

## **DATA PROTECTION AND THE RIGHTS TO PRIVACY IN INDIA: LEGAL CHALLENGES AND EMERGING TRENDS**

*by*

L. UMA RANI, BA

S. Thangapazham Law College, Tamilnadu.

&

K. RAJESH KUMAR, B.COM.ML.,(Ph.D)

Faculty of Law, S. Thangapazham Law College, Tamilnadu

### **ABSTRACT**

The rapid growth of digital technologies, artificial intelligence, social media, cloud computing, and e-governance has significantly increased the collection and processing of personal data in India. While these technological advancements have enhanced public services and economic development, they have also raised serious concerns regarding data privacy, cybersecurity, surveillance, identity theft, and unauthorized use of personal information. This concern is borne out by recent industry data: cybersecurity incidents reported in India more than doubled between 2022 and 2024, rising from approximately 1.03 million to 2.27 million cases. Such figures illustrate why safeguarding personal data has moved from a narrow compliance concern to a matter of broader digital resilience (VISTA InfoSec, 'DPDP Act Non-Compliance Penalties: What You Must Know' (VISTA InfoSec, 2 April 2026) <<https://vistainfosec.com/blog/dpdp-act-non-compliance-penalties/>> accessed 11 August 2026).

Recognizing the importance of informational privacy, the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. declared the Right to Privacy as a fundamental right under Article 21 of the Constitution. Subsequently, the

enactment of the Digital Personal Data Protection Act, 2023 marked a significant step towards establishing a comprehensive legal framework for the protection of digital personal data in India.

This study examines the constitutional and statutory framework governing data protection and Privacy in India, with particular emphasis on the Digital Personal Data Protection Act, 2023. It analyzes the legal challenges associated with government surveillance, data breaches, cross-border data transfers, technological innovations, and the balance between privacy, transparency, and national security. The research adopts a doctrinal and analytical methodology based on primary legal sources, including statutes and judicial decisions, and secondary sources such as books, research articles, government reports, and academic databases.

**Keywords:** *Data protection, Right to Privacy, Constitution of India, Personal Data, Cybersecurity and Informational Privacy*

## 1) Introduction

The rapid expansion of digital technologies, artificial intelligence, cloud computing, social media, e-commerce, and e-governance has transformed the way personal information is collected, processed, stored, and shared. While these developments have improved governance and economic growth, they have also increased concerns regarding misuse of personal data, cybercrime, identity theft, surveillance, and unauthorized data sharing. The right to privacy was recognized as a Fundamental Right under Article 21 of the Constitution of India by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1. This landmark judgment established informational privacy as an essential part of the right to life and personal

liberty. To regulate digital personal data, Parliament enacted the Digital Personal Data Protection Act, 2023 (DPDP Act). The Act establishes a legal framework governing the collection, processing, storage, and transfer of digital personal data while imposing obligations on organizations handling such data. However, debates continue regarding broad governmental exemptions, surveillance powers, implementation challenges, and the balance between privacy and transparency. This research examines India's evolving legal framework for data protection, the constitutional foundations of privacy, current legal challenges, and emerging trends in privacy governance. The financial dimension of this risk has grown correspondingly: the average cost borne by an Indian organisation following a data breach reached a record Rs 25.5 crore in 2026, an increase of nearly sixteen per cent over the preceding year. This trend underscores the practical stakes underlying the constitutional and statutory debates examined in this study ('Cost of Org-Level Data Breach Touches Its Highest Level in India at Rs 25.5 Crore: IBM' CXOToday (Bengaluru, 3 August 2026) <<https://cxotoday.com/cybersecurity/cost-of-org-level-data-breach-touches-its-highest-level-in-india-at-rs-25-5-crore-ibm/>> accessed 11 August 2026).

## 2) Review of Literature

### 2.1 Justice K.S. Puttaswamy Judgment (2017) 10 SCC 1

The Supreme Court unanimously declared privacy is a constitutionally protected fundamental right, primarily connected with Article 14, 19, and 21. The judgment laid down the principles of legality, necessity, and proportionality for any restriction on privacy rights.<sup>1</sup> The judgment was delivered by a nine-judge Constitution Bench that ruled unanimously, although the decision comprised six separate opinions rather than a single authored judgment, a feature

---

<sup>1</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (Supreme Court of India).

that has itself generated academic discussion on how to identify its precise ratio. The size of this Bench, the largest to consider the question of privacy since the earlier decisions it overruled, is often cited as evidence of the weight the Court attached to the issue (Supreme Court Observer, 'Fundamental Right to Privacy' (Supreme Court Observer) <<https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/>> accessed 11 August 2026).

