THE LAWWAY WITH LAWYERS JOURNAL

Website: www.the lawway with lawyers.com

VOLUME:-38 ISSUE NO:- 38 , SEPTEMBER 23, 2026

ISSN (ONLINE):- 2584-1106

Email: thelawwaywithelawyers@gmail.com

Digital Number : 2025-23534643

CC BY-NC-SA

Authored By:- **Rashmi Rani**

Amity Law School, Amity University Patna, Bihar

THE RIGHT TO PRIVACY IN THE DIGITAL AGE: LEGAL CHALLENGES AND CONSTITUTIONAL SAFEGUARDS IN INDIA

Abstract

Digital technologies have rapidly changed the way personal information is collected, processed, stored, and shared. Online platforms, mobile apps, digital payments, biometric identification, location services, artificial intelligence, facial recognition, and large-scale data analysis bring important social and economic benefits. At the same time, they can threaten individual autonomy, dignity, anonymity, and control over personal information. In India, the Supreme Court's nine-judge decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) recognized privacy as a fundamental right protected by Part III of the Constitution, particularly Article 21, and linked it to dignity, liberty, and autonomy. This recognition has become central to discussions about surveillance, data protection, digital identity, online profiling, and technology-led governance. This paper examines the constitutional basis of privacy in India, key judicial developments, and the laws governing personal data and digital activity. It discusses the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025,

while distinguishing their enactment and notification from the phased commencement of individual provisions. It also considers ongoing concerns about meaningful consent, State access to personal data, children's information, cross-border processing, automated decisions, platform accountability, and effective remedies. The study uses a doctrinal and qualitative approach, drawing on constitutional provisions, legislation, judicial decisions, official materials, and scholarly literature. It argues that formal recognition alone cannot ensure privacy. Effective protection also requires necessity and proportionality in State interference, transparent data practices, independent oversight, accessible remedies, strong security measures, and a careful balance between privacy, legitimate public purposes, and freedom of expression.

Keywords: Right to Privacy, Article 21, Puttaswamy Judgment, Informational Privacy, Digital Personal Data Protection Act, 2023, Data Protection, Surveillance, Artificial Intelligence, Constitutional Safeguards, India.

INTRODUCTION

Digital technology now plays a role in almost every part of daily life. People use digital systems to communicate, study, work, shop, make payments, access public services, and maintain relationships. These activities create data about their identity, location, habits, preferences, relationships, health, finances, and behaviour. When large amounts of this information are collected and analysed together, they can reveal intimate details about a person, even if each individual piece of data seems harmless on its own.

The challenge of digital privacy goes beyond keeping personal information secret. It also concerns who collects the data, the reasons for collecting it, how long it is kept, whether it is shared, how it is combined with other information, and whether it is used to classify or influence people. Someone may formally agree to a platform's terms without fully understanding how extensively their information will be processed. In some cases, there may be no realistic alternative to accepting those terms. Data breaches, profiling, targeted manipulation, location tracking, facial recognition, and automated decisions can all affect personal autonomy and equal participation in society.

Privacy was not expressly listed as a separate right in the original text of the Indian Constitution. Its constitutional status developed through judicial interpretation of the guarantees relating to

life, personal liberty, equality, and freedom. The key turning point came in Justice K.S. Puttaswamy (Retd.) v. Union of India, when a nine-judge Bench unanimously held on 24 August 2017 that privacy is a fundamental right protected by the Constitution. The Court recognised privacy as intrinsic to life and personal liberty under Article 21 and as part of the freedoms guaranteed by Part III.

Recognising privacy as a constitutional right does not, by itself, answer every practical question. The State may seek access to information for reasons such as national security, crime prevention, public health, welfare delivery, or other legitimate purposes. Private organisations may also process data to provide services or conduct business. The central legal challenge is to allow legitimate uses of information while preventing interference with privacy that is arbitrary, excessive, unclear, or discriminatory. This paper examines that challenge within India's constitutional and statutory framework.

