International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 05-06-2025, Accepted: 06-07-2025, Published: 21-07-2025
Volume 11, Issue 7, 2025, Page No. 58-62

Right to privacy and data protection

Dr. Shikha Bhatnagar
Department of Law, Swami vivekanand Subharti University, Meerut, Uttar Pradesh, India

Abstract
Privacy has increasingly been recognized as a fundamental human right across the globe, and in India, it has been affirmed as a Fundamental Right under Article 21 of the Constitution. Closely tied to this right is the protection of personal data, which has become particularly challenging in today's technologically advanced and globalized world. The absence of comprehensive legal safeguards has made it possible for the ruling majority to infringe upon this right through discriminatory legislation.
Initially, the Indian legal system did not acknowledge the Right to Privacy as a Fundamental Right, nor did it have any specific legislation addressing data protection to uphold this right. Over the years, both the Government and private commercial entities have faced numerous allegations of violating individuals' privacy rights. Several such instances have been brought before the judiciary, resulting in landmark judgments that have shaped the legal discourse around privacy and data protection in India.
In light of these developments, it becomes essential to examine the evolving legal framework to assess how effectively it protects citizens' Right to Privacy. While the Indian legal regime has made notable progress in recognizing and safeguarding this right—particularly through efforts aimed at preventing data breaches and the misuse of sensitive information—there remains significant scope for further reforms. Strengthening the data protection regime is crucial to ensuring comprehensive privacy protection for Indian citizens in the modern digital age.

Keywords: Privacy, data protection, personal information, sensitive information, confidentiality, public interest

Introduction

Meaning of Privacy

Privacy refers to the right of an individual to keep their personal life and information away from public scrutiny or unauthorized access. It involves the ability to control who has access to your personal data, communications, body, space, and decisions.

In Law

In legal terms, privacy is often considered a fundamental human right, protected by constitutions or laws in many countries. For example:
India: Privacy was declared a fundamental right under Article 21 of the Constitution in the Puttaswamy v. Union of India case (2017).

USA: While not explicitly mentioned in the Constitution, privacy is inferred from several amendments (1st, 4th, 5th, 9th).

EU: Strong data protection and privacy laws under the GDPR (General Data Protection Regulation)

Privacy is a valuable aspect of personality. Sociologists and psychologists agree that a person has a fundamental need for privacy. A person's right to privacy entails that such a person should have control over his or her personal information and should be able to conduct his or her personal affairs relatively free from unwanted intrusions. Privacy is also at the core of our democratic values. An individual has an interest in the protection of his or her privacy as preserving privacy encourages dignity, self-determination, individual autonomy and ultimately promotes a more robust and participatory citizenry. Among all the human rights in the international catalogue, privacy is perhaps the most difficult to define. Despite attempts of jurists, scholars and theorists to define privacy, there remains confusion over the true meaning and scope of privacy. One of the problems is that, the very breadth of the idea, and its tendency, produces a lack of definition which weakens its force in the political discourse. Despite the difficulties to ring fence the concept of privacy, Privacy International has suggested that privacy can be said to comprise four separate nonetheless related aspects:

a. Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as "data protection";
b. Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
c. Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and
d. Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and identity checks.

Privacy Laws under the Indian Constitution

1. Evolution of the Right to Privacy as a Fundamental Right

The Indian Constitution does not explicitly define the Right to Privacy. In a general sense, privacy refers to a person's right to live with dignity, autonomy, and freedom from unwarranted intrusions. Despite its significance, many individuals are unaware that privacy is a basic human right, now recognized as a Fundamental Right under Indian law.
International human rights instruments like the Universal

Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR) have influenced India's evolving privacy jurisprudence. Over time, Indian courts have interpreted the Right to Privacy as implicit under Article 21 of the Constitution, which guarantees the Right to Life and Personal Liberty.

2. Judicial Recognition: Landmark Cases

a. MP Sharma v. Satish Chandra (1954)

Issue: Constitutionality of search and seizure provisions.

Ruling: The SC held that the Constitution did not recognize a fundamental right to privacy, as there is no such express provision in Part III.

b. Kharak Singh v. State of UP (1962)

Issue: Legality of police surveillance under UP Police Regulations.

