



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

RIGHT TO PRIVACY IN INDIA: EVOLUTION AFTER THE PUTTASWAMY JUDGMENT.

AUTHORED BY - HARSHIT RAJ

Introduction

In 2017, when an elderly retired judge challenged the government's Aadhaar scheme in the Supreme Court, he posed a question that had haunted Indian constitutional law for decades: Does India's Constitution protect privacy?¹

Privacy remains one of the most debated constitutional and legal issues in contemporary Indian society. The history of privacy protection in India can be traced through judicial decisions such as *Kharak Singh v. State of U.P.*², which denied privacy protection under Article 21, and *People's Union for Civil Liberties v. Union of India (PUCL)*³, which recognized privacy interests in telephonic communications and imposed procedural safeguards on telephone interception.

The 2017 *Justice K.S. Puttaswamy (Retd.) v. Union of India*⁴ judgment transformed this landscape by recognizing privacy as a fundamental right. However, constitutional recognition alone does not guarantee effective protection. Post-*Puttaswamy* India reveals a significant gap between principle and practice: while courts expanded privacy jurisprudence and Parliament enacted the *Digital Personal Data Protection Act, 2023*⁵, concerns regarding enforcement, surveillance, and institutional accountability persist. This paper examines the evolution of privacy protection in India after *Puttaswamy* through judicial application, legislative response, and continuing implementation challenges.

¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, AIR 2017 SC 4161

² *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.

³ *People's Union for Civil Liberties v. Union of India*, AIR 1997 SC 568.

⁴ *Supranote 1*

⁵ Digital Personal Data Protection Act, 2023.

I. From Denial to Recognition: How Puttaswamy Constitutionalized Privacy as a Fundamental Right

The Constitution of India does not expressly recognize privacy as a fundamental right. The judicial evolution of privacy protection in India can be traced through two significant phases:

A. The Denial Phase

1. *Kharak Singh v. State of U.P. (1962)*⁶: While striking down certain police surveillance measures, the majority maintained that “the right of privacy is not a guaranteed right” under the Constitution.
2. *People's Union for Civil Liberties (PUCL) v. Union of India (1997)*⁷: The Supreme Court held that telephonic conversations fall within the sphere of privacy and that interception constitutes a serious intrusion requiring procedural safeguards.

B. The Constitutional Turning Point

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*⁸: In a landmark unanimous judgment, a nine-judge Constitution Bench held that privacy is a constitutionally protected fundamental right under Part III of the Constitution. The Court overruled *M.P. Sharma* and *Kharak Singh* to the extent that they denied constitutional protection to privacy, recognizing privacy as inherent in Articles 14, 19, and 21.

The judgment broadened the understanding of privacy to include bodily privacy, decisional autonomy, and informational privacy. It further established that restrictions on privacy must satisfy the tests of legality, legitimate state aim, and proportionality, thereby transforming privacy from a contested constitutional concept into an enforceable fundamental right.

II. The Aadhaar Judgment and the Application of the Proportionality Test

Following the *Puttaswamy* verdict, the Supreme Court's critical challenge was translating constitutional principle into judicial practice. The 2018 *Justice K.S. Puttaswamy v. Union of India* (Aadhaar) case provided this opportunity. The government defended Aadhaar, a

⁶ *Supranote2*

⁷ *Supranote3*

⁸ *Supranote1*

biometric identification scheme involving the collection of fingerprints, iris scans, and demographic data, as essential for efficient welfare delivery and administrative governance. However, the Court subjected the scheme to the proportionality framework established in the *Puttaswamy* judgment.

The Court's analysis operated on three key principles: legality, legitimate state aim, and proportionality. It examined whether Aadhaar was backed by valid legislation, whether it pursued a legitimate governmental objective, and whether the intrusion into individual privacy was proportionate to the benefits sought to be achieved. While the Court upheld Aadhaar for the targeted delivery of welfare benefits under Section 7 of the Aadhaar Act⁹, it struck down provisions that extended its use beyond welfare administration, including mandatory linkage with bank accounts and mobile phone services. The Court emphasized that the collection and use of biometric data must remain proportionate to the objectives pursued and be accompanied by adequate safeguards against misuse.

The judgment was significant for two reasons. First, it demonstrated that the privacy principles articulated in *Puttaswamy*¹⁰ could effectively constrain state action, thereby transforming privacy from a theoretical constitutional guarantee into an enforceable right. Second, it highlighted that privacy is not an absolute right and may be balanced against competing public interests. By applying the proportionality doctrine to a large-scale state programme, the Court established a constitutional framework for resolving future privacy disputes, marking the beginning of a new phase in post-*Puttaswamy* privacy jurisprudence.