1. RESEARCH BACKGROUND AND EVOLUTION OF THE RIGHT TO PRIVACY

Early judicial developments

The constitutional development of privacy in India shows a gradual shift from uncertainty towards clear recognition. In M.P. Sharma v. Satish Chandra (1954), the Supreme Court considered search and seizure in relation to constitutional protection against compelled self-incrimination, but did not recognise a general fundamental right to privacy. In Kharak Singh v. State of Uttar Pradesh (1962), the Court examined police surveillance, including visits to a person's home. Although the majority struck down certain forms of surveillance, it did not accept a broad constitutional right to privacy. Later decisions increasingly acknowledged privacy-related interests through personal liberty, dignity, and freedom. [1]

Development under Article 21

In Maneka Gandhi v. Union of India (1978), the Supreme Court gave Article 21 a broader interpretation. It held that any procedure depriving a person of life or personal liberty must be

just, fair, and reasonable. This decision strengthened the connection between Article 21 and other fundamental rights. Later cases considered privacy in specific settings, including telephone tapping, reproductive choice, bodily integrity, and personal autonomy. Together, these developments helped establish that constitutional liberty protects more than a person's physical existence.[2]

Justice K.S. Puttaswamy v. Union of India (2017)

In Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, a nine-judge Constitution Bench unanimously held that privacy is a fundamental right. The Court rejected the view that privacy fell entirely outside constitutional protection and overruled earlier decisions to the extent that they denied such protection. The judgments connected privacy with human dignity, individual autonomy, bodily integrity, family life, personal choices, and control over personal information.

The judgment did not establish privacy as an absolute right. Instead, it made clear that any interference must meet constitutional standards. The framework commonly drawn from the decision asks whether the interference is authorised by law, serves a legitimate State aim, and is proportionate to that aim. Proportionality requires a rational connection between the measure and its objective, along with an assessment of whether the intrusion goes further than necessary. How this standard applies depends on the legal context and the nature of the right affected.

Aadhaar and subsequent developments

In K.S. Puttaswamy (Aadhaar) v. Union of India (2019) 1 SCC 1, the Supreme Court considered the constitutional validity of the Aadhaar framework and its connection with privacy, identity verification, welfare delivery, and State power. The decision shows that privacy questions often involve competing constitutional and public-policy interests. Whether a particular data system is lawful depends on its design, purpose, safeguards, scope, and actual operation—not simply on the fact that it uses technology.[4]

2. STATEMENT OF THE PROBLEM

This research focuses on the gap between constitutional recognition of privacy and people's practical ability to control their personal information in digital settings. Data collection is often continuous, difficult to see, and hard to understand. Information may pass between several organisations, be combined with other datasets, remain stored for long periods, or be used for purposes that were not clear when it was first collected. People may also have little bargaining power when essential services are available only through digital systems.

A further concern is State surveillance and access to personal data. Public authorities may have valid reasons to investigate crime, protect national security, or administer public programmes. However, powers that are too broad or subject to inadequate supervision can discourage expression, association, and dissent, and may lead to unnecessary or disproportionate monitoring. Enforcement presents another difficulty: legal rights offer limited protection if people cannot identify misuse, receive clear explanations, challenge decisions, request deletion where the law permits it, or obtain an effective remedy.

The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 are important developments in this area. However, their provisions are being brought into force in phases. As of October 2026, it is important not to assume that every substantive provision is already operative. This research therefore considers both the framework created by the legislation and the consequences of its staged implementation.

3. RESEARCH QUESTIONS

• What is the constitutional foundation and scope of the right to privacy in India?

• How have the Supreme Court's decisions shaped the legal standards governing interference with privacy?

• To what extent does India's statutory framework protect personal data in the digital age?

• What legal and practical difficulties arise from surveillance, platform data collection, profiling, and automated technologies?

• What safeguards are needed to balance privacy with legitimate public interests, innovation, and freedom of expression?

4. OBJECTIVES OF THE STUDY

• To examine the constitutional basis of privacy under Article 21 and related fundamental rights.

• To analyse leading judicial decisions on privacy, personal liberty, surveillance, and data protection.

• To explain the relevant provisions and phased implementation of the Digital Personal Data Protection Act, 2023 and Rules, 2025.