Ruling: The majority did not recognize privacy as a fundamental right. However, Justice Subba Rao (dissenting) emphasized that privacy is intrinsic to personal liberty under Article 21.

c. Govind v. State of Madhya Pradesh (1975)

Issue: Validity of MP Police Regulations enabling domiciliary visits.

Ruling: The SC cautiously acknowledged that privacy is a fundamental right, but subject to reasonable restrictions in public interest.

d. Malak Singh v. State of Punjab & Haryana (1981)

Ruling: State surveillance is valid if it does not violate personal liberty or go beyond legal limits.

e. R. Rajagopal v. State of Tamil Nadu (1994)

Ruling: The SC held that the Right to Privacy includes personal autonomy in matters of marriage, procreation, education, and family life. Publishing personal details without consent amounts to a violation of privacy.

f. People's Union for Civil Liberties (PUCL) v. Union of India (1997)

Issue: Validity of telephone tapping.

Ruling: The SC ruled that telephone conversations are protected under the Right to Privacy. Tapping is only permissible when authorized by law (e.g., Telegraph Act).

3. The Puttaswamy Judgment (2017)

In Justice K.S. Puttaswamy v. Union of India, a nine-judge Constitution Bench of the Supreme Court overruled earlier judgments (MP Sharma and Kharak Singh) and unanimously held that:

Right to Privacy is a Fundamental Right

It is protected under Article 21 (Right to Life and Personal Liberty), and also derives from Articles 14 (Right to Equality) and 19 (Freedom of Expression and Movement).

Privacy includes decisional autonomy, bodily integrity, and protection from data misuse.

This judgment laid the foundation for privacy as a core constitutional value in the digital age.

Data Privacy under Information Technology (IT) Law

1. Existing Legal Framework

India currently lacks a comprehensive, standalone data protection law. However, the Information Technology Act, 2000 and its subordinate rules offer limited protection.

Key Provisions

Section 43A of the IT Act: Holds a body corporate liable for negligent handling of sensitive personal data, resulting in wrongful loss or gain.

IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:

Define Sensitive Personal Data (e.g., financial info, health data, biometric data).

Mandate organizations to follow privacy policies, obtain consent, and adopt reasonable security practices.

2. Anticipated Reforms

In 2019, the Personal Data Protection Bill (PDP Bill) was introduced in Parliament. It proposed:

Setting up a Data Protection Authority.

Granting individuals rights like data access, correction, and erasure.

Imposing obligations on data fiduciaries (companies handling personal data).

This Bill has undergone several revisions, and the Digital Personal Data Protection Act, 2023, was later introduced (you can mention this if you're covering developments post-2019). Bills Pending. Various sectoral laws also impose confidentiality obligations or limit personal data transfers, including laws governing banking, telecommunications, healthcare, and securities.

The Information Technology Act 2000 as amended (IT Act) allows individuals to sue an organization for damages caused by its negligence in implementing and maintaining "reasonable security practices and procedures" to secure sensitive personal data or information (Section 43-A, (IT Act)). The IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (IT Act Rules) define sensitive personal data or information as personal information relating to:

- Passwords.
- Financial information, such as bank account or credit card details or other payment details.
- Physical, physiological, and mental health condition.
- Sexual orientation.
- Medical records and history.
- Biometric information. (Rule 3, IT Act Rules.) Sensitive personal data or information does not include information that is:
- Freely available.
- Publicly accessible.
- Furnished under the Right to Information Act 2005 or other applicable law.

Meaning of Data Protection: Data privacy refers to the protection of personal information, ensuring that individuals have control over how their data is collected, processed, stored, and shared. It encompasses the right of individuals to keep their information private and secure, limiting unauthorized access or use by others. "Data privacy" usually refers to the handling of critical personal information, also called "personally identifiable information" (PII). This

information can include social security numbers, health records, and financial data, including bank account and credit card numbers. In a business context, data privacy goes beyond the PII of employees and customers. This could involve things like proprietary research, development data, or financial information.

Meaning of Personal Data Sensitive personal data (also called sensitive personal information) refers to information that is more private or intimate in nature and, if disclosed or mishandled, can cause significant harm, discrimination, or distress to an individual. This category of data typically requires a higher level of protection under privacy laws and regulations.
Examples of Sensitive Personal Data:
Depending on the jurisdiction, this may include:
Racial or ethnic origin
Political opinions
Religious or philosophical beliefs
Trade union membership
Genetic data
Biometric data (used for identification)
Health data
Sex life or sexual orientation
Criminal convictions and offenses
In some contexts, data such as:
Financial information
Government-issued ID numbers (like Aadhaar in India, SSN in the US)
Location data
Personal communication content

may also be considered sensitive, especially if combined with other identifying information.

