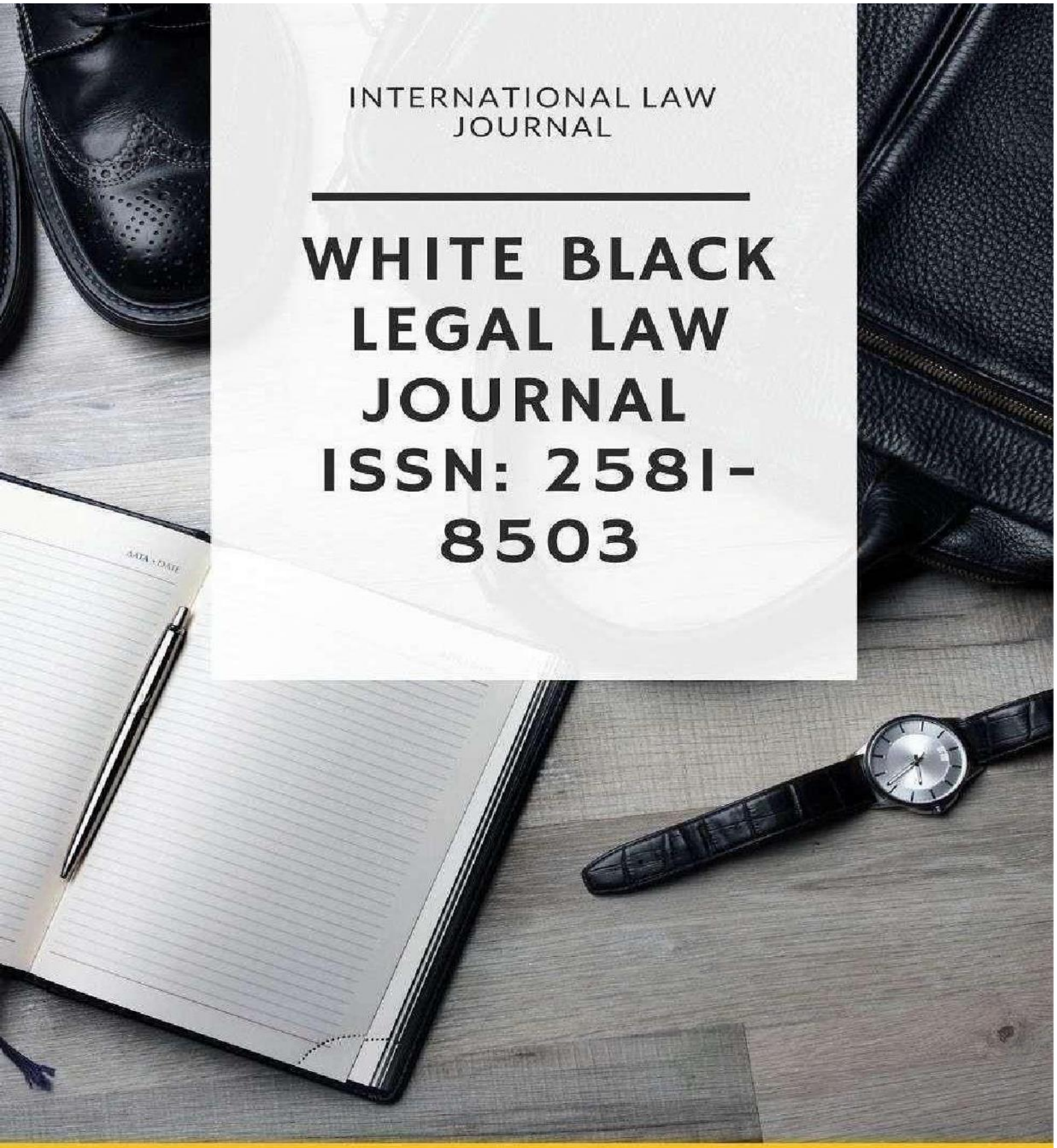


INTERNATIONAL LAW JOURNAL

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.

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.

