Journal of Advances and Scholarly Researches in Allied Education
Vol. 22, Issue No. 01, January-2025, ISSN 2230-7540

DOI: https://doi.org/10.29070/zr35bw04

Check for updates

The Evolution and Protection of Privacy as a Fundamental Right in India: Constitutional Milestones, Judicial Interpretations, and Contemporary Challenges

Kirtika Sahu [1] * , Dr. Rakesh Kumar Pandey [2]

1. Research Scholar Department of Law CSJM University, Kanpur, U.P., India
kirtika.s9804@gmail.com ,
2. Professor, Department of Law CSJM University, Kanpur, U.P., India

Abstract: The constitutional recognition of privacy in India has undergone a significant transformation, evolving from implicit acknowledgments within Article 21 to explicit validation through landmark judicial pronouncements. This review traces the constitutional journey of privacy in India, highlighting key judicial interpretations, legislative actions, and the interplay with societal norms. It examines the pivotal Supreme Court judgment in Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017), which solidified privacy as a fundamental right, and explores subsequent legal and legislative developments. The review also addresses contemporary challenges posed by technological advancements, digital surveillance, and data protection, emphasizing the need for adaptive legal frameworks and robust enforcement mechanisms. By analyzing the dynamic interaction between the judiciary, legislature, and societal changes, this paper underscores the ongoing efforts and future directions necessary to uphold privacy as a cornerstone of personal liberty in India.

Keywords: Privacy, India, Article 21, Puttaswamy judgment, data protection, digital surveillance, Personal Data Protection Bill

X

INTRODUCTION

Privacy, though not explicitly enumerated in the original text of the Indian Constitution adopted in 1950, has emerged as a fundamental right through a dynamic interplay of judicial interpretation, legislative action, and evolving societal norms. This evolution reflects a gradual yet steadfast recognition of privacy's paramount importance within the constitutional framework of India. Article 21 of the Indian Constitution, which guarantees the protection of life and personal liberty, has been instrumental in this journey, serving as the cornerstone for privacy jurisprudence. This review explores the constitutional trajectory of privacy in India, highlighting key judicial pronouncements, legislative measures, and the contemporary challenges that shape its protection.

The significance of privacy in the modern era cannot be overstated, especially with the advent of digital technologies that permeate every aspect of personal and professional life. The transformation from viewing privacy as a mere facet of personal liberty to recognizing it as an intrinsic right reflects broader global trends and India's commitment to upholding human dignity and autonomy. This paper delves into the historical context, judicial milestones, legislative advancements, and the multifaceted challenges that India faces in safeguarding privacy in the digital age.

Historical Journey of Privacy in Indian Constitutional Law

Initially, Article 21 was interpreted narrowly, focusing primarily on safeguarding individuals from physical harm and ensuring due process. Early judicial stances, exemplified by cases such as *Kharak Singh vs. State of Uttar Pradesh* (1962)[1] and *Mohammed Ashfaq v. State of Punjab* (1984)[2], confined the scope of personal liberty to preventing unlawful detention and protecting against state overreach. Although these cases did not explicitly address privacy, they implicitly recognized the importance of personal space and freedom from arbitrary interference, laying the foundational groundwork for privacy considerations within the broader ambit of personal liberty (Bhatia, 2014).

I n *Kharak Singh*, the Supreme Court emphasized the protection against unlawful detention, which indirectly safeguarded aspects of personal freedom. Similarly, *Mohammed Ashfaq* highlighted the necessity of fair procedure, ensuring that state actions do not infringe upon individual liberties without due process. These early interpretations set the stage for a more expansive view of Article 21, paving the way for privacy to be recognized as an essential component of personal liberty.

Over the decades, the Supreme Court of India adopted a more expansive view of Article 21, encompassing broader aspects of personal liberty, including the right to privacy. This incremental approach allowed the judiciary to adapt to changing societal needs and technological advancements that increasingly threatened individual privacy. The Court began to interpret Article 21 to include informational privacy, bodily integrity, decisional autonomy, and territorial privacy, aligning with global human rights discourses and international legal principles (Pertin & Singh, 2022[3]; Jha, 2023[4]).

EVOLUTION THROUGH JUDICIAL INTERPRETATIONS

The evolution of privacy as a fundamental right in India can be traced through various judicial pronouncements that expanded the interpretation of Article 21. The judiciary employed a progressive approach, recognizing privacy's multifaceted nature and its critical role in safeguarding individual autonomy and dignity.