Privacy and Data Protection Laws in India: Legal Context and Analysis

1. Legal Context

Globally, data protection is governed through a range of laws tailored to specific jurisdictions:
GDPR (European Union): The General Data Protection Regulation is the benchmark for comprehensive personal data protection globally.

HIPAA (United States): Specifically governs medical data and healthcare information.

DPDP Act, 2023 (India): Marks India's transition to a comprehensive data privacy framework.

India's data protection landscape has seen significant evolution—from fragmented sectoral regulations to the enactment of a dedicated law—the Digital Personal Data Protection Act, 2023—affirming privacy as a right and reinforcing mechanisms to protect digital personal data.

2. Key Data Protection Legislation in India

Digital Personal Data Protection (DPDP) Act, 2023
Enacted: August 2023
Scope: Governs the processing of digital personal data.

Key Features

Applicability
To data processed within India.
To data processed outside India, if connected to the offering of goods/services to Indian residents.

Definition of Personal Data
Any data related to an individual who is identifiable by or in relation to that data.

Consent-Based Processing
Data processing is permitted only with free, informed, specific, and clear consent of the data principal, except under certain legitimate uses (such as legal obligations, emergencies, etc.).

Rights of Data Principals
Right to access personal data.
Right to correction and erasure.
Right to grievance redressal.
Right to nominate someone to exercise rights in case of death/incapacity.

Obligations of Data Fiduciaries
Maintain accuracy of data.
Implement technical and organizational safeguards.
Inform the Data Protection Board and affected individuals in case of a data breach.

Cross-Border Data Transfers
Permitted by default, unless restricted by the government through specific notifications.

Penalties
Fines up to ₹250 crore (approx. $30 million) for serious non-compliance.

Regulatory Authority
Data Protection Board of India: Empowered to oversee enforcement, issue directions, and resolve disputes.

Sectoral Laws Impacting Data Privacy
While the DPDP Act is now the principal law, sector-specific regulations continue to play a supporting role:

a. Information Technology Act, 2000 (IT Act)
Section 43A: Provides for compensation for failure to protect sensitive personal data.

b. SPDI Rules, 2011
Define Sensitive Personal Data or Information (SPDI) including financial details, health records, and biometric data.
Require consent for data collection and restrict disclosure.

c. Other Relevant Laws
Indian Penal Code (IPC): Addresses criminal misuse of data.
Intellectual Property Laws: Offer indirect protection for proprietary data.
Consumer Protection Act: Recognizes data misuse as an unfair trade practice.

3. Constitutional Perspective: Right to Privacy

The Right to Privacy was formally recognized as a Fundamental Right under Article 21 of the Indian Constitution by the Supreme Court in the landmark case:

Justice K.S. Puttaswamy v. Union of India (2017)
The Court unanimously held that privacy is intrinsic to life and liberty, and thus protected under Article 21.
Overruled earlier decisions in M.P. Sharma (1954) and Kharak Singh (1962).
Created a legal foundation for enacting modern data protection laws like the DPDP Act.
ase Laws:

Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India (2017) [7]
This landmark case was a constitutional challenge to the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 on the grounds that it violated the right to privacy. The Supreme Court of India held that the right to privacy is a fundamental right under Article 21 of the Constitution, and that the collection of personal data under the Aadhaar Act must meet the test of proportionality and be done through informed consent.

R. Rajagopal v. State of Tamil Nadu (1994) [8]
This case established the right to privacy as a part of the right to freedom of speech and expression under Article 19(1)(a) of the Constitution. The Supreme Court held that the publication of an individual's personal information without their consent would amount to a violation of their right to privacy.

Selvi and Ors. v. State of Karnataka (2010) [9]
This case dealt with the issue of the admissibility of evidence obtained through narco-analysis and other forms of involuntary testing. The Supreme Court held that such methods of obtaining evidence violate an individual's right to privacy and dignity under Articles 20(3) and 21 of the Constitution.

