LAW MANTRA
ISSN 2321-6417
www.journal.lawmantra.co.in

LAW MANTRA THINK BEYOND OTHERS
(I.S.S.N 2321- 6417 (Online)
Ph: +918255090897 Website: journal.lawmantra.co.in
E-mail: info@lawmantra.co.in contact@lawmantra.co.in

RIGHT TO PRIVACY AS A FUNDAMENTAL RIGHT: JUDICIAL RECOGNITION AND LEGISLATIVE FRAMEWORK IN INDIA[*]

Abstract

The right to privacy has grown from a legal curiosity into a central pillar of modern constitutional democracies. Once regarded as a peripheral right, it is today recognized as fundamental in many jurisdictions, especially due to technological developments, datafication, and surveillance risks. This paper explores the concept, evolution, normative sources, jurisprudence (with special reference to India), recent legislative developments, challenges, comparative perspectives, and recommendations.

Key words : Privacy ,Rights ,Constitution Challenges

Introduction

Privacy is often described as the ability of individuals to have control over information about themselves, boundaries of personal space (physical, informational, decisional), and protection from intrusions both by the state and by non-state actors. The surge of digital data collection, pervasive surveillance, social media, biometrics, and global data transfers has made privacy more important and more vulnerable.

In India, the legal recognition of privacy as a fundamental right came relatively late compared to some jurisdictions. The landmark judgment in *Justice K.S. Puttaswamy (Retd.) & Anr. vs Union of India & Ors.* [2]re-established the constitutional foundation for privacy. Alongside, legislative efforts like the Digital Personal Data Protection Act, 2023 seek to regulate digital data flows. This paper examines all these in depth.

Defining Privacy: Conceptual Foundations

To analyse "right to privacy"must understand what *privacy* means. Key dimensions include:

- **Decisional/Autonomy Privacy**: freedom to make personal decisions (marriage, sexual orientation, reproductive rights, lifestyle).
- **Territorial Privacy**: protecting physical space from intrusion (homes, personal correspondence).

[*] **Prof, Dr.V.K.Shrama, School Of Legal Studies Sangam University Bhilwara.**

[2] 2017 10 SCC 1.

- **Informational Privacy**: control over collection, storage, use, and dissemination of personal information.
- **Communicational Privacy**: confidentiality of communications (letters, calls, emails).

Privacy is not absolute; conflicts arise (e.g., national security, public interest, freedom of expression). Legal systems thus adopt tests: whether interference is by law, whether it pursues a legitimate aim, whether it is necessary and proportionate.

Normative and Legal Sources of the Right to Privacy

International / Regional Instruments

- **Universal Declaration of Human Rights (UDHR), 1948** — Article 12[3]: “No one shall be subjected to arbitrary interference with his privacy…”
- **International Covenant on Civil and Political Rights (ICCPR), 1966** — Article 17: protection from “unlawful or arbitrary interference” and “attacks upon honour and reputation.”

Constitutional & Domestic Sources

- Constitution of various countries may contain explicit or implicit rights to privacy (e.g., U.S. Fourth Amendment, Indian Constitution via Articles 14, 19, 21; European countries via ECHR Article 8).
- Statutes, rules, and regulations regarding data protection, surveillance, and information privacy also serve as legal sources.

Jurisprudence in India: Key Cases

Indian court how have treated privacy.

(a) Early Cases: MP Sharma; Kharak Singh

- **M.P. Sharma vs Satish Chandra (1954)** [4]— held that the Constitution does *not* explicitly recognize a fundamental right to privacy; searches and seizures under colonial era laws were allowed without an express constitutional privacy right. Overturned
- **Kharak Singh vs State of Uttar Pradesh (1962)** [5]— Supreme Court held that there is no general right to privacy under Articles 19 or 21. This case included dissenting views, especially around surveillance; but ultimately held that certain kinds of police surveillance (like domiciliary visits, patrols) may infringe on liberty, yet privacy per se was not fully recognised.

These early rulings established that Indian constitutional law did *not* treat privacy as a standalone fundamental right.

(b) Puttaswamy vs. Union of India (2017) [6](“Right to Privacy” judgment)

[3] Article 12 Universal Declaration of Human Rights (UDHR), 1948
[4] M.P. Sharma & Ors. vs. Satish Chandra and Ors.1954
[5] Kharak Singh vs State of Uttar Pradesh (1962
[6] *Justice K. S. Puttaswamy (Retd.) & Anr. vs Union of India & Ors.* (2017) 10 SCC 1

This is the landmark case. A nine-judge bench of the Supreme Court unanimously held that privacy is a fundamental right under the Constitution of India, especially under Article 21 (Right to life and personal liberty), as well as being protected under Articles 14, 19.