## 2.2 Digital Personal Data Protection Act, 2023

Recent scholarship recognizes the Digital Personal Data Protection Act, 2023 (DPDP Act). India's principal comprehensive statutory framework for digital personal data protection data but highlights concerns regarding government exemptions, limited institutional independence, and enforcement gaps.<sup>2</sup> These concerns have gained practical relevance since the Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025, bringing into effect the provisions establishing the Data Protection Board of India while leaving most substantive compliance obligations, including consent management and breach notification, to a phased implementation window extending to around May 2027. Commentators have observed that this staggered timeline means the Act's practical impact on data governance in India is still unfolding rather than fully realised ('India Switched On Its Data Protection Board: The Localisation Clock Is Now Ticking' (Mickai, 4 July 2026) <<https://mickai.co.uk/articles/india-dpdp-first-enforcement-localisation>> accessed 11 August 2026).

## 2.3 Comparative Privacy Studies

Researchers compare India's framework with the European Union's GDPR and conclude that while India's law adopts consent-based principles, it provides broader exemptions to public authorities and weaker regulatory safeguards.<sup>3</sup> This divergence is thrown into sharper

---

<sup>2</sup> *Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, sec 3, 17, 18–29 (India).*

<sup>3</sup> *Yadav & Pandey, "Data Privacy Across Borders," 10 University of Bologna Law Review 177 (2025).*

relief by developments elsewhere: the European Union's AI Act has, since February 2025, prohibited the real-time use of facial recognition technology by law enforcement in public spaces, a categorical restriction that has no equivalent under Indian law. Commentators reviewing recent litigation over police surveillance in India have observed that this absence leaves courts, rather than the legislature, to fashion safeguards on a case-by-case basis ('Delhi Police Scanned Student Protesters With AI: Courts Are Now Asking Who Authorized That' TechTimes (29 July 2026) <<https://www.techtimes.com/articles/322033/20260729/delhi-police-scanned-student-protesters-ai-courts-are-now-asking-who-authorized-that.htm>> accessed 11 August 2026).

#### **2.4 Emerging Technologies**

Recent literature identifies Artificial Intelligence, facial recognition, blockchain, big data analytics, and biometric surveillance as new threats requiring stronger legal regulation. The scale of India's biometric infrastructure illustrates the stakes involved: more than a billion residents have been enrolled in the Aadhaar identity scheme, which links each individual to fingerprint and iris data, making questions of biometric security and misuse a matter of mass rather than marginal concern. Literature on the subject accordingly treats safeguards against unauthorised biometric processing as inseparable from the wider debate on emerging technologies (Hugh Tomlinson, 'Case Law, India: Puttaswamy v Union of India, Supreme Court Recognises a Constitutional Right to Privacy in a Landmark Judgment' (Inform's Blog, 4 September 2017) <<https://inform.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/>> accessed 11 August 2026).

#### **2.5 Current Constitutional Debates**

Recent constitutional challenges before the Supreme Court question whether certain

provisions of the DPDP Act weaken transparency under the RTI Act and expand governmental powers beyond constitutional limits. The political salience of this debate is reflected in Parliament itself: members of the opposition INDIA bloc, comprising more than 120 Members of Parliament, have formally called for the removal of the provision amending the Right to Information Act, describing it as a threat to governmental accountability and transparency. This legislative opposition, alongside the pending constitutional challenge, suggests that the tension between privacy and transparency remains an unsettled and actively contested area of Indian public law ('Supreme Court Set to Adjudicate Validity of India's Digital Personal Data Protection Act, 2023' Mondaq (7 July 2026) <<https://www.mondaq.com/india/privacy-protection/1812916/supreme-court-set-to-adjudicate-validity-of-indias-digital-personal-data-protection-act-2023>> accessed 11 August 2026).

### 3) Objectives

The objectives of this research are:

To examine the constitutional basis of the Right to Privacy in India.

To analyze the provisions of the Digital Personal Data Protection Act, 2023.

To study major legal challenges affecting data protection.

To evaluate judicial decisions relating to privacy rights.