Informational Privacy: The protection of personal data and prevention of unauthorized surveillance became paramount as digital technologies advanced. Cases addressing unauthorized data collection and breaches highlighted the need for stringent safeguards to protect individuals' informational privacy (Chatterjee, 2019)[5].

Bodily Privacy: Ensuring bodily autonomy and protecting individuals from invasive procedures underscored the importance of bodily integrity as a facet of privacy. Judicial decisions emphasized the necessity of consent and the right to make personal decisions without undue interference (Acharya, 2015)[6].

Decisional Privacy: Upholding the freedom to make personal choices, whether related to marriage, lifestyle, or reproductive rights, underscored decisional autonomy. The judiciary recognized that personal decisions are integral to an individual's sense of self and dignity (Singh, 2021)[7].

Territorial Privacy: Protecting personal space from intrusion, whether by state or non-state actors,

highlighted the significance of territorial privacy. Cases involving unauthorized surveillance and encroachment into personal spaces reinforced the need for robust protections against such intrusions (Bhatia, 2014)[8].

Landmark Judgment: Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017)

A pivotal moment in India's constitutional journey of privacy was the *Justice K.S. Puttaswamy (Retd.) vs. Union of India* (2017) judgment. The Supreme Court unequivocally declared the right to privacy as an intrinsic part of the right to life and personal liberty under Article 21. This unanimous verdict solidified privacy's constitutional status and provided a comprehensive framework for its protection.

The Court's analysis encompassed various dimensions of privacy, including:

Informational Privacy: Protection of personal data and prevention of unauthorized surveillance were emphasized, recognizing the challenges posed by digital technologies and mass data collection (Acharya, 2015)[9].

Bodily Privacy: Safeguarding individuals from invasive procedures and ensuring bodily autonomy were highlighted as essential components of privacy (Yadav & Varshney, 2024)[10].

Decisional Privacy: Upholding the freedom to make personal choices without undue interference was recognized as a critical aspect of individual autonomy (Bisht & Sreenivasulu, 2024)[11].

Territorial Privacy: Protecting personal space from intrusion by state or non-state actors was reaffirmed, ensuring that individuals are free from unwarranted surveillance and encroachments (Jha, 2023)[12].

The *Puttaswamy* judgment integrated international legal principles from instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, tailoring them to India's unique socio-cultural and legal context. This synthesis ensured that privacy was recognized not only in principle but also in practice, addressing specific challenges like digital surveillance and data breaches (Acharya, 2015)[13].

JUDICIAL REASONING AND IMPLICATIONS

The Supreme Court, in its reasoning, underscored the indivisible nature of fundamental rights, emphasizing that the right to privacy is essential for the enjoyment of other fundamental rights. The Court also highlighted the role of privacy in fostering human dignity, autonomy, and individuality, which are cornerstones of a democratic society (Pertin & Singh, 2022)[14].

The implications of the *Puttaswamy* judgment are profound. It mandated that any state action infringing upon privacy must meet the standards of legality, necessity, and proportionality. This framework ensures that privacy violations are scrutinized rigorously, balancing state interests with individual rights (Chatterjee, 2019)[15].

Post-Puttaswamy Developments: Judicial and Legislative Responses

Following the *Puttaswamy* judgment, privacy rights in India have seen significant judicial affirmations and legislative initiatives. The Supreme Court has consistently upheld and expanded the principles established in *Puttaswamy*, reinforcing privacy as a cornerstone of personal liberty and human dignity.

Judicial Affirmations

Subsequent Supreme Court cases have built upon the *Puttaswamy* framework, addressing various facets of privacy in different contexts. For instance, cases related to digital privacy, data protection, and surveillance have emphasized the necessity of robust legal safeguards to protect individuals from invasive state actions and corporate malfeasance. The judiciary has also addressed issues like biometric data collection, surveillance in public spaces, and the right to be forgotten, ensuring that privacy protections evolve in tandem with technological advancements (Bisht & Sreenivasulu, 2024)[16].

Legislative Initiatives

Legislatively, the introduction of the Personal Data Protection Bill exemplifies the commitment to creating a structured framework for data privacy. Inspired by the *Puttaswamy* judgment and the European Union's General Data Protection Regulation (GDPR), the bill addresses issues such as data collection, processing, storage, and individuals' rights to control their personal information (Vashisht, 2023)[17].