Key features of the judgment:

- Overruled M.P. Sharma and Kharak Singh to the extent they held privacy is *not* a fundamental right.
- Defined what aspects of privacy are included: informational privacy, bodily privacy, autonomy of decision making, etc.
- Established that the right to privacy is **not absolute**. Restrictions must satisfy a three-part test: legality (there must be a law), legitimate aim, and proportionality. Also there must be procedural safeguards.

(c) Aadhaar Case / Later Cases

After Puttaswamy, several issue tested whether particular State-measures violate privacy rights.

- In *Puttaswamy II / Aadhaar judgement* (Justice K.S. Puttaswamy (Retd.) & Anr. vs Union of India & Ors., 2018[7], the Supreme Court addressed the Aadhaar Act. Certain provisions of Aadhaar Act were upheld, others struck down for lack of proportionality, due process, etc. For instance, Section 33(2) (sharing of identity information on basis of national security) was struck down. The requirement by private entities to insist on Aadhaar for authentication (Section 57) was seen as problematic because it violates informed consent.

These cases illustrate how the privacy right is applied in concrete scenarios where State action or legislation is at issue, especially in identity systems and large-scale data collection.

Legislative & Policy Developments in India

Legal recognition must be accompanied by statute to guarantee enforcement, remedies, and regulation.

Earlier Legal Regime

- **IT Act, 2000** and its rules (e.g. SPDI Rules, and reasonable security practices) dealt with certain aspects of data privacy. But these regulations were limited in scope (focusing more on sensitive personal data, certain entities) and had weak enforcement.
- There was no comprehensive law for data protection until recently; much of data governance depended on sectoral rules, contract law, tort law, etc.

Digital Personal Data Protection (DPDP) Act, 2023[8]

India recently passed the **Digital Personal Data Protection Act, 2023**. Key features:

- Applies to digital personal data, whether collected in digital form, or collected non-digitally and digitised later.

[7] *Justice K. S. Puttaswamy (Retd.) & Anr. vs Union of India & Ors.* (Aadhaar Case, 2018)

[8] **Digital Personal Data Protection Act, 2023**.

- Requires explicit consent from data principals for processing, except in certain legally defined situations (public interest, sovereignty, security, law enforcement) where exceptions apply.
- Provides rights for data principals: access, correction, erasure of data; revoking consent; protections for children’s data; etc.
- Establishes penalties: failure to prevent breach, failure to notify, etc., with substantial fines (upto thousands of crores in INR) depending on the nature of violation.
- Exclusions: Act does not apply in certain situations e.g., personal/domestic use, publicly available data, etc.

Status of Implementation & Critiques

- Although the DPDP Act, 2023 has been enacted (i.e., received presidential assent, published in Gazette), various key parts await notification/enforcement.
- Critics are concerned about broad exemptions, especially for State agencies and national security, potential gaps in oversight, and whether the enforcement bodies will be sufficiently independent and strong.

Comparative & International Perspectives

Understanding how other legal systems protect privacy helps put India’s developments in perspective, and may suggest lessons.

International Covenants & Declarations

- **ICCPR, Article 17** protects privacy internationally. Many countries are party and subject to monitoring by UN human rights mechanisms.
- **UDHR**, **Convention on the Rights of the Child**, etc., also contain related protections.

European Convention on Human Rights (ECHR)

- **Article 8, ECHR**: “Right to respect for private and family life, home and correspondence” is probably one of the best developed international constitutional law doctrines on privacy. The European Court of Human Rights (ECtHR) has a long line of cases interpreting its scope, restrictions, etc. (e.g., surveillance, data retention, informational privacy).
- The Court employs tests such as: is there an interference with private life? Is the interference “in accordance with the law”? Is it necessary in a democratic society? Is it proportionate to the legitimate aim?

United States

- **Fourth Amendment** to the U.S. Constitution protects against unreasonable searches and seizures, effectively limiting government intrusion into individuals’ persons, homes, papers, and effects.

- U.S. courts have also extended protection to unauthorized surveillance, metadata in certain circumstances, privacy in digitally stored communications (e.g., e-mail, phone records) though often with distinctions.

Other Jurisdictions

- Many countries (EU member states, Canada, Australia etc.) have adopted comprehensive data protection laws (e.g., EU GDPR) which codify rights like access, correction, erasure, portability, breach notification, and set obligations on data controllers/fiduciaries. These laws often provide independent regulatory authorities, oversight, and penalties.

Challenges to Privacy in the Digital Age

Even with laws and court rulings, privacy is under stress from many directions.

(a) State Surveillance

- Government agencies increasingly use biometric ID systems, video surveillance (CCTV), facial recognition, location tracking, interception of communications.
- The challenge is ensuring oversight, transparency, legal safeguards, accountability.