### 4) Methodology and Database Used

#### 4.1 Research Design

The research adopts a doctrinal and qualitative research design to examine the legal

framework governing data protection and the Right to Privacy in India.<sup>4</sup>

## **4.2 Nature of Study**

The study is descriptive, analytical, and exploratory in nature, focusing on the existing legal provisions, judicial decisions, legal challenges, and emerging trends in data protection.<sup>5</sup>

## **5) Sources of Data**

The study relies on both primary and secondary sources of data relating to privacy and data protection laws in India.

### **5.1 Primary Sources:**

Primary sources include the Constitution of India, the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, rules and regulations, government documents, and relevant judgments of the Supreme Court and High Courts of India.

### **5.2 Secondary Sources:**

Secondary sources include books, research papers, law journals, articles, commentaries, government reports, policy papers, newspapers, and other scholarly publications relating to data protection and privacy.

### **6) Databases Used:**

The research materials were collected and reviewed through legal and academic databases such as SCC Online, Manupatra, HeinOnline, JSTOR, SSRN, and Google scholar, along with official government and judicial websites.

## **7) Research Discussion:**

---

<sup>4</sup> S.N. Jain, *Doctrinal Legal Research, in Legal Research and Methodology* (Eastern Book Company, 2011).

<sup>5</sup> R. W. M. Dias, *Jurisprudence, 5th ed.* (Aditya Books, 1985).

## 7.1 Constitutional Protection of Privacy

Privacy protects dignity, autonomy, liberty, and informational self-determination. The Puttaswamy judgment established that privacy restrictions must satisfy legality, necessity, and proportionality. Commentators note that although the Puttaswamy Bench spoke through six separate opinions, all nine judges converged on the proportionality standard as the operative test for evaluating state interference with privacy, giving the judgment a practical coherence despite its plurality of reasoning. This convergence has allowed the proportionality framework to be applied consistently in subsequent privacy-related litigation, including challenges to surveillance and data-processing measures (Supreme Court Observer, 'Judgment of the Court in Plain English (I)' (Supreme Court Observer, 23 August 2022) <<https://www.scobserver.in/reports/k-s-puttaswamy-right-to-privacy-judgment-of-the-court-in-plain-english-i/>> accessed 11 August 2026).

## 7.2 Digital Personal Data Protection Act, 2023

### 7.2.1 Consent-Based Processing

The Act requires consent as one of the principal grounds for processing personal data. Section 4(1)(a) provides that a person may process the personal data of a Data Principal “for which the Data Principal has given her consent.” Section 5 requires that every request for consent be accompanied or preceded by a notice informing the Data Principal of “the personal data and the purpose for which the same is proposed to be processed.” Section 6 further requires consent to be “free, specific, informed, unconditional and unambiguous” and provides that the Data Principal may withdraw consent at any time.<sup>6</sup> **The effectiveness of this consent architecture, however, depends on the quality of the interface through which it is**

---

<sup>6</sup> *Digital Personal Data Protection Act, 2023, Sec 4(1)(a), 5(1)(i) & 6(1), Act No. 22 of 2023 (India).*

obtained. Regulators have separately flagged that manipulative interface design, commonly termed dark patterns, such as disguised advertisements and forced continuity, can undermine genuinely free and informed consent even where a platform technically complies with notice requirements, prompting closer scrutiny of how consent is actually presented to users online ('India's CCPA Guidelines on Dark Patterns: Welcome Signal, but Law Is Still Soft' (IAPP, 28 May 2026) <<https://iapp.org/news/a/india-s-ccpa-guidelines-on-dark-patterns-welcome-signal-but-law-is-still-soft>> accessed 11 August 2026).

### 7.2.2 Rights of Data Principals and Privacy Protection

Under the Digital Personal Data Protection Act, 2023, a “Data Principal” means the individual to whom the personal data relates. The Act recognizes important rights of Data Principals, including the right to access information about their personal data, the right to correction, completion, updating and erasure of personal data, the right to grievance redressal, and the right to nominate another individual. These statutory rights strengthen the protection of informational privacy and give individuals greater control over their personal data.<sup>7</sup>

### 7.2.3 Duties of Data Fiduciaries

A Data Fiduciary means any person who determines the purpose and means of processing personal data. Under Section 8 of the Digital Personal Data Protection Act, 2023, a Data Fiduciary is responsible for complying with the Act and must implement “appropriate technical and organisational measures” to ensure effective observance of the Act. It must also protect personal data by taking “reasonable security safeguards to prevent personal data breach” and, in the event of a breach, give intimation to the Board and each affected Data Principal.<sup>8</sup>

### 7.2.4 Children's Data Protection

---

<sup>7</sup> *Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, Sec 2(j), 11–14 (India).*