III. From Constitutional Right to Statutory Framework: The DPDP Act, 2023

Following *Puttaswamy's* constitutional recognition of privacy as a fundamental right, the Indian legislature enacted the Digital Personal Data Protection (DPDP) Act, 2023 India's first comprehensive data protection statute. The Act operationalizes the constitutional principle of informational privacy by establishing a consent-based framework requiring organizations to obtain explicit consent before processing personal data. The statute grants individuals substantive rights aligned with *Puttaswamy's* vision: access to personal data, correction of

⁹ Aadhaar Act, 2016, § 7.

¹⁰ Ministry of Electronics and Information Technology, Government of India, materials relating to implementation of the Digital Personal Data Protection Act, 2023

inaccuracies, and erasure under specified circumstances. The establishment of a Data Protection Board and compliance obligations for Data Fiduciaries represents an institutional framework for privacy protection previously absent in Indian law.

However, the DPDP Act reveals important limitations in realizing *Puttaswamy's* broader constitutional promise. While regulating both private and governmental processing of personal data, it grants extensive exemptions to the State in circumstances involving national security, public order, and governance. Critics argue these exemptions risk weakening accountability mechanisms and may dilute the robust privacy protections envisioned by the Supreme Court. Consequently, although the DPDP Act represents **a significant legislative effort** to operationalize informational privacy, it highlights the continuing tension between individual privacy rights and state interests, reflecting both **the progress and the limitations** of India's post-*Puttaswamy* privacy framework.

IV. Implementation Challenges and the Enforcement Gap

Despite *Puttaswamy's* constitutional recognition of privacy and the enactment of the DPDP Act, 2023, significant implementation gaps persist in India's privacy protection framework. Technological advancements have enabled unprecedented collection and processing of personal data, raising concerns regarding surveillance, transparency, and accountability. The increasing use of facial recognition technologies, digital monitoring systems, and large-scale government databases has intensified debates regarding the adequacy of existing safeguards and the effective enforcement of privacy rights.

The implementation of the DPDP Act remains at a developing stage. Although the legislation establishes a framework for protecting personal data, concerns persist regarding the institutional capacity and independence of enforcement mechanisms. Furthermore, broad state exemptions relating to national security, public order, and governance have generated criticism from privacy advocates, who argue that such provisions may weaken accountability and limit meaningful oversight. As a result, significant areas of surveillance and data processing continue to operate within a fragmented and evolving regulatory environment.

Judicial enforcement presents an additional challenge. Since privacy violations often occur through large-scale technological systems, individual litigation may be insufficient to address

systemic concerns. Moreover, public awareness of privacy rights remains limited, reducing the likelihood that violations will be identified and challenged. These challenges demonstrate that constitutional recognition and legislative codification, while essential, are insufficient on their own. Effective privacy protection¹¹ ultimately depends upon robust enforcement institutions, transparent governance mechanisms, and sustained judicial oversight capable of translating constitutional guarantees into practical realities.

V. CONCLUSION

The evolution of privacy protection in India since *Puttaswamy* represents significant progress: constitutional recognition as a fundamental right, judicial application through the Aadhaar case, and statutory codification via the DPDP Act, 2023. Yet this evolution remains incomplete. Implementation gaps persist—institutional enforcement mechanisms lack capacity, concerns regarding state surveillance continue, particularly in light of broad regulatory exemptions, and public awareness remains limited. Judicial reliance on individual litigation often proves inadequate for addressing systemic privacy violations.

India's post-*Puttaswamy* privacy framework thus stands between aspiration and reality. Constitutional recognition has been achieved, and statutory frameworks have been established. Yet translating these advances into comprehensive protection requires sustained institutional strengthening, effective enforcement, and meaningful accountability mechanisms. The *Puttaswamy* judgment opened the constitutional door; realizing its full promise remains the ongoing task of Indian democracy.

BIBLIOGRAPHY

Cases

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. *Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

Statutes

Constitution of India, 1950.

¹¹ Gautam Bhatia, *Privacy and the Indian Constitution* (Oxford University Press, 2019).

Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

Government Sources

Ministry of Electronics and Information Technology, Government of India, *Digital Personal Data Protection Act, 2023*.

Books and Articles

Gautam Bhatia, *Privacy and the Indian Constitution* (Oxford University Press, 2019).

M.P. Jain, *Indian Constitutional Law* (LexisNexis, 9th ed.).

V.N. Shukla, *Constitution of India* (Eastern Book Company).

