



International Journal of Advance Studies and Growth Evaluation

Protecting Data Privacy and Individual Rights in the Era of Artificial Intelligence: A Critical Study of the Indian Legal Framework

^{*1} Jyoti Verma

^{*1} Assistant Professor, Shriji Institute of Legal and Vocational Education and Research, (SILVER Law College), Bareilly Uttar Pradesh, India.

Article Info.

E-ISSN: 2583-6528

Impact Factor (QJIF): 8.4

Peer Reviewed Journal

Available online:

www.alladvancejournal.com

Received: 03/Aug/2026

Accepted: 06/Sep/2026

Abstract

Artificial Intelligence (AI) is increasingly embedded in healthcare, banking, governance, education, transportation, commerce and legal services. Its capacity to collect, infer, classify and process very large volumes of information creates substantial opportunities for efficiency and innovation, but also intensifies risks to privacy, autonomy, equality and dignity. This paper critically examines the Indian legal framework governing data privacy and individual rights in the AI era, with particular attention to constitutional privacy jurisprudence, the Digital Personal Data Protection Act, 2023 (DPDP Act), the Digital Personal Data Protection Rules, 2025, the Information Technology Act, 2000, and the emerging India AI Governance Guidelines. The paper argues that India has moved from a fragmented data-protection landscape toward a more coherent statutory framework, yet important AI-specific questions remain insufficiently resolved. These include opacity in automated decision-making, inferential privacy, algorithmic bias, profiling, allocation of responsibility across AI value chains, effective contestability, and the interaction between data protection and state surveillance. The analysis uses a doctrinal, analytical and comparative method and draws upon constitutional principles and leading Supreme Court decisions. It proposes a rights-based, risk-sensitive and institutionally coordinated approach that combines data-protection compliance with algorithmic accountability, human oversight, impact assessment, transparency, effective remedies and technical safeguards. The objective is not to inhibit responsible innovation, but to ensure that technological progress remains compatible with human dignity, liberty, equality and informational self-determination.

*Corresponding Author

Jyoti Verma

Assistant Professor, Shriji Institute of Legal and Vocational Education and Research, (SILVER Law College), Bareilly Uttar Pradesh, India.

Keywords: Artificial Intelligence; Data Privacy; Informational Privacy; Digital Personal Data Protection Act, 2023; Algorithmic Accountability; Automated Decision-Making; Fundamental Rights; AI Governance; India.

1. Introduction

Artificial Intelligence has become a foundational technology of the contemporary digital economy. Unlike conventional software, modern AI systems can identify patterns, generate predictions, classify individuals, recommend actions and, in some contexts, execute decisions with limited human intervention. These functions depend heavily on data. Personal data may be collected directly from individuals, generated through digital interactions, inferred from behaviour, or combined from multiple sources. Consequently, the expansion of AI changes not only the scale of data processing but also the nature of the privacy problem.

The proposal underlying this study identifies the central tension clearly: AI can improve efficiency and productivity while simultaneously creating serious concerns about

protection of personal data and preservation of individual rights. It particularly identifies consent, privacy, accountability, surveillance, algorithmic bias, automated decision-making and transparency as recurring legal concerns. The research therefore asks whether the Indian framework is capable of addressing harms that arise when personal data becomes an input into predictive and automated systems.

The issue is constitutionally significant. In Justice K.S. Puttaswamy (Retd.) v. Union of India, a nine-Judge Bench of the Supreme Court recognised privacy as a constitutionally protected fundamental right. The judgment connected privacy with liberty, dignity and autonomy and treated informational privacy as an important dimension of the right. The constitutional foundation is particularly relevant to AI because large-scale data processing can affect an individual's

ability to control information about themselves and can create consequences that are difficult to detect or challenge. India's statutory position has also changed substantially. The DPDP Act, 2023 was enacted on 11 August 2023. It establishes a framework for processing digital personal data and sets out obligations of Data Fiduciaries, rights and duties of Data Principals, exemptions, and an institutional mechanism through the Data Protection Board of India. The Act is technologically neutral in many respects, which gives it adaptability, but also means that it does not answer every AI-specific question expressly.