Vishakha and Ors. v. State of Rajasthan and Ors. (1997)
This case dealt with the issue of sexual harassment in the workplace and established the need for guidelines to prevent and redress such harassment. The Supreme Court held that the right to work with dignity is a fundamental right under Article 21 of the Constitution, and that the prevention of sexual harassment is essential to ensure the exercise of this right.

Shreya Singhal v. Union of India (2015)
This case dealt with the issue of online freedom of speech and the constitutionality of Section 66A of the IT Act, which criminalized certain types of online speech. The Supreme Court held that Section 66A violated the right to freedom of speech and expression under Article 19(1)(a) of the Constitution and was therefore unconstitutional.
These cases highlight the importance of the right to privacy and data protection in India and demonstrate the evolving jurisprudence in this area. The courts have played an important role in recognizing and protecting these rights, and their decisions have set important precedents for the future development of privacy and data protection laws in India.

Conclusion and Suggestions
India's recognition of privacy as a Fundamental Right is a critical step toward safeguarding individual autonomy and dignity. However, in the face of rapid digital transformation and growing cyber threats, there is an urgent need to strengthen implementation, close regulatory loopholes, and enhance public awareness.

Key Suggestions
Stronger Enforcement Mechanism
The Data Protection Board must be empowered and adequately resourced to act swiftly against violations.

Public Awareness and Education
Citizens must be educated about their data rights, especially in rural and under-informed populations.

Stricter Accountability
Data fiduciaries (both government and private entities) must be held strictly liable for breaches due to negligence.

Enhanced Cybersecurity Infrastructure
Data repositories should be protected by robust technical safeguards like encryption, multi-factor authentication, and real-time intrusion detection.

Judicial Remedies
Efficient and accessible grievance redressal mechanisms should be provided to victims of data misuse.

Clarity in Cross-Border Transfers
The government must clearly outline which countries are restricted and ensure reciprocity in data protection standards.

Unified Framework
Harmonize the DPDP Act with sectoral regulations (like RBI and health sector data norms) to avoid overlaps and conflicts.

References

1. INDIA CONST. art. 21.
2. Information Technology Act, 2000.
3. Indian Contract Act, 1872.
4. Right to Information Act, 2005.
5. Aadhaar Act, 2016.
6. The Indian Penal Code, 1860.
7. Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India, (2017) 10 SCC 1.
8. R. Rajagopal v. State of Tamil Nadu, 1995 AIR 264.
9. Selvi and Ors. v. State of Karnataka, (2010) 7 SCC 263.
10. K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.
11. Vishakha and Ors. v. State of Rajasthan and Ors., (1997) 6 SCC 241.
12. Shreya Singhal v. Union of India, AIR 2015 SC 1523.
13. Apar Gupta, "Balancing online privacy in India", 6 IJLT, (2010).
14. Asok Kini, "Aadhaar the summary of majority (4:1) judgement", pdf.
15. Credit Information Companies Regulation act, 2005
16. Dr Payal Jain &Ms Kanika Arora, "Invasion of Aadhaar on right to privacy: huge concern of
17. issues and challenges", 45 (2) ILR (2018).
18. Indian Penal Code, 1980
19. Right to Privacy…. 73 B. Das & J. Boruah
20. Intellectual Property Law
21. Kalyani Menon Sen, "Aadhaar: wrong no, or big brother calling", 11(2) socio-legal rev. 85

22. (2015).
23. Latha. R. Nair, “Data Protection Efforts in India. Blind leading the blind”. 4IJLT1,23-
24. 27.(2018).
25. Rukhmini Bobde, “Data protection and the Indian BPO industry, 2 law Rev. GLC,79-88(2002-
26. 03) nlu.5
27. Shiv Shankar singh, “Privacy and data protection in India: a critical assessment”, 53 JILI,
28. 683(2011).
29. Shraddha, “What impact the recent right to privacy judgement will have on existing law”, April
30. 24, 2018.
31. Subhajit Basu, “Policy- making, technology, and privacy in India” 6 IJLT (2010).
32. The Indian Evidence Act, Act, 1872
33. The Information Technology (Amendment) Act, 2008
34. The Information Technology (Reasonable Security Practices and procedures and sensitive personal data or information), Rules, 2011
35. Vivek Baid and Shyam Panday, “Privacy on the internet-protected by legislation” 1lawRev.
36. GLC 14, 21-23(2001-02)
37. The Digital Personal Data Protection Act, 2023 (DPDP Act)