regulatory capacity to enforce them. The Act is based on the core tenets of purpose limitation, storage limitation, data minimisation and consent for processing of personal data. It introduces the idea of "Data Fiduciaries" that are responsible for protecting the "Data Principals" (users) and grants the individual rights to access, correct, and delete their personal data.

Challenges in Implementation and the Need for a Comprehensive Data Governance Framework

However, beyond statutory provisions, the realization of privacy rights in India is hindered by systemic and structural issues. There is an institutional weakness and lack of competence in implementing authorities. While doing so, COSH finds that the cyber cells, judicial officers, and regulators remain incapable of understanding and resolving complex data privacy concerns, more so in the background of social media[11]. What is more is that Indian users are often not aware of their digital rights, while grievance redress mechanisms are either not accessible or ineffective." A significant issue is the lack of a single, coherent digital policy that balances privacy, cyber security, free speech and national security. Disintegration under various legislations and rules has resulted in a crazy-quilt approach which inevitably causes wide variations in interpretation[12].

Rights-Respecting Digital Ecosystem

Finally, this Comment has found that while India's legal and constitutional framework for privacy rights has advanced there still remains a gap that needs to be addressed to cover the intricate issues brought on by the use of social media. The normative grounding is provided by the constitutional right to privacy. However, the legislation such as the IT Act 2000, IT Rules 2021, DPDP Act 2023 (while progressive in parts) is unable to deliver comprehensive, transparent and rights based data governance[13].

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

Impact of Social Media Platforms on Individual Privacy Rights in India

Social media networks have reshaped the face of communication, information sharing, and public debate for the digital age[14]. In a country of more than a billion people, many Indians freely share with millions of strangers their dreams and desires on social media platforms like Facebook, Instagram, X (previously known as Twitter) and WhatsApp, and the lines between private and public lives have grown hazy.

Judicial Interpretations: Expanding the Scope of Privacy Rights

The altered path of the juridical process leading to the Indian recognition of privacy as a constitutional right has been tortuous and delicate. Landmark judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[15] as a result of that Judgment had set the jurisprudence on digital privacy in India in motion. The Supreme Court ruled unanimously that the right to privacy is an intrinsic part of the right to life and personal liberty on 21 Article of the Indian Constitution. Crucially, the verdict noted that privacy includes informational self-determination, data protection and freedom from surveillance.

Corporate Data Policies: Commercial Exploitation and Consent Fatigue

The business model of social media is about Surveillance Capitalism: turning personal data into a commodity for targeted advertising, and behavioral engineering[16]. Companies like Meta, Google and ByteDance amass and analyze reams of personal information — including location data, browsing habits, interaction records and private messages — often with minimal disclosure or real user consent.

Until 2023, India had no strong data protection laws, which allowed only corporate profiteers to capture, store, and share user data any which way they pleased. The 2021 Facebook–Cambridge Analytica scandal demonstrated how third-party apps could obtain huge datasets without users' awareness or meaningful consent. Likewise, TikTok and other platforms have faced allegations that they secretly harvested biometric data, sparking investigations by regulators and courts.

While the DPDP of 2023 itself aims to regulate these corporate behaviours by imposing purpose limitation, informed consent, and a user's right to correction and erasure, there are still some gaps[17]. The Law does not have a stringent data minimization requirement, and allows for broad exceptions on behalf of government offices. Nor does it sufficiently tackle algorithmic decision-making, data brokerage, or dark patterns that nudge users into behavior on social media.

Proposed Legal and Policy Reforms for Enhanced Privacy Protection

India will need a comprehensive framework in order to protect privacy not just from state surveillance and corporate exploitation, but also from weak enforcement practices. The subsequent reforms have been suggested:

Enactment of a Comprehensive Surveillance Law

There is a need in India to have a dedicated Surveillance Regulation Act, providing a full statutory framework, limits in which surveillance can be conducted, oversight by the judiciary and transparency and accountability safeguards[18]. The law should also mandate that agencies get judicial warrants for access to private communications on social media and create a public registry of surveillance requests and authorizations.