A significant development after the original research proposal is the notification of the Digital Personal Data Protection Rules, 2025 on 14 November 2025. The Rules provide the operational framework for the Act and adopt a phased commencement structure. This development must be incorporated into any current assessment of Indian data protection law. In parallel, the India AI Governance Guidelines were released in November 2025, adopting a principle-based and risk-sensitive governance approach that seeks to combine innovation with safeguards.

The central argument of this paper is that India's emerging framework is a substantial improvement over a purely fragmented regime, but its effectiveness in the AI context will depend on implementation, institutional capacity and the development of complementary safeguards for algorithmic accountability. Privacy protection cannot be reduced to obtaining consent at the beginning of data processing; it must also address what is inferred from data, how automated systems affect people, who remains responsible for outcomes, and whether affected persons have meaningful remedies.

1.1 Scope and Research Gap

The research proposal identifies a gap in scholarship that often examines AI, privacy and Indian law separately. This paper addresses their intersection. It focuses on personal-data processing by AI systems, constitutional privacy, automated decision-making, profiling, surveillance, transparency and regulatory accountability. It does not attempt to provide a technical audit of individual AI models; rather, it examines the legal principles and institutional mechanisms required to govern their use.

2. Research Objectives, Questions and Methodology

2.1 Objectives

- To examine the concept of data privacy in the context of Artificial Intelligence.
- To analyse the constitutional protection of the right to privacy in India.
- To study the relationship between AI technologies and personal data.
- To evaluate existing Indian laws related to data protection.
- To identify legal challenges created by AI systems, including bias, profiling, opacity and automated decision-making.
- To evaluate the efficacy of the DPDP Act, 2023 and the 2025 Rules in the context of emerging AI technologies.
- To examine the effect of AI on consent and the ability to seek correction or erasure of personal data.
- To suggest legal and institutional reforms capable of balancing innovation with protection of individual rights.

2.2 Research Questions

- How can legal accountability be fixed when an AI system violates an individual's data privacy?
- Does the existing Indian framework provide adequate protection against AI-driven surveillance?
- How can transparency and meaningful contestability be ensured in AI systems?
- What legal challenges arise from automated decision-making and profiling?
- What is the role of AI in the collection, processing, inference and reuse of personal data?
- What reforms are required to strengthen privacy protection while supporting responsible innovation?
- How do comparative regulatory approaches illuminate possible reforms for India?

2.3 Hypotheses

H1: The existing Indian legal framework relating to data protection and privacy, although strengthened by the DPDP Act, 2023 and subsequent Rules, is not by itself sufficient to address all complex challenges created by AI, particularly opaque automated decision-making, algorithmic bias, inferential profiling and allocation of responsibility across AI value chains.

H2: Stronger legal safeguards, risk-based governance, transparent AI policies, meaningful human oversight, effective accountability mechanisms and accessible remedies can significantly enhance protection of data privacy and individual rights while permitting socially beneficial AI innovation.

2.4 Research Methodology

The research adopts a doctrinal and analytical methodology, consistent with the methodology stated in the proposal. Primary sources include the Constitution of India, statutes, delegated legislation, judicial decisions and government policy documents. Secondary materials include books, journal literature, policy reports and comparative regulatory materials. A limited comparative perspective is used to identify principles that may inform Indian law, particularly concerning risk classification, transparency, accountability and individual remedies.

The method is primarily qualitative. The paper evaluates legal rules against the practical characteristics of AI systems and asks whether traditional concepts such as notice, consent and accountability remain adequate when processing is continuous, probabilistic, inferential and distributed across developers, deployers and service providers.