<sup>8</sup> *Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, § 8(4)-(6) (India).*

The Digital Personal Data Protection Act, 2023 provides specific safeguards for the processing of children's personal data. Under Section 9 of the Act, a Data Fiduciary must obtain verifiable parental consent before processing the personal data of a child, subject to the exemptions provided under the Act and the applicable Rules. The Act also prohibits processing that is likely to cause harm to a child and restricts the tracking or behavioural monitoring of children and targeted advertising directed at children. The Digital Personal Data Protection Rules, 2025 further prescribe mechanisms for verifying parental consent and provide limited exemptions for specified purposes, including certain healthcare, educational, childcare, safety, and related activities. These provisions seek to protect children from misuse of personal data while permitting necessary processing for their welfare and safety.<sup>9</sup> **The scale of the population these provisions are intended to protect is considerable: a government-backed survey conducted in 2024 found that nearly ninety per cent of adolescents between fourteen and sixteen years of age had access to a smartphone at home, indicating that verifiable parental consent requirements will need to operate across a very large and growing base of young users. This underlines the practical importance of effective age-verification mechanisms under the Rules (UNICEF India, 'Children's Online Safety in Education: Guidance Note' (UNICEF, 2026) <<https://www.unicef.org/india/media/18011/file/Children%E2%80%99s%20Online%20Safety%20in%20Education.pdf>> accessed 11 August 2026).**

### 7.2.5 Data Protection Board

The Act provides for the establishment of the Data Protection Board of India. The Board Deals with complaints, data breaches, and violations of the Act. It can also impose penalties for certain cases of non-compliance. **The process of staffing the Board has itself attracted**

<sup>9</sup> *Digital Personal Data Protection Rules, 2025, rr. 10–11 (India)*

**public attention: the Ministry of Electronics and Information Technology issued a notification on 6 May 2026 inviting applications for the posts of Chairperson and Members, describing the Board as a digital-by-design adjudicatory authority responsible for enforcing the Act and the accompanying Rules. The composition of the Board, once finalised, is expected to require expertise spanning data governance, law, and information technology (nasscom, 'Operationalisation of the Data Protection Board: MeitY Invites Applications for Chairperson and Members of the Board' (nasscom, 14 May 2026) <<https://community.nasscom.in/communities/public-policy/operationalisation-data-protection-board-meity-invites-applications>> accessed 11 August 2026).**

#### **7.2.6 Penalties for Non-Compliance**

The Digital Personal Data Protection Act, 2023 provides for financial penalties for breaches of its provisions. Section 33 empowers the Board to impose a monetary penalty after considering the factors specified in the Act. Under the Schedule to the Act, breach of the obligation of a Data Fiduciary to take “reasonable security safeguards to prevent personal data breach” under Section 8(5) may result in a penalty that may extend to two hundred and fifty crore rupees. **It is worth noting, however, that this penalty regime is not yet fully operative: most substantive obligations under the Act, including the breach notification duties underlying this penalty, are expected to become enforceable only around May 2027 under the phased rollout accompanying the 2025 Rules. Until that date, the deterrent effect of these financial penalties therefore remains largely prospective rather than immediately operative ('India Switched On Its Data Protection Board: The Localisation Clock Is Now Ticking' (Mickai, 4 July 2026) <<https://mickai.co.uk/articles/india-dpdp-first-enforcement-localisation>> accessed 11 August 2026).**

#### **7.2.7 Cross-Border Data Transfer Framework**

The Act allows personal data to be transferred outside India, subject to its provisions. The Central Government can restrict transfers to certain countries or territories. This framework seeks to balance international data use with the protection of personal information. **In practice, the Act adopts what commentators describe as a negative-list model, meaning that cross-border transfers are permitted by default unless the Central Government specifically notifies a country or territory as restricted. As of the middle of 2026, no such notification had been issued, so the practical scope of any transfer restriction remained, for the present, undefined ('India Switched On Its Data Protection Board: The Localisation Clock Is Now Ticking' (Mickai, 4 July 2026) <<https://mickai.co.uk/articles/india-dpdp-first-enforcement-localisation>> accessed 11 August 2026).**