• To identify the main risks created by digital data collection, profiling, biometrics, artificial intelligence, and State surveillance.

• To propose legally workable safeguards that improve accountability, transparency, proportionality, and access to remedies.

5. RESEARCH METHODOLOGY

This paper uses doctrinal and qualitative legal research methods. Its primary sources include the Constitution of India, legislation, rules, official notifications, and Supreme Court judgments. Secondary sources include legal scholarship, books, research articles, and publications by institutions dealing with privacy and digital governance. The analysis examines principles set out in judicial decisions, compares them with the statutory framework, and considers the practical problems that arise in digital environments. The focus is mainly on Indian law, with limited reference to other jurisdictions where comparison helps explain regulatory choices. The study is not an empirical survey of individuals or organisations.

6. CONSTITUTIONAL SAFEGUARDS FOR PRIVACY IN INDIA

Article 21: life, personal liberty, and dignity

Article 21 states that no person may be deprived of life or personal liberty except according to a procedure established by law. Judicial interpretation has given this guarantee a wider and more substantive meaning. Privacy protects a person's ability to make personal choices, maintain bodily integrity and intimate relationships, and exercise control over aspects of their personal

information. In digital settings, Article 21 may be relevant when State conduct intrudes into personal data, communications, movement, or autonomy. The fact that information is stored digitally does not, by itself, settle the constitutional question; the nature and extent of the interference must also be considered.[5]

Articles 14 and 19

Article 14 guarantees equality before the law and equal protection of the laws. It becomes relevant when data systems or surveillance practices are arbitrary, make unjustified distinctions, or lead to discriminatory outcomes. Article 19 protects specific freedoms, including speech and expression, peaceful assembly, and association, subject to restrictions permitted by the Constitution.[6]

Limits on State interference: legality, legitimate aim, and proportionality

Under the constitutional standard associated with Puttaswamy, interference with privacy must have a lawful basis, pursue a legitimate State aim, and be proportionate to the objective. In practice, a measure that affects privacy should be supported by clear legal authority, serve a permissible purpose, and avoid unnecessary intrusion. Depending on the circumstances, safeguards may include prior authorisation, independent review, limits on purpose and duration, audit trails, and access to remedies. National security and administrative convenience should not automatically settle every objection based on privacy.

Horizontal and institutional dimensions

The Constitution mainly governs State action, but privacy harms can also be caused by private companies, employers, online platforms, data brokers, and other organizations. Statutory data-protection obligations, consumer law, contract law, criminal law, and sector-specific rules all have a role in addressing these harms. The State must also create an effective legal framework through which people can seek protection against serious privacy violations by private actors.[16]

7. DIGITAL PRIVACY: KEY AREAS OF RISK

Personal data collection and profiling

Websites and apps may collect identifiers, browsing records, device details, purchase histories, location data, and inferred interests. When these details are combined, they can create extensive profiles that affect advertising, credit, recruitment, pricing, and access to services. The concern is not just that private information might be disclosed. A profile may be inaccurate, difficult to challenge, or used in ways the individual could not reasonably have expected. Purpose limitation, data minimization, accuracy, retention limits, and clear explanations are therefore important safeguards.

Consent and unequal bargaining power

Consent is an important part of data protection, but it may offer limited protection when notices are long, technical, bundled with other terms, or difficult to refuse. A person may click “agree” without understanding how their information will be shared or used. Where the law provides for withdrawal, consent should be informed, specific, clear, and capable of being withdrawn. Even so, consent cannot resolve every privacy concern. Organisations must also define clear purposes, collect only proportionate amounts of data, protect it securely, and remain accountable for their practices.

Government surveillance and digital identity

Digital identity systems and data-driven public services can make services easier to access, reduce duplication, and improve administrative efficiency. They can also create risks when authentication data are centralised, access controls are weak, information is used for new purposes, or people cannot correct errors. Surveillance technologies may affect privacy in communications, movement, and association. The law should specify who may access information, the purposes for which access is permitted, the required authorisation, how long the information may be retained, and what independent checks apply.