3. Constitutional Foundations of Privacy and Individual Rights

The constitutional basis of data privacy in India rests principally on the guarantees of dignity, liberty and personal freedom, read with the broader structure of fundamental rights. The decisive development was the nine-Judge Bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. The Court unanimously recognised privacy as a fundamental right protected by the Constitution. The decision rejected the idea that privacy is merely a common-law or statutory interest and placed it within the constitutional protection of liberty and dignity.

For AI governance, the significance of Puttaswamy lies in its recognition of informational dimensions of privacy. Data about a person can reveal identity, preferences, relationships, location, health, finances and behavioural patterns. AI may go further by generating new information from apparently innocuous data. This phenomenon of inference makes privacy protection more complex: an individual may never have supplied the particular sensitive conclusion that an algorithm derives about them. The proportionality framework developed in constitutional jurisprudence is also relevant where State action interferes with privacy. In general terms, a restriction on a fundamental right must have a lawful basis and must pursue a legitimate objective through means that satisfy constitutional requirements of necessity and proportionality. AI-enabled surveillance and large-scale data analytics therefore raise questions not merely of technical capability but of legal authority, safeguards, purpose limitation, oversight and remedies. In *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632, the Supreme Court recognised an individual's interest in privacy and protection against unauthorised publication of aspects of private life. In *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301, the Court addressed telephone interception and emphasised procedural safeguards for surveillance. These cases pre-date contemporary AI but remain conceptually important because AI can make surveillance more scalable, persistent and analytically powerful.

The Aadhaar judgment, *K.S. Puttaswamy (Retd.) v. Union of India*, (2018) 1 SCC 809, further demonstrated the constitutional importance of informational practices and the need to examine State data architectures through the lens of legality, legitimate purpose and proportionality. Similarly, *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637, illustrates the Court's approach to digital-era rights and restrictions, although the case did not establish a general AI framework. The constitutional position therefore supplies a normative floor for statutory data protection. Parliament and regulators may create more detailed rights and obligations, but AI systems that affect dignity, autonomy, equality or liberty cannot be evaluated solely as commercial data-processing arrangements. The State's use of AI, especially for policing, welfare, identity, immigration or other high-impact functions, requires particularly careful constitutional scrutiny.

3.1 Privacy as Autonomy and Informational Self-Determination

AI challenges the traditional understanding of privacy because harm may occur without disclosure to another human being. Profiling, inference and prediction can influence opportunities or treatment even when the underlying data remains technically confidential. Accordingly, meaningful privacy protection should include not only secrecy but also reasonable control over collection, use, inference, retention and consequential decision-making.

4. Indian Statutory and Regulatory Framework

4.1 Digital Personal Data Protection Act, 2023

The DPDP Act, 2023 is the principal general statute governing digital personal data in India. India Code records its enactment on 11 August 2023 and describes its purpose as regulating processing in a manner that recognises both individual data-protection rights and lawful data processing. The Act uses the concepts of 'Data Principal' and 'Data Fiduciary', reflecting a rights-and-obligations model rather than a purely contractual approach.

The Act establishes grounds for processing, notice and consent requirements, certain legitimate uses, general obligations of Data Fiduciaries, special provisions concerning children's data, and additional obligations for Significant Data Fiduciaries. It also provides rights relating to access to information about personal data, correction and erasure, grievance redressal and nomination. These provisions are highly relevant to AI systems because AI development and deployment can involve repeated processing, data combination, model improvement and downstream use.

The Act's architecture is nevertheless not an AI statute. It does not comprehensively regulate the technical lifecycle of an AI model, nor does it create a general statutory right to receive an explanation of every automated decision. This creates an important distinction: compliance with data-protection requirements does not necessarily establish that an AI decision is fair, accurate, non-discriminatory or contestable.

4.2 Consent and Its Limits in AI

Consent is important but cannot be treated as a complete solution. AI processing may be difficult for ordinary individuals to understand because future uses, inferences and model interactions may not be predictable at the point of collection. Repeated or bundled notices can also create formal rather than substantive choice. The legal challenge is therefore to ensure that consent is informed, specific enough for the relevant processing, capable of withdrawal where applicable, and supplemented by independent duties where consent is not the appropriate safeguard.