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

Amendments to the DPDP Act, 2023

The DPDP Act requires to the amended to[19]:

1. Repeal or cap the state's exemptions.
2. Mandate responsibilities for social media platforms including a requirement to disclose their algorithms, information profiling users and third parties with the ability to distribute user information.
3. Mandate data protection impact assessments (DPIAs) for high-risk processing activities, including behavioral advertising.
4. Add new rights, such as a "right to object to automated processing" and a "right to data portability."

Regulation of Algorithmic Governance

The government should set up an enzyme body for algorithmic accountability to audit social media algorithms that impact privacy, free speech or access to information. It should have rules that force platforms to tell us how content is ranked, or moderated, or censored and for us to be allowed to opt out of behavioral personalization.

Strengthening the Data Protection Board

The independence of the Data Protection Board should be guaranteed by the DPDP Act through legislatively safeguarding it[20]. The Board's appointment process should be protected from the influence of the executive and the Board should have the authority to investigate and punish privacy breaches by both public and private actors.

Enhancing Public Awareness and Digital Literacy

Law alone cannot protect privacy; public understanding is key. It is the role of the government and civil society to sustain investments in digital literacy campaigns that teach users about the risks of privacy, their rights to consent and safer use of social media. Schools should have curriculums on digital rights and data ethics.

Mandating Privacy by Design and Default

Regulations ought to obligate social media companies to design privacy protections into their products, making use of a range of available privacy-enhancing technologies like end-to-end encryption, anonymization, and differential privacy[21]. Design platforms from which the users have control, data is minimized and where by default it has to be actively disabled to share and track.

International Data Transfer Standards

With the internet having no territories, India has to create a framework for transborder data transfer that strikes a balance between the protection of privacy and the cooperation of the global community. Data sharing terms with foreign regulators should include robust data protection clauses, localization requirements should be aligned to our constitutional privacy guarantees. To protect privacy in an age of social media, a robust legal reform, institutional mechanism and public discourse is needed in India. We need sound surveillance law, stronger provisions for data protection, and mechanisms for algorithmic accountability.

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

Inclusion and Exclusion Criteria

Inclusion Criteria

This study comprises all the key aspects to comprehend the implications of social media on the rights to privacy at the personal level in India. It incorporates:

1. **Judicial Interpretations**: Notable ureka decisions, including Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[22] which held that privacy is a fundamental right, are there in order to pencil in constitutional protections.
2. **Legal Regime:** Various Indian legislations such as the Information Technology Act, 2000, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[23] and the Digital Personal Data Protection Act, 2023[24] will be examined in order to determine their efficacy in relation to digital privacy.
3. **Policy Implications:** The paper offers prescriptive legal and regulatory changes to strengthen digital privacy protections for Indian social media users.

Exclusion Criteria

There are some things I deliberately left out to simplify and deepen the discussion:

1. Privacy concerns that thing happen (bank, health records, telecom metadata etc.) are excluded as long as not intersected with the use of social media.
2. Comparative international systems of law receive relatively little attention, except as they are contextually relevant for proposed reforms.
3. Non-digital privacy issues (e.g., physical or locational privacy that is not related to social platforms) are out of scope.

CONCLUSION

The ability to reconcile the effective use of social media and the right to individual privacy in India is a highly complex and emergent area of law. As digital platforms have exploded in number, anxiety about the safety of personal data, illicit gaze monitoring and corporate data policies have grown. Judicial decisions, including Puttaswamy, have been instrumental in establishing the constitutional underpinnings by recognising the right to privacy as inherent in the concept of right to life and personal liberty in Article 21. But the current legal landscape—encompassing the Information Technology Act, 2000, the IT Rules, 2021, and the gradiently-recently passed Digital Personal Data Protection Act, 2023—though progressive in aspirations, suffers from inadequacies in enforcement, overreach of state surveillance powers, lack of agency for users in terms of their data. Social media represent a duality, allowing as they do for free speech and connections, while also accumulating and committing to market personal data (and on occasion to exploit it), with little transparency and even less accountability. What's more, the state's growing use of surveillance technologies with little judicial scrutiny plays into the disproportionate formula of the balance between national security and civil liberties. To meet these challenges, India needs to bolster its regulatory systems, improve accountability within institutions, promote transparency in all data practices, both public and private – and harmonise its laws with global privacy standards. Protecting privacy in an online world is not only a legal issue, but also a matter of democracy, requiring ongoing scrutiny, flexible policy strategies and rights-respecting digital governance.