Biometrics, facial recognition, and artificial intelligence

Biometric identifiers, including fingerprints, facial features, and iris patterns, are especially sensitive because they are closely tied to bodily identity and may be difficult or impossible to replace if compromised. Facial-recognition tools can identify people in public places, while AI systems may infer personal characteristics or make decisions using large datasets. Accuracy, bias, explainability, security, and access to human review are therefore important concerns. Using AI does not automatically make a practice unlawful, but it does not remove the need for a lawful basis, necessity, proportionality, and accountability.

Data breaches and cybersecurity

A data breach may expose financial details, identity documents, medical records, login credentials, or private communications. Possible consequences include fraud, identity misuse, harassment, reputational damage, and a lasting loss of control over personal information. Organisations that handle personal data should use reasonable security measures, restrict access according to roles, maintain incident-response procedures, and notify affected people as required by applicable law. Security is essential to privacy, but privacy also requires limits on collection and use that may be lawful yet excessive.

Children and vulnerable users

Children may not fully appreciate the long-term effects of sharing information online, behavioural advertising, or persistent digital profiles. Their data may influence future opportunities and expose them to profiling or exploitation. Safeguards should take account of age-appropriate information, responsible processing, safety, and children's evolving capacity to make decisions. They should also avoid imposing unnecessary surveillance or preventing children from accessing beneficial digital services.

8. STATUTORY FRAMEWORK FOR DIGITAL PRIVACY IN INDIA

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 creates a framework for processing digital personal data in India and, in specified circumstances, for processing carried out outside India. It refers to the individual whose personal data is involved as a "Data Principal" and to the person who decides the purpose and means of processing as a "Data Fiduciary." The Act addresses consent and certain legitimate uses, the duties of data fiduciaries, the rights and duties of individuals, children's data, security safeguards, personal data breaches, and the Data Protection Board of India.[8]

The Act is important because it moves data protection beyond separate rules for individual sectors and establishes a general statutory framework. Its practical effect, however, will depend on when provisions commence, how the rules are implemented, the capacity of relevant institutions, public awareness, and the way exemptions and enforcement powers are applied. The framework should be judged not only by its stated aims, but also by whether people can understand and exercise their rights and whether organisations have meaningful reasons to comply.

Digital Personal Data Protection Rules, 2025 and phased commencement

The Digital Personal Data Protection Rules, 2025 were notified in November 2025. The commencement notification for the Act sets different effective dates for different provisions. As of October 2026, the framework is in a phased transition: institutional and preliminary provisions have commenced, while many key processing duties and individual rights are scheduled to take effect later, including provisions set to commence eighteen months after the notification was published in November 2025. It would therefore be inaccurate to say that every substantive requirement of the Act is fully in force in October 2026. Researchers and practitioners should consult the relevant Gazette notifications to confirm the commencement status of each provision.[9]

The Rules explain how parts of the Act are to be implemented, including requirements relating to notices, security safeguards, data breaches, and procedures. They must be read alongside the Act, the commencement notifications, and any later amendments or corrigenda. Their effectiveness will depend on clear compliance expectations, accessible complaint channels, proportionate enforcement, and public understanding.

Information Technology Act, 2000 and related rules

The Information Technology Act, 2000 remains an important part of India's legal framework for electronic records, cyber offences, and matters involving intermediaries. Depending on the circumstances, provisions dealing with unauthorized access, identity misuse, cheating by personation, and the publication or transmission of certain unlawful material may be relevant to privacy-related harm. Section 43A historically provided for compensation where a body corporate failed to protect sensitive personal data, subject to the terms of that provision and the later legal transition associated with the DPDP framework. The current status and application of a particular provision should be checked before relying on it, rather than assumed from older commentary.[10]

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended, also address intermediary due diligence and grievance handling. They may be relevant when privacy-violating content or personal information is circulated online. Their application must remain consistent with constitutional guarantees, legal authority, and procedural fairness.[11]

Other relevant laws

Privacy disputes may also involve the Bharatiya Nyaya Sanhita, 2023, where the conduct satisfies the elements of offences such as cheating, criminal intimidation, or defamation. The Bharatiya Sakshya Adhiniyam, 2023 may be relevant when electronic records are used as evidence. Consumer-protection rules may apply in commercial settings, while banking, telecommunications, health, and other regulated sectors may have their own requirements. These laws deal with different forms of harm and do not replace the constitutional standard governing State interference.