The Personal Data Protection Bill delineates responsibilities for data fiduciaries, outlines the rights of data principals, and establishes mechanisms for data protection authorities to enforce compliance. Key provisions include:

Consent Mechanism: Ensuring that individuals provide informed consent before their data is collected or processed.

Data Minimization: Limiting data collection to what is necessary for the intended purpose.

Right to Access and Correction: Allowing individuals to access their data and request corrections if necessary.

Data Breach Notification: Mandating timely notifications to affected individuals in case of data breaches.

These legislative measures align with global best practices, providing a comprehensive framework to safeguard data privacy in India's increasingly digital economy (Gupta, 2024)[18].

CONTEMPORARY CHALLENGES TO PRIVACY IN INDIA

Despite significant strides, India faces numerous contemporary challenges that undermine the effective protection of privacy:

Digital Surveillance and Data Privacy: Government initiatives like Aadhaar have streamlined service delivery but raised concerns about data security, informed consent, and potential misuse of personal information (Beduschi, 2019). The vast scale of data collection makes individuals vulnerable to breaches and unauthorized access, necessitating stringent regulatory frameworks (Vashisht, 2023)[19].

The Aadhaar project, while innovative in providing a unique identification system, has been criticized for potential privacy infringements. Issues such as data breaches, lack of consent in data collection, and insufficient safeguards have sparked debates about the balance between utility and privacy (Kaur, 2024)[20].

Artificial Intelligence and Facial Recognition: The integration of AI and facial recognition technologies poses risks related to consent, accuracy, biases, and expansive surveillance capabilities. The absence of comprehensive regulations allows unchecked data practices, leading to privacy erosion and potential discrimination.

AI-driven technologies can analyze vast amounts of personal data, often without individuals' explicit consent or awareness. This raises ethical concerns about surveillance, profiling, and the potential for misuse by both state and private entities (Ness & Khinvasara, 2024)[21].

Social Media and Digital Sharing: The pervasive use of social media increases vulnerability to data breaches, cyber harassment, and identity theft. Inadequate privacy settings and the blurring of public and private spheres demand more effective data protection measures and enhanced public awareness (Vashisht, 2023)[22].

Social media platforms often collect and monetize personal data, sometimes without transparent consent mechanisms. Users frequently share sensitive information, sometimes unknowingly exposing themselves to privacy risks.

Government Surveillance Practices: Balancing national security with individual privacy rights remains contentious. Existing laws permitting surveillance often lack sufficient checks and balances, risking privacy infringements without adequate judicial oversight (Hiranandani, 2011)[23].

Laws like the Information Technology Act and the National Security Act provide the government with extensive surveillance powers. However, these laws often lack robust oversight mechanisms, leading to potential abuses and violations of privacy.

Implementation and Enforcement Gaps: Despite a robust legal framework, enforcement remains inconsistent due to delays in judicial processes, insufficient regulatory infrastructure, and lack of public awareness about privacy rights (Imam, 2023)[24].

The effectiveness of privacy laws depends on timely enforcement and the capacity of regulatory bodies. Challenges such as bureaucratic inefficiency, resource constraints, and lack of expertise hinder the implementation of privacy protections (Subramanian, 2010)[25].

Evolving Legislative Framework: The Personal Data Protection Bill aims to address many privacy concerns but requires timely enactment, competent regulatory bodies, and consistent enforcement to be effective (Vashisht, 2023)[26].

The bill's success hinges on its ability to adapt to emerging technologies and threats. Ensuring that regulatory bodies have the necessary powers and resources to enforce compliance is critical for the bill to

achieve its objectives (Rawal & Patel, 2023)[27].

Strategies for Enhancing Privacy Protection

Addressing these challenges requires a multifaceted approach:

Robust Regulatory Frameworks: Comprehensive data protection laws that regulate data collection, processing, and storage, ensuring transparency and accountability. This includes establishing clear guidelines for data fiduciaries and enforcing penalties for non-compliance (Bygrave, 2010)[28].

Effective Enforcement Mechanisms: Strengthening judicial processes, enhancing regulatory capacities, and fostering a culture of compliance and respect for privacy. Establishing independent data protection authorities with the power to investigate and enforce privacy laws is crucial (Bisht & Sreenivasulu, 2024)[29].