WHITE BLACK LEGAL

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

From Puttaswamy to the Digital Age

A human-centred study of constitutional rights, personal data and digital life in India

AUTHORED BY - RAGHAV GOYAL
Chandigarh University

Abstract

Privacy is more than the ability to keep information secret. It gives people room to make personal choices, develop relationships, express opinions and live with dignity without unnecessary observation or interference. In India, the Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) recognised privacy as a fundamental right and provided a constitutional foundation for responding to new forms of surveillance and data collection. Since then, digital technologies have made the question more urgent: personal information may be gathered through phones, websites, identity systems, financial services and public platforms, often at a scale that ordinary users cannot easily understand or control.

This paper traces the development of privacy in Indian constitutional law, explains the importance of the Puttaswamy judgment, and considers the Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025. It discusses consent, government surveillance, data security, automated profiling and unequal access to remedies. It argues that effective privacy protection must be measured not only by the existence of laws, but by whether people can understand their choices, challenge misuse and obtain fair treatment. A humane digital future requires innovation to be accompanied by responsibility, proportionality and respect for every person's dignity.

1. Introduction

A person should not have to surrender their private life simply to participate in modern society. Yet using a phone, applying for a job, receiving a public benefit, visiting a doctor or opening a bank account can involve the collection of personal information. Digital systems can make services faster and more accessible, but they can also make it difficult to know who holds

our information, how long it is kept, or what conclusions are drawn from it.

Privacy is sometimes misunderstood as a demand for secrecy. In reality, it is about having appropriate control over access to oneself. A person may have nothing to hide and still reasonably object to constant monitoring, unnecessary data collection or the use of personal information for a purpose they never expected. Privacy allows people to think freely, form relationships, seek advice and make decisions without feeling permanently watched.

In India, the constitutional status of privacy developed through decades of judicial debate. The turning point came on 24 August 2017, when a nine-judge bench of the Supreme Court unanimously recognised privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India*. The decision connected privacy with dignity, liberty and autonomy. The later growth of digital services and the enactment of data-protection legislation have made the judgment especially relevant.

This paper examines that journey and asks a practical question: how can India protect the human being behind the data while still allowing technology to serve society?

2. Objectives and research questions

The paper has five objectives: (1) to outline the constitutional development of privacy in India; (2) to analyse the contribution of the Puttaswamy judgment; (3) to assess the relevance of digital data-protection law; (4) to identify practical risks arising from surveillance, data breaches and automated decisions; and (5) to suggest a rights-based, human-centred approach.

The main questions are: How did Indian courts come to recognise privacy as a fundamental right? What constitutional standards should govern interference with privacy? How far can statutory data-protection measures address modern digital risks? And what would make privacy protections usable for ordinary people, including those with limited digital literacy or bargaining power?

3. Research methodology and scope

This is a doctrinal and analytical paper based on constitutional provisions, reported judicial decisions, legislation and official government materials. It interprets legal principles and considers their everyday implications through illustrative examples. These examples are explanatory, not original fieldwork or statistical findings.

The paper focuses on Indian constitutional law and digital personal data. It does not claim to measure the rate of privacy violations or to provide an exhaustive account of every sector-

specific law. Because commencement of the Digital Personal Data Protection framework is phased, readers should check the current official notifications before relying on any particular provision in a live legal matter.

4. Historical development of privacy in India

4.1 Early judicial uncertainty

In *M.P. Sharma v. Satish Chandra* (1954), the Supreme Court considered searches and seizures during an investigation. The decision was later read as denying a general constitutional privacy right in the context then before the Court. In *Kharak Singh v. State of Uttar Pradesh* (1962), the Court examined police surveillance. Although the majority did not recognise a comprehensive right to privacy, the dissent of Justice K. Subba Rao gave a more expansive account of personal liberty and the individual's interest in being left alone.

4.2 A broader understanding of liberty

Constitutional interpretation gradually moved beyond rigid compartments between fundamental rights. In *R.C. Cooper v. Union of India* (1970), the Court challenged an overly isolated approach to rights. In *Maneka Gandhi v. Union of India* (1978), it strengthened the principle that a restriction on personal liberty must satisfy constitutional requirements of fairness and non-arbitrariness. These decisions did not settle every question about privacy, but they helped create a more rights-centred constitutional framework.

4.3 The question referred to a larger bench

Questions surrounding the Aadhaar identification system brought the status of privacy into sharp focus. Earlier judicial observations had created uncertainty, so a nine-judge bench was asked to determine whether privacy was constitutionally protected. On 24 August 2017, the Court unanimously answered yes. It overruled *M.P. Sharma* and *Kharak Singh* to the extent that they denied the existence of a constitutionally protected right to privacy.