9. LANDMARK JUDICIAL DECISIONS

K.S. Puttaswamy v. Union of India (2017)

In this case, the nine-judge Bench held that privacy is a fundamental right inherent in life and personal liberty under Article 21 and protected by Part III. It remains the leading constitutional authority on privacy in India. The judgment sets out foundational principles concerning dignity, autonomy, informational privacy, and the requirement that State interference meet constitutional standards.

Kharak Singh v. State of Uttar Pradesh (1962)

This case dealt with police surveillance and visits to a person's home. Its earlier approach to privacy was substantially reconsidered in Puttaswamy, which overruled it to the extent that it denied constitutional protection to privacy. The decision remains relevant to understanding how the legal position developed over time.

Maneka Gandhi v. Union of India (1978) [2]

The Court held that any procedure depriving a person of life or personal liberty must be fair, just, and reasonable. Although the case did not concern modern data protection, its interpretation of Article 21 remains central to constitutional review of measures that interfere with personal liberty.

PUCL v. Union of India (1997)

People's Union for Civil Liberties v. Union of India concerned telephone tapping and recognized the serious privacy concerns raised by interception of communications. It is relevant to the need for procedural safeguards and controls when the State intercepts communications. [13]

K.S. Puttaswamy (Aadhaar) v. Union of India (2018)

The Aadhaar decision examined the constitutionality of a national identity system and the relationship between identity verification, welfare benefits, privacy, and proportionality. It shows why a digital system must be assessed in light of its actual design and use, including the reasons for collecting data and the safeguards against misuse.

Anuradha Bhasin v. Union of India (2020)

In a case concerning restrictions on internet access in Jammu and Kashmir, the Supreme Court considered the publication and review of orders restricting internet services and the connection between internet access and constitutionally protected freedoms. Although the case was not exclusively about privacy, it shows how digital infrastructure can affect the exercise of fundamental rights and why restrictions must be legally scrutinised.[14]

10. MAJOR LEGAL AND PRACTICAL CHALLENGES

Meaningful consent and information asymmetry

Digital services commonly rely on lengthy privacy notices and standard terms. Users may have little ability to negotiate those terms or compare how different services handle personal information. As a result, formal consent may not represent a genuinely informed choice. Clear notices presented in layers and privacy settings that ordinary users can understand may help, but they must be accompanied by substantive limits on excessive collection and use.

State exemptions and independent oversight

The State has legitimate reasons to investigate crime and protect national security, but broad powers to obtain personal data can lead to disproportionate interference. Exemptions should be clearly drafted and narrowly interpreted. Independent authorization or review, proper record-keeping, audits, and effective remedies can help prevent arbitrary use. Oversight bodies

should be independent enough to examine both the legality and the proportionality of the measures used.

Enforcement, awareness, and access to remedies

Many people are unsure what information an organization holds about them, how to make a complaint, or which authority can help. Digital literacy and straightforward grievance procedures are therefore essential. Remedies should be timely and accessible, especially for people with limited technical knowledge, disabilities, language barriers, or limited financial resources. Institutions also need the expertise and capacity to investigate complex data practices.

Cross-border processing and jurisdiction

Personal data may pass through servers, service providers, and corporate groups based in several countries. This raises questions about which laws apply, how regulators can cooperate, how evidence can be obtained, and how decisions can be enforced against organizations without a substantial physical presence in India.

Automated decisions, bias, and explainability

Automated systems may make or influence decisions about employment, credit, education, insurance, and access to services. If the data used are inaccurate or a model repeats historical discrimination, people may be harmed without understanding the reason. Privacy protection should therefore work alongside equality law, consumer protection, sector-specific regulation, and procedural fairness. Where a decision has a significant impact, meaningful explanations, opportunities to correct information, and human review may be necessary safeguards.