Public Awareness and Education: Campaigns and initiatives to educate citizens about their privacy rights and how to protect personal information. Empowering individuals with knowledge about data privacy enables them to make informed decisions and advocate for their rights (Kumaraguru & Cranor, 2005)[30].

Adaptive Legislation: Continuous updating and refinement of privacy laws to keep pace with technological advancements and emerging threats. Legislative bodies must engage with stakeholders, including technologists and civil society, to ensure laws remain relevant and effective (Vashisht, 2023).

Balancing Privacy with Other Rights: Navigating the interplay between privacy and other fundamental rights, ensuring a harmonious legal framework that respects multiple aspects of personal liberty. This involves carefully weighing state interests against individual privacy rights to achieve an equitable balance (Burman & Sreekumar, 2024).

International Collaboration: Engaging with global partners to align privacy standards and share best practices. International cooperation is essential in addressing transnational privacy issues and ensuring that India's privacy framework is compatible with global norms (Bygrave, 2004)[31].

CONCLUSION

The constitutional trajectory of privacy in India reflects a dynamic and evolving understanding of individual rights and state responsibilities. From implicit recognition in early judicial interpretations to explicit constitutional validation through the *Puttaswamy* judgment, privacy has become a cornerstone of personal liberty in India. However, the contemporary landscape presents multifaceted challenges that demand continuous vigilance and adaptive strategies.

Addressing issues such as digital surveillance, AI, social media dynamics, and government surveillance requires robust legal frameworks, effective enforcement mechanisms, and a cultural shift towards valuing privacy. By leveraging global best practices and fostering collaboration between the judiciary, legislature, and society, India can uphold the constitutional promise of individual dignity and autonomy. Ensuring that privacy remains a resilient and integral aspect of personal liberty in the face of rapid technological and

societal changes is essential for maintaining the democratic fabric of the nation.

References

1. Ibid
2. Mohammed Ashfaq v. State of Punjab (1984).
3. Pertin, T., & Singh, R. (2022). Evolution of Right to Privacy in the Constitution of India. International Journal of Law Management & Human, 5(166). https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ijlmhs17&section=16
4. Jha, S. (2023). Concept of Privacy in India: A Socio-Legal Critique. Journal of Management and Public Policy, 15(1), 33-44. https://search.proquest.com/openview/d48a91da01c71430bed289bb626ae3d5/1?pq-origsite=gscholar&cbl=906342
5. Chatterjee, S. (2019). Is data privacy a fundamental right in India? An analysis and recommendations from policy and legal perspective. International Journal of Law and Management, 61(1), 170-190.

   https://www.emerald.com/insight/content/doi/10.1108/IJLMA-01-2018-0013/full/html
6. Acharya, B. (2015). The four parts of privacy in India. Economic and Political Weekly, 32-38. https://www.jstor.org/stable/24482489
7. Singh, P. (2021). Aadhaar and data privacy: biometric identification and anxieties of recognition in India. Information, Communication & Society, 24(7), 978-993. https://www.tandfonline.com/doi/abs/10.1080/1369118X.2019.1668459
8. Bhatia, G. (2014). State surveillance and the right to privacy in India: A constitutional biography. National Law School India Review, 26, 127. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/nlsind26&section=16
9. Acharya, B. (2015). The four parts of privacy in India. Economic and Political Weekly, 32-38. https://www.jstor.org/stable/24482489
10. Yadav, R., & Varshney, R. (2024). Right To Be Forgotten Amidst Data Protection, Right To Privacy And Cyber Security. Library Progress International, 44(2s), 1750-1757.

    https://bpasjournals.com/library-science/index.php/journal/article/view/2092
11. Bisht, A. K., & Sreenivasulu, N. S. (2024). Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023. IntechOpen. https://www.intechopen.com/online-first/1190882
12. Jha, S. (2023). Concept of Privacy in India: A Socio-Legal Critique. Journal of Management and Public Policy, 15(1), 33-44.

    https://search.proquest.com/openview/d48a91da01c71430bed289bb626ae3d5/1?pq-origsite=gscholar&cbl=906342

13. Acharya, B. (2015). The four parts of privacy in India. Economic and Political Weekly, 32-38.

https://www.jstor.org/stable/24482489

14. Pertin, T., & Singh, R. (2022). Evolution of Right to Privacy in the Constitution of India. International Journal of Law Management & Human, 5(166).