### 7.3 Legal Challenges

#### 7.3.1 Government Surveillance

Use of facial recognition, AI surveillance, and mass data collection raises constitutional concerns. Recent litigation challenges the legality of AI-assisted surveillance practices.<sup>10</sup> The scale of such deployments has drawn public attention beyond the courtroom: media investigations into AI-enabled surveillance vans deployed by the police during student protests in 2026 documented real-time facial recognition, automatic number-plate recognition, and crowd-density monitoring conducted without any dedicated statutory framework governing police use of such technology. Digital rights organisations have highlighted this regulatory gap as a central weakness in India's current approach to surveillance oversight (Outlook India, 'CJP Protest Under AI Watch: Delhi Police's Facial Recognition Vans Spark Privacy Concerns'

---

<sup>10</sup> *Aishe Ghosh v. Union of India & Ors., W.P.(C.) (Delhi High Court, 2026).*

(Outlook India) <<https://www.outlookindia.com/national/cjp-protest-under-ai-watch-delhi-polices-facial-recognition-vans-spark-privacy-concerns>> accessed 11 August 2026).

### 7.3.2 Government Exemptions

The Digital Personal Data Protection Act, 2023 provides certain exemptions from its provisions. Under Section 17, specified provisions of the Act shall not apply in circumstances such as processing necessary for enforcing a legal right or claim, judicial or regulatory functions, and the prevention, detection, investigation or prosecution of any offence or contravention of any law. These exemptions may raise concerns regarding the balance between governmental functions and the protection of the right to privacy. **Petitioners challenging these exemptions have specifically argued that they fail to satisfy the established constitutional test of legality, legitimate aim, and proportionality applicable to restrictions on the right to privacy, since the exemptions permit government processing of personal data outside the ordinary consent framework without corresponding independent oversight. Legal commentary has framed this as one of the central questions that will need to be resolved in assessing the overall validity of the Act ('Supreme Court Set to Adjudicate Validity of India's Digital Personal Data Protection Act, 2023' Mondaq (7 July 2026) <<https://www.mondaq.com/india/privacy-protection/1812916/supreme-court-set-to-adjudicate-validity-of-indias-digital-personal-data-protection-act-2023>> accessed 11 August 2026).**

### 7.3.3 Right to Information vs Right to Privacy

Section 44(3) of the Digital Personal Data Protection Act, 2023 amended Section 8(1)(j) of the Right to Information Act, 2005, relating to disclosure of personal information. The amendment has raised concerns about the balance between privacy and transparency. In *Anjali Bhardwaj & Anr. v. Union of India & Ors.*, the amendment and related provisions have been challenged before the Supreme Court. The issue involves balancing the Right to Privacy under

Article 21 with the Right to Information under Article 19(1)(a).<sup>11</sup>

#### 7.3.4 Weak Enforcement

Challenges include limited public awareness, evolving implementation, and concerns about the independence and effectiveness of enforcement mechanisms. These concerns are borne out by the regulator's own timeline: although the Digital Personal Data Protection Rules, 2025 brought the provisions constituting the Data Protection Board of India into effect from 13 November 2025, investigative reporting several months later found that no Chairperson or Member had actually been appointed to the Board, leaving it, in practical terms, an adjudicatory body that existed on paper without the capacity to hear complaints. Such delays illustrate how institutional design alone cannot guarantee effective enforcement in the absence of timely appointments (LiveLaw, 'India's Data Protection Board: Established in Law, Absent in Fact' (LiveLaw) <<https://www.livelaw.in/articles/india-data-protection-board-established-law-543751>> accessed 11 August 2026).

#### 7.4 Emerging Trends

Data protection in India is changing rapidly with the growth of new technologies such as Artificial Intelligence, facial recognition, biometric systems, cloud computing, and social media. These technologies involve the collection and use of large amounts of personal information, creating new privacy risks. There is also a growing focus on online safety, cybersecurity, children's data protection, and secure sharing of data across countries. The idea of Privacy by Design, where privacy is considered while developing new technologies, is also becoming important. These emerging trends show the need for stronger laws, better security

measures, and greater awareness among people to protect personal data and the right to privacy

---

<sup>11</sup> *Venkatesh Nayak v. Union of India*, W.P.(C) No. 177 of 2026; *The Reporters Collective Trust v. Union of India*, W.P.(C) No. 211 of 2026; *National Campaign for People's Right to Information v. Union of India*, W.P.(C) No. 212 of 2026 (Supreme Court of India, notice issued 16 February 2026)

in the digital age. The urgency of these emerging trends is reinforced by industry data showing that artificial intelligence is not only a subject of regulation but increasingly a tool used to commit privacy violations: nearly twenty-six per cent of malicious data breaches recorded in India in 2026 were found to be AI-generated, underscoring the need for regulatory frameworks capable of keeping pace with rapidly evolving technology ('Cost of Org-Level Data Breach Touches Its Highest Level in India at Rs 25.5 Crore: IBM' CXOToday (Bengaluru, 3 August 2026) <<https://cxotoday.com/cybersecurity/cost-of-org-level-data-breach-touches-its-highest-level-in-india-at-rs-25-5-crore-ibm/>> accessed 11 August 2026).