Balancing privacy with freedom of expression and public interest

Privacy protection should not be used to silence journalism, public-interest reporting, research, or lawful criticism. At the same time, freedom of expression should not automatically justify revealing highly sensitive personal information. Courts and regulators should consider the context, consent, public interest, potential harm, and applicable law. Remedies should be

proportionate and should avoid unnecessarily broad restrictions that remove lawful information or discourage public debate.

11. COMPARATIVE PERSPECTIVE

Experience from other jurisdictions can help identify useful principles, but foreign approaches cannot simply be copied without taking India's constitutional structure and institutions into account. The European Union's General Data Protection Regulation (GDPR) offers a comprehensive framework built around lawful processing, transparency, data-subject rights, organizational accountability, and independent supervisory authorities. Within the EU legal system, data protection is also recognized as a fundamental right.[15]

The United States uses a more fragmented, sector-based approach. It combines federal and state laws, constitutional protections in particular settings, consumer-protection enforcement, and rules for specific industries. This model can address particular risks, but protection may vary between sectors and states. India's DPDP framework creates a general statutory model, though its practical value will depend on implementation, the scope of exemptions, regulatory independence, enforcement capacity, and the relationship between statutory rights and the constitutional right to privacy.

The main lesson from comparison is not that India should adopt another legal system in full. An effective framework needs clear rules, independent oversight, proportionate enforcement, accessible remedies, security obligations, and protection against arbitrary State action. These features should be shaped to fit India's constitutional principles and administrative realities.

12. FINDINGS AND ANALYSIS

• Privacy in India is a fundamental right grounded in Article 21 and supported by the broader guarantees in Part III of the Constitution.

• The Puttaswamy judgment makes clear that privacy is not absolute; interference must satisfy constitutional requirements, including legality, legitimate aim, and proportionality.

• Digital privacy concerns extend beyond secrecy to profiling, autonomy, data combination, biometric identification, security, and the ability to challenge decisions.

• The DPDP Act, 2023 and DPDP Rules, 2025 create a general framework, but their phased commencement must be considered when describing which obligations are currently operative.

• The effectiveness of legal protection depends on institutional capacity, public awareness, transparency, accessible complaints, and remedies that work in practice.

• Surveillance and data-processing systems should be designed around necessity, purpose limitation, minimization, security, retention controls, and meaningful oversight.

• Privacy safeguards must be balanced with legitimate public purposes and freedom of expression through contextual, proportionate, and reviewable decisions.

13. SUGGESTIONS AND RECOMMENDATIONS

Apply necessity and proportionality to State data practices

Public authorities should specify the legal basis, purpose, scope, duration, and safeguards for any programme that intrudes on privacy. They should collect only the information necessary for the stated purpose. Independent review, audit trails, retention limits, and access to remedies should be built into systems from the beginning.

Strengthen independent and transparent oversight

Regulatory bodies need suitable technical expertise, adequate resources, and operational independence. Public reports should describe the number and types of complaints, responses to breaches, enforcement measures, and broader risks while preserving confidential information. Oversight of State access to personal data should be independent enough to examine whether access is lawful and proportionate.

Improve notice, consent, and user control

Privacy notices should be written in clear language, with short summaries and more detailed information available where needed. Users should be able to locate and change privacy settings without unnecessary difficulty. Organizations should avoid dark patterns that pressure or trick people into sharing data. Consent should not be used to justify unnecessary collection or hide the actual purposes of processing.

Build privacy and security into digital systems

Privacy by design should be part of procurement, software development, and system upgrades. Measures may include data minimization, encryption, access controls, pseudonymization where appropriate, secure deletion, vulnerability testing, and privacy-impact assessments for high-risk systems. Organizations should also maintain clear incident-response plans and report breaches as required by applicable law.

Ensure effective remedies and digital literacy

People should have simple ways to access information, correct inaccurate records, report misuse, and obtain remedies available under the law. Public education should cover common privacy risks, safer digital practices, consent, fraud prevention, and complaint procedures. Information should be available in Indian languages and designed for people with different levels of digital literacy.