https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ijlmhs17&section=16

15. Chatterjee, S. (2019). Is data privacy a fundamental right in India? An analysis and recommendations from policy and legal perspective. International Journal of Law and Management, 61(1), 170-190.

https://www.emerald.com/insight/content/doi/10.1108/IJLMA-01-2018-0013/full/html

16. Bisht, A. K., & Sreenivasulu, N. S. (2024). Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023. IntechOpen.

https://www.intechopen.com/online-first/1190882

17. Vashisht, B. (2023). Data Protection Laws: A Contemporary Study of EU and Indian Laws. International Journal of Law Management & Human, 6(793).

https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ijlmhs24&section=76

18. Gupta, A. K. (2024). Right to privacy in digital technology act: Issues and policy in India. Indian Journal of Public Administration, 70(3), 532-545.

https://journals.sagepub.com/doi/abs/10.1177/00195561241271517

19. Vashisht, B. (2023). Data Protection Laws: A Contemporary Study of EU and Indian Laws. International Journal of Law Management & Human, 6(793).

https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ijlmhs24&section=76

20. Kaur, D. (2024). A Comparative Study of the Evaluation on the Right to Privacy in India and the UK, Their Legal Frameworks and Judicial Interpretation: A Cyber Law Perspective.

https://ijlsi.com/wp-content/uploads/A-Comparative-Study-of-the-Evaluation-on-the-Right-to-Privacy-in-India-and-the-UK-Their-Legal-Frameworks-and-Judicial-Interpretation.pdf

21. Ness, S., & Khinvasara, T. (2024). Emerging Threats in Cyberspace: Implications for National Security Policy and Healthcare Sector. Journal of Engineering Research and Reports, 26(2), 107-117.

https://www.researchgate.net/profile/Stephanie-Ness-3/publication/377774384_Emerging_Threats_in_Cyberspace_Implications_for_National_Security_Policy_

and_Healthcare_Sector/links/65ba19e279007454974f6428/Emerging-Threats-in-Cyberspace-Implications-for-National-Security-Policy-and-Healthcare-Sector.pdf

22. Vashisht, B. (2023). Data Protection Laws: A Contemporary Study of EU and Indian Laws.

International Journal of Law Management & Human, 6(793).

https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ijlmhs24&section=76

23. Hiranandani, V. (2011). Privacy and security in the digital age: contemporary challenges and future directions. The International Journal of Human Rights, 15(7), 1091-1106.

    https://www.tandfonline.com/doi/abs/10.1080/13642987.2010.493360

24. Imam, M. A. (2023). Fundamental Rights and Personal Data Protection: Analyzing the Impact of the Right to Privacy on India's Data Protection Framework. International Journal of Law Management & Human, 6(2021).

    https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ijlmhs26&section=178

25. Subramanian, R. (2010). Security, privacy and politics in India: A historical review. Journal of Information Systems Security (JISSec), 6(2).

    https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2186523

26. Vashisht, B. (2023). Data Protection Laws: A Contemporary Study of EU and Indian Laws. International Journal of Law Management & Human, 6(793).

    https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ijlmhs24&section=76

27. Rawal, M. S., & Patel, H. (2023). A critical analysis of national and international legal framework for protection of the right to privacy and data protection. Resmilitaris, 13(1), 4042-4057.

    https://scholar9.com/publication/ae79c08a4a0e8201a06e1ec097531851.pdf

28. Bygrave, L. A. (2010). Privacy and data protection in an international perspective. Scandinavian Studies in Law, 56(8), 165-200. https://www.scandinavianlaw.se/pdf/56-8.pdf

29. Bisht, A. K., & Sreenivasulu, N. S. (2024). Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023. IntechOpen. https://www.intechopen.com/online-first/1190882

30. Kumaraguru, P., & Cranor, L. (2005, May). Privacy in India: Attitudes and awareness. In International Workshop on Privacy Enhancing Technologies (pp. 243-258). Springer Berlin Heidelberg. https://link.springer.com/chapter/10.1007/11767831_16

31. Bygrave, L. A. (2004). Privacy protection in a global context–a comparative overview. Scandinavian Studies in Law, 47, 319-348. https://scandinavianlaw.se/pdf/47-15.pdf