5. The Puttaswamy judgment and its meaning

5.1 Privacy as a fundamental right

The Puttaswamy judgment located privacy within the protections of Part III of the Constitution, especially Article 21's guarantee of life and personal liberty, while recognising

its relationship with other fundamental freedoms. Privacy was not treated as a narrow right limited to closed doors or confidential documents. It also concerned the choices through which people shape their identities and lives.

5.2 Dignity and autonomy

The constitutional importance of privacy becomes clear when we consider ordinary experiences. A patient may need to discuss a deeply personal condition with a doctor. A young person may want to explore an idea without public judgement. A family may wish to keep intimate matters within a trusted circle. Unnecessary disclosure or surveillance can create shame, fear or discrimination. Protecting privacy helps people remain authors of their own lives rather than objects of constant scrutiny.

5.3 Privacy supports other freedoms

Privacy is closely connected with freedom of speech, association and belief. People who think that every conversation or search is being monitored may avoid expressing unpopular opinions, seeking sensitive information or joining lawful groups. This chilling effect can weaken public debate and democratic participation. Privacy is therefore not the enemy of democracy; it can be one of the conditions that allows democracy to function openly.

5.4 Privacy is not absolute

Recognising privacy as a fundamental right does not mean that all information collection is unlawful. Investigating crime, delivering public services and protecting public health may sometimes justify limited interference. But the purpose must have a lawful basis and the measure must be constitutionally justified. The Puttaswamy framework is commonly understood to require legality, a legitimate aim, proportionality and safeguards against abuse. A worthy objective does not automatically justify every method used to pursue it.

6. Privacy in the digital age

6.1 Personal data and the loss of control

Digital systems can collect information continuously and combine records from different parts of a person's life. A purchase history, location record and social-media activity may together reveal habits, relationships or vulnerabilities that the person never deliberately disclosed. The concern is not simply that information is stored electronically; it is that its later combination

and use may go far beyond what a person reasonably expected.

6.2 Social media and digital identity

Online platforms have made it easier to learn, create and stay connected. They have also made personal material easier to copy and spread. Photographs, private messages and opinions can be reposted without permission, sometimes leading to harassment, reputational injury or threats to safety. Deleting an original post may not remove screenshots or copies. Privacy protection must therefore consider not only collection but also onward sharing and the real consequences of disclosure.

6.3 Artificial intelligence and profiling

Automated systems can identify patterns, estimate behaviour and help organisations make decisions. These tools may be useful in healthcare, accessibility and public administration, but they can also produce inaccurate inferences or reproduce existing bias. A person might be categorised as risky or unsuitable without knowing why. Where automated assessments affect important opportunities, transparency, accountability and a meaningful way to question the outcome become especially important.

6.4 Government surveillance

Government agencies may need information to investigate crime, administer benefits or respond to emergencies. At the same time, large-scale or poorly supervised surveillance can intrude deeply into private life. A rights-based approach asks whether the power is authorised by law, necessary for a legitimate objective, proportionate in scope and subject to meaningful oversight. Clear rules on access, retention, disclosure and remedies help ensure that exceptional powers do not quietly become routine.

6.5 Inequality and practical choice

People do not bargain on equal terms with large platforms or public systems. Someone may accept extensive terms because they need a service for school, work, banking or welfare. Others may struggle with long notices, technical language or inaccessible complaint systems. Privacy should not become a privilege for people who have money, time and specialist knowledge. Fair protection requires understandable information and responsibility on the part of institutions, not just caution on the part of individuals.

7. India's data-protection framework

7.1 The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, received presidential assent on 11 August 2023. It establishes a statutory framework for processing digital personal data, balancing individuals' interest in protecting their information with specified lawful uses. The Act is important, but it is not a substitute for the Constitution and does not exhaust every dimension of privacy. Constitutional rights and statutory data-protection duties perform related but distinct functions.

7.2 Consent and its limits

Consent matters when people are told clearly what information is being collected and why. But consent is not meaningful merely because a person clicks a button. If an essential service is available only after accepting complex terms, the individual's practical freedom to refuse may be limited. The Act recognises consent as a principal basis for processing while also providing for specified legitimate uses and exceptions. A careful analysis must therefore avoid the inaccurate claim that every processing activity always depends on consent.