REFRENCES

1. L Caruso, 'Digital Innovation and the Fourth Industrial Revolution: Epochal Social Changes?' (2018) 33 *AI & Society* 379.
2. LB Andrews, *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* (Simon and Schuster 2012).
3. K Srilakshmi and JS Harshitha, 'Guardians of Privacy: Navigating the Complexities of Data Protection in India's Digital Epoch' (2024) 4 *Legal Lock Journal* 25.
4. C Nyst and T Falchetta, 'The Right to Privacy in the Digital Age' (2017) 9(1) *Journal of Human Rights Practice* 104.
5. Information Technology Act 2000.
6. Digital Personal Data Protection Act 2023 (No 22 of 2023).
7. *K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.
8. H Ebert, 'Hacked IT Superpower: How India Secures Its Cyberspace as a Rising Digital Democracy' (2020) 19(4) *India Review* 376.
9. S Ashwini, 'Social Media Platform Regulation in India – A Special Reference to The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' (2021) *Perspectives on Platform Regulation* 215.
10. K Sundara and N Narendran, 'The Digital Personal Data Protection Act, 2023: Analysing India's Dynamic Approach to Data Protection' (2023) 24(5) *Computer Law Review International* 129.
11. O Vasylchyshyn, L Storozhenko, T Babkova, V Kuchmenko and V Kovalchuk, 'Social Media as a Factor in the Transformation of Public Administration, Justice and Legality' (2024) 7 *Multidisciplinary Reviews*.
12. AV Stearns, 'Patch by Patch: North Carolina's Crazy Quilt of Campaign Finance Regulations' (2018) 40 *Campbell Law Review* 669.
13. SMPJ Gomes, *EU Personal Data Protection Standards Beyond Its Borders: An Analysis of the European External Governance through GDPR on Data Protection Laws in the ASEAN Region* (Master's thesis, 2024).
14. L Baruch and others, *Social Networking: Redefining Communication in the Digital Age* (Rowman & Littlefield 2016).
15. *K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1
16. SM West, 'Data Capitalism: Redefining the Logics of Surveillance and Privacy' (2019) 58(1) *Business & Society* 20.
17. D Kumar, G Kaur, A Srivastava, A Ghosh and S Ghosh, 'The Ethical and Regulatory Challenges of Consumer Privacy in the Digital Era' in *AI Marketing and Ethical Considerations in Consumer Engagement* (IGI Global Scientific Publishing 2025) 173.
18. D Kumar, G Kaur, A Srivastava, A Ghosh and S Ghosh, 'The Ethical and Regulatory Challenges of Consumer Privacy in the Digital Era' in *AI Marketing and Ethical Considerations in Consumer Engagement* (IGI Global Scientific Publishing 2025) 173.
19. AK Bisht and NS Sreenivasulu, 'Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023' in *Data Privacy—Techniques, Applications, and Standards* (IntechOpen 2024).
20. AK Bisht and NS Sreenivasulu, 'Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023' in *Data Privacy—Techniques, Applications, and Standards* (IntechOpen 2024).
21. N Kaaniche, M Laurent and S Belguith, 'Privacy Enhancing Technologies for Solving the Privacy-Personalization Paradox: Taxonomy and Survey' (2020) 171 *Journal of Network and Computer Applications* 102807.
22. ibid
23. *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021* (India).
24. ibid