(b) Private Data Collectors, Big Tech

- Social media platforms, online advertisers, data brokers collect huge amounts of data. The use of such data for profiling, algorithmic decision making, predictive analytics raises risks of discrimination, manipulation, loss of autonomy.
- Often consent is poorly informed; terms of service are opaque; people may not know what happens with their data.

(c) Technology & Innovation

- Advances like AI, IoT (Internet of Things), biometrics, cloud computing, seamless cross-border data flows make privacy risks more complex.
- Worst outcomes include misuse of data, data breaches, re-identification from allegedly anonymized data, etc.

(d) Trade-offs: Security, Public Interest, Emergencies

- During public emergencies (e.g. pandemics, terrorism), states tend to expand surveillance and data collection. Legal frameworks must ensure proportionality and post-event accountability.
- There is often tension between privacy and law enforcement, national security, policy tracking, etc.

(e) Implementation, Enforcement & Public Awareness

- Laws are only as good as their enforcement. In many cases, regulatory bodies lack resources or independence.
- People may not know their rights, or find remedies difficult. There may be lack of legal aid or delay in judicial process.

- International dimensions cross-border data flows, cloud storage, global business operations require harmonization and cooperation, which is often lacking.

Critiques & Limitations of Current Frameworks in India

While India has made major strides, there remain gaps and criticisms:

1. **Delay in Enforcement**: Although the DPDP Act was passed in 2023, many provisions await notification. This delays its impact.
2. **Exemptions & Ambiguities**: Exemptions for State, for "sovereignty, security, law enforcement" are significant; definitions may be vague. This may allow misuse or wide interpretation.
3. **Lack of strong independent oversight**: Effectively enforcing data protection requires regulatory authorities that are independent, transparent, with teeth; concerns exist about the proposed Data Protection Board's autonomy.
4. **Consent Fatigue & Informational Asymmetry**: Many people do not truly understand consent agreements, privacy notices; there is information overload; people often assent without real understanding.
5. **Cross-border data transfer issues**: Indian laws need to address transfer of data outside India, ensure that foreign jurisdictions maintain adequate protections.
6. **Technological challenges**: Anonymization, encryption, secure data storage, handling of big data, AI; often the law lags behind tech.
7. **Public awareness & culture**: In many places, people do not know about their rights under Puttaswamy or DPDP; lack of digital literacy aggravates vulnerability.

Recommendations

To strengthen the right to privacy in India (and similar jurisdictions), here are some proposals:

1. **Promptly notify and enforce the DPDP Act's provisions**, ensuring that the rules enabling its operation are transparent and participatory.
2. **Strengthen the independence and effectiveness of the regulatory authority** (Data Protection Board), with appropriate funding, accountability, powers to investigate, impose penalties, order remedies.
3. **Clarify and narrow exemptions**, especially for State agencies, security and national interest, with judicial oversight and sunset clauses.
4. **Enhance privacy by design practices**, ensure default settings in technological platforms are privacy friendly; encourage minimizing data collection; require data anonymization wherever possible.
5. **Improve public awareness and education**, not just via law, but through digital literacy programs, mandatory privacy notices in clear language, transparency reports.

6. **Judicial oversight of intrusive systems**, such as mass surveillance, biometric systems, facial recognition, with mechanisms for review, redress.
7. **Regulate private actors firmly**, enforce obligations on private data fiduciaries, ensure consent is meaningful, protect against profiling and algorithm-bias.
8. **Cross-border legal cooperation**, so data leaving India is protected under adequate safeguards; mutual legal assistance for privacy rights.
9. **Periodic review of laws** to keep pace with technology (AI, IoT, biometric tools), ethical standards, international norms.
10. **Access to remedies**, including swift judicial process, compensation for privacy violations, class action suits or collective redress where violations affect many.

Conclusion

After the recognition of the right to privacy as a fundamental right in India is a major sept. Legislative reforms like the DPDP Act, 2023 provide much-needed legal scaffolding. But law alone won't sufficient, effective enforcement, clear rules, public awareness, and continual adaptation to new technologies are necessary. The balance between privacy and other public interests must be maintained via robust checks and democratic oversight. Privacy in the digital age is both a challenge and an opportunity protecting it well is critical for democratic dignity, autonomy, and human rights.

References

- *Justice K. S. Puttaswamy (Retd.) & Anr. vs Union of India & Ors.* (2017) 10 SCC 1 Supreme Court of India. Recognition of right to privacy under Articles 14, 19, 21.
- *Justice K. S. Puttaswamy (Retd.) & Anr. vs Union of India & Ors.* (Aadhaar Case, 2018) — Supreme Court. Examination of Aadhaar Act's compatibility with privacy.
- Digital Personal Data Protection Act, 2023 — Key Provisions, penalties, rights of data principals.
- "Defining the Right to Privacy in India in light of Justice K.S. Puttaswamy & Anr. v. Union of India (2017)" — Oxford Human Rights Hub analysis.