7.3 Rights and organisational duties

The Act provides for rights that include access to information about personal data processing, correction and erasure in applicable circumstances, grievance redressal and nomination. It also places obligations on data fiduciaries, including duties relating to security safeguards and personal-data-breach responsibilities. The Data Protection Board of India is part of the statutory enforcement structure. The practical value of these measures depends on clear procedures, fair decisions and remedies people can actually use.

WHITE BLACK LEGAL

7.4 Children and vulnerable users

Children may not fully understand how a post, photograph or behavioural record could affect them years later. The Act contains special provisions for children's personal data, including parental-consent requirements, subject to the applicable framework and exemptions. Effective protection should go beyond formalities: digital services should be safe by design, explanations should be age-appropriate, and children's developing autonomy should be treated with care.

7.5 Exemptions and public interest

The Act provides exemptions for specified circumstances, including certain legal, judicial, regulatory and crime-prevention functions. Exceptions can serve legitimate public interests, but their scope and use deserve scrutiny. A sound framework must allow necessary public functions without making accountability meaningless. The existence of an exemption should not end the discussion about whether a particular use of information is fair, justified and consistent with applicable constitutional requirements.

8. The Digital Personal Data Protection Rules, 2025

The Digital Personal Data Protection Rules, 2025, were notified in November 2025 and provide implementation details under the Act, including matters relating to notices, consent management, security safeguards and operational responsibilities. The framework has phased commencement. Accordingly, it is important to distinguish between provisions already in force and those scheduled to commence later; notification of the Rules does not mean every obligation became enforceable at once.

The Rules matter because rights need practical processes behind them. People should be able to understand notices, make requests and raise concerns without needing a lawyer or a technical expert for every step. Yet the real test is implementation: whether organisations comply, whether the Board can perform its functions effectively, and whether individuals receive timely and meaningful remedies. Official notifications should be checked for the current commencement status before this paper is submitted or relied upon for legal advice.

9. Judicial development after Puttaswamy: Aadhaar

In *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, decided in 2018 and reported in 2019, the Supreme Court examined the constitutionality of the Aadhaar framework. The Court upheld important parts of the statutory scheme, including specified welfare uses, while invalidating or restricting particular provisions and uses. The case illustrates the difficult balance between effective administration and privacy.

Reliable identification may help people access benefits and services. But authentication failures, excessive data collection or misuse can also exclude eligible people or expose them to harm. A humane system must recognise both risks. Privacy safeguards should not prevent people from receiving essential welfare, and the promise of efficient welfare should not justify unrestricted collection or use of personal information.

10. Major challenges

10.1 Awareness and accessibility

Rights are difficult to exercise when people do not know they exist or cannot understand the procedure. Privacy information should be available in clear language and, where appropriate, in Indian languages and accessible formats. Complaint processes should be easy to find and use.

10.2 Breaches and identity misuse

A data breach can lead to fraud, impersonation, harassment or financial loss. Once intimate information is disclosed, it may be impossible to make it private again. Organisations should use appropriate security measures, restrict access, limit retention and respond responsibly when incidents occur.

10.3 Unequal power

Large organisations may have extensive legal and technical resources, while individuals have little time or ability to negotiate. Effective law should therefore place real obligations on those collecting and processing data rather than expecting every person to defend themselves by reading every policy.

10.4 Automated decisions

When systems use personal data to rank, predict or classify people, errors may affect access to employment, credit, education or services. Individuals need ways to understand and challenge consequential decisions, especially where an automated conclusion may be wrong or unfair.

10.5 The gap between law and lived experience

A legal right is not fully effective if a person cannot get a response, understand a decision or obtain a remedy. Implementation should be assessed through practical outcomes: how complaints are handled, how breaches are addressed, and whether people with fewer resources can exercise their rights.

11. A human-centred approach

A humane privacy framework starts with a simple question: what does this system mean for the person whose information it uses? Imagine a student asked to provide personal details

through an education app. The student should be told why the information is needed, who may receive it and how long it will be kept. Imagine an older person using digital banking who cannot understand a technical notice. The service should offer clear explanations and a straightforward way to report suspicious activity. Imagine a patient sharing sensitive medical information. Confidentiality should be central to the design of the service.