#### **8) Rule of Interpretation of Statutes – Golden Rule**

The Golden Rule of Interpretation is a principle used by courts to interpret statutory provisions in a manner that avoids absurdity, inconsistency, or an unreasonable result. Under this rule, the ordinary meaning of the words in a statute is generally followed, but the court may modify the interpretation where a literal interpretation would lead to an absurd or unjust outcome. In the context of data protection law, this principle may assist courts in interpreting provisions of the Digital Personal Data Protection Act, 2023, particularly where privacy rights, governmental interests, transparency, and technological developments come into conflict. The rule helps ensure that statutory provisions are interpreted consistently with the purpose of the legislation and constitutional values, including the Right to Privacy under Article 21.

#### **9) Suggestions**

Conduct nationwide digital privacy awareness programs.

Encourage Privacy by Design in technology development.

Provide stronger safeguards for children's data.

Mandate standardised, publicly accessible breach-transparency reporting, given that reported cybersecurity incidents in India more than doubled between 2022 and 2024 and that the average cost of a breach reached a record Rs 25.5 crore in 2026. Regular public reporting of this kind would allow citizens and regulators to track the practical effectiveness of the DPDP Act's security obligations over time (VISTA InfoSec, 'DPDP Act Non-Compliance Penalties: What You Must Know' (VISTA InfoSec, 2 April 2026) <<https://vistainfosec.com/blog/dpdp-act-non-compliance-penalties/>> accessed 11 August 2026).

Harmonize Indian law with evolving international privacy standards.

Periodically review the DPDP Act to address emerging technologies.

## 10) Conclusion

## Indian Journal of Contemporary Legal and Social Issues

Data protection and the right to privacy have become essential legal concerns in India due to the rapid growth of digital technologies and online services. The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1. established an important constitutional foundation for protecting personal autonomy, dignity and informational privacy. The enactment of the Digital Personal Data Protection Act, 2023 further represents a significant step towards creating a comprehensive framework for the

protection and processing of digital personal data in India. However, several legal and practical challenges continue to exist. Government surveillance, data breaches, unauthorized processing, cybersecurity threats, cross-border data transfers and the increasing use of artificial intelligence and biometric technologies create new risks to individual privacy. At the same time, there is a need to maintain a proper balance between the individual's right to privacy, national security, public interest, transparency and technological innovation. Effective implementation of data protection legislation therefore requires strong regulatory institutions, accountability and appropriate judicial oversight. In conclusion, India's data protection framework is developing in response to the changing digital environment, but continuous legal and technological reforms are necessary. Greater public awareness, stronger enforcement mechanisms, privacy-by-design practices and effective safeguards against misuse of personal data can strengthen individual rights. A balanced and rights-based approach will help India protect privacy while encouraging digital innovation, economic development and responsible use of emerging technologies.

## 11) Reference

- a) Constitution of India
- b) Digital Personal Data Protection Act, 2023, s. 44(3).
- c) Right to Information Act, 2005, s. 8(1)(j), as amended by s. 44(3) of the Digital Personal Data Protection Act, 2023.
- d) Information Technology Act, 2000
- e) Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. MeitY. Digital Personal Data Protection Act, 2023.
- f) Chaturvedi, S. (2025). Right to Privacy in the Digital Age: Legal Challenges and Emerging Trends in India. International Journal of Legal Science and Innovation.
- g) Ahmed, S. A., & Nasir, M. N. (2026). Stakeholder perceptions of India's Digital Personal

Data Protection Act of 2023. *Frontiers in Sociology*.

- h) Dixit, A. (2026). Data Protection in India after the Digital Personal Data Protection Act, 2023: A Critical Evaluation of Privacy and State Power. *Indian Journal of Legal Review*.
- i) Bareh, C. K. (2024). Reviewing the Privacy Implications of India's Digital Personal Data Protection Act (2023). *DESIDOC Journal of Library & Information Technology*.



Indian Journal of Contemporary  
Legal and Social Issues