Regulate high-risk technologies with safeguards

Facial recognition, biometric databases, large-scale behavioral profiling, and automated systems that have major effects on people require careful risk assessment. Regulation should be technology-neutral where possible, while still being specific enough to address identifiable harms. Depending on the risk, safeguards may include documentation, testing, human review,

and a way to challenge adverse decisions. Rules should also avoid blanket restrictions that unnecessarily block beneficial research or innovation.

Clarify implementation and public guidance under the DPDP framework

Government guidance should clearly state which provisions are already in force and which are due to commence later. Organizations and individuals need accessible information about timelines, compliance requirements, complaint mechanisms, and how the DPDP framework interacts with existing sector-specific laws. Clear guidance can reduce uncertainty and support responsible compliance.

14. CONCLUSION

The right to privacy is now essential to constitutional democracy in the digital age. Personal data can improve public services, support innovation and communication, and contribute to economic development. However, uncontrolled collection and use can expose people to surveillance, manipulation, discrimination, identity misuse, and a loss of autonomy. Privacy is therefore not merely a technical issue of data security; it is a constitutional and legal concern involving dignity, liberty, equality, and people's practical ability to exercise their fundamental rights.

The Supreme Court's decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) established the constitutional foundation by recognizing privacy as a fundamental right under Article 21 and the broader framework of Part III. Its emphasis on legality, legitimate State aims, and proportionality provides a way to assess interference with privacy. Other decisions concerning surveillance, personal liberty, internet access, and Aadhaar show that these principles must be applied to the actual design and operation of digital systems.

The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 are significant steps in the development of India's statutory framework. However, because their provisions are commencing in phases, the status of each relevant provision must be checked carefully. Real protection will depend on clear implementation, independent and capable

oversight, meaningful control for users, secure system design, accessible remedies, and transparent limits on State access to information.

The aim should not be to stop all collection or use of digital information. Rather, information should be handled lawfully, fairly, securely, and for legitimate purposes, while measures that intrude on privacy should be necessary, proportionate, and open to review. A rights-based approach can protect individuals while allowing responsible technological development. The success of privacy law in India will depend not only on constitutional and statutory guarantees existing on paper, but also on whether people can rely on them in everyday digital life.

References

- Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- K.S. Puttaswamy (Aadhaar) v. Union of India, (2019) 1 SCC 1.
- Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
- Digital Personal Data Protection Rules, 2025, Ministry of Electronics & Information Technology, Gazette of India (Nov. 2025).
- Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India (as amended).
- M.P. Sharma v. Satish Chandra, AIR 1954 SC 300; 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.
- Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1.

TABLE OF AUTHORITIES

Cases

• Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

• Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

- K.S. Puttaswamy (Aadhaar) v. Union of India, (2019) 1 SCC 1.
- Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
- Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
- M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
- People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

Statutes and Articles

- Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023).
- Bharatiya Sakshya Adhiniyam, No. 47 of 2023, INDIA CODE (2023).
- Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
- Digital Personal Data Protection Rules, 2025, Ministry of Electronics & Information Technology, Gazette of India (Nov. 2025).
- INDIA CONST. arts. 14, 19, 21.
- Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
    - Radha Ranjan, "Evolution of the Doctrine of Proportionality: Assessing its Scope and Ambit in Relation to the Right to Privacy in India" 10(1) Indian Journal of Law and Human Behavior 31–38 (January–June 2024), p-ISSN: 2454-7107, e-ISSN: 2455-4189, DOI: 10.21088/ijlhb.2454.7107.10124.3
    - Radha Ranjan and Pallavi Singh, "Cyber Crime Against Women in Cyber Space: A Critical Analysis of Indian Legislations," 10(1A) Kanpur Philosophers (2023).
    - Radha Ranjan and Jivantika Gulati, "The Sexual Harassment against Women in Cyber Space: Concept, Reality and the Law," 10(1) Kashmir Journal of Legal Studies 79–90 (2023).
    - Bheem Singh Meena, Radha Ranjan and Shyam Kumar Anand, 'Virtual Meetings under Attack: Assessing the Legal and Security Risks of Zoom Bombing in the Digital Era' (2023) 4(2) ShodhKosh: Journal of Visual and Performing Arts 1256–1263.
    - • Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India (as amended).

- • Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1.