These examples show that privacy is not only about preventing leaks. It concerns the relationship between people and the institutions that hold information about them. A human-centred approach rests on five principles:

Dignity: people should be treated as individuals, not merely as data points. **Autonomy:** they should have meaningful opportunities to understand and influence the use of their information. **Fairness:** protection should not depend on wealth, language or technical skill. **Accountability:** institutions should explain their practices and respond to complaints. **Proportionality:** collection and surveillance should not exceed what a legitimate purpose reasonably requires.

These principles do not require rejecting technology. They ask that technology be designed and governed in ways that respect the people it is supposed to serve.

12. Recommendations

12.1 Public education

Schools, universities, public agencies and civil-society organisations should provide accessible privacy education. It should explain consent, data sharing, online safety, children's privacy and complaint options without relying on technical jargon.

12.2 Better notices and consent

Notices should clearly state what is collected, why it is needed and how it may be used. Organisations should avoid manipulative interface design and make withdrawal or grievance processes accessible where the law provides for them.

12.3 Effective and fair enforcement

The data-protection framework needs adequate expertise, transparent procedures and fair decision-making. Enforcement should be understandable to the public and should offer appropriate remedies under the law.

12.4 Safeguards for State surveillance

Surveillance powers should have clear legal foundations and be necessary and proportionate to legitimate objectives. Appropriate oversight, review and remedies can reduce the risk of arbitrary interference.

12.5 Privacy-conscious design

Organisations should consider privacy from the beginning of a project. Data minimisation, secure storage, access controls, limited retention and risk assessments can reduce avoidable harm.

12.6 Protection for vulnerable groups

Children, older adults, persons with disabilities and people with limited digital literacy may need accessible explanations and additional safeguards. Systems should account for different languages, abilities and circumstances.

12.7 Regular review

Implementation should be reviewed through transparent reporting, consultation and evidence about outcomes. Particular attention should be given to enforcement, breach response, exemptions and the ability of ordinary people to exercise statutory rights.

13. Discussion

The path from the early privacy cases to Puttaswamy and modern data-protection legislation shows a substantial change in Indian constitutional thinking. Privacy is now recognised as a fundamental right, but its practical protection depends on more than a landmark judgment or a statute. It requires organisations to comply, institutions to act fairly and people to have realistic ways to seek help.

Consent alone cannot solve every problem. A person who depends on a digital service for education, work, healthcare or welfare may have little practical ability to refuse its terms. In such situations, fair design, data minimisation, institutional responsibility and effective oversight become especially important.

The central choice is not between technology and privacy. Digital tools can improve lives, but they should not make people powerless over the information that describes them. India's digital future should be judged not only by speed, convenience or innovation, but also by whether

people can live, speak and make decisions with dignity.

14. Conclusion

The Puttaswamy judgment of 2017 was a defining moment because it recognised privacy as an essential part of constitutional liberty and human dignity. Its importance reaches far beyond the question of whether information should be kept secret. It concerns the freedom to make personal decisions, maintain relationships, express views and participate in public life without unjustified intrusion.

The Digital Personal Data Protection Act, 2023, and the Rules notified in 2025 are important developments in India's response to digital data risks. Their success will depend on phased implementation, effective enforcement, understandable procedures and meaningful remedies. The current commencement status of individual provisions should always be verified against official notifications.

Ultimately, privacy is not an obstacle to development and should not be a privilege available only to those who understand technology or can afford legal assistance. It is a condition of human dignity. A just digital society is one in which institutions use information responsibly, public power remains accountable, and every person is treated as more than a profile, record or data point.

References

Primary legal authorities

1. Constitution of India, arts. 14, 19 and 21.
2. Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, Government of India.
3. Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.
4. *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
5. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
6. *R.C. Cooper v. Union of India*, (1970) 1 SCC 248.
7. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
8. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
9. *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1.

Official resources

1. Supreme Court of India, judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, 24 August 2017.
2. India Code, *Digital Personal Data Protection Act, 2023*, https://www.indiacode.nic.in/.
3. Ministry of Electronics and Information Technology, *Digital Personal Data Protection Rules, 2025*, https://www.meity.gov.in/.

Submission reminder: add your personal and institutional details, check the citation style required by your course, and verify each authority against the official text. This paper is educational and is not legal advice.

WHITE BLACK
LEGAL