4.3 Duties of Data Fiduciaries

The Act places significant responsibility on Data Fiduciaries. For AI deployment, this should translate into governance practices such as data-quality controls, security measures, retention discipline, breach response, vendor oversight and documentation of processing purposes. Significant Data Fiduciaries face enhanced obligations, making the framework potentially important for large-scale or high-impact AI ecosystems.

4.4 Rights to Correction and Erasure

Correction and erasure are especially significant where inaccurate or outdated information becomes part of an automated profile. However, practical implementation becomes complex where data has been incorporated into model-development pipelines or derived representations. Indian regulation will need to clarify how statutory rights interact with model retraining, data deletion, derived information and technically feasible forms of machine unlearning.

4.5 Digital Personal Data Protection Rules, 2025

A major post-proposal development is the notification of the Digital Personal Data Protection Rules, 2025 on 14 November 2025. The Ministry of Electronics and Information Technology describes the Rules as the implementation framework for the Act and provides an eighteen-month phased timeline for compliance. This means that the legal framework should be assessed as an evolving regime rather than as a fully instantaneous set of obligations. The Rules strengthen operational detail concerning matters such as notices, security safeguards, breach-related obligations and institutional implementation.

5. AI-Specific Challenges to Data Privacy and Individual Rights

5.1 Algorithmic Bias and Discrimination

AI systems learn patterns from data. Where historical data reflects social inequalities, under-representation or discriminatory practices, a model may reproduce or amplify those patterns. Bias may arise from the training data, the selection of variables, proxy characteristics, model design, deployment context or feedback loops. In high-impact settings such as employment, credit, insurance, education or public services, biased outputs may directly affect legal or material interests. Data protection law and equality law therefore intersect. A system may process data lawfully yet still produce discriminatory outcomes. A comprehensive rights framework must consequently move beyond privacy and include fairness, non-discrimination, human review and effective avenues for challenge.

5.2 Automated Decision-Making and Contestability

The traditional legal model assumes that a decision can be attributed to an identifiable human decision-maker who can explain and defend the reasons for action. AI can complicate this model. Outputs may be probabilistic, generated from complex models, influenced by numerous variables and difficult to reconstruct after deployment. The resulting accountability gap is particularly serious when an individual is denied a benefit or subjected to adverse treatment.

Indian law should therefore develop a principle of meaningful contestability: affected persons should, where appropriate, be able to know that AI materially influenced a decision, identify the responsible institution, seek human reconsideration, challenge inaccurate data and obtain an effective remedy. Transparency should be calibrated to protect legitimate trade secrets and security without allowing opacity to defeat legal rights.

5.3 Profiling and Inferential Privacy

The privacy risk of AI is not limited to the information an individual knowingly supplies. Systems can infer characteristics, preferences, risk scores and behavioural predictions from multiple datasets. Such inferences may be wrong but still influential. The legal framework should therefore recognise that the creation of new personal information through inference can itself create a privacy and autonomy concern.

5.4 AI-Driven Surveillance

Facial recognition, behavioural analytics, location analysis and automated pattern detection can expand the scale of surveillance. The constitutional principles emerging from Puttaswamy and PUCCL suggest that State surveillance requires a lawful basis, procedural safeguards and protection against arbitrary intrusion. AI intensifies the need for independent oversight, purpose limitation, retention controls, accuracy safeguards and mechanisms to prevent function creep.

5.5 Security and Re-identification

AI systems can create new security risks because datasets may be combined, models may expose information indirectly, and data may flow among multiple processors and vendors. Security obligations therefore need to be understood as continuous risk management rather than a one-time technical exercise. Privacy-enhancing technologies, access controls, encryption, audit logs and appropriate de-identification can reduce risk but cannot substitute for legal accountability.

6. AI Governance in India: From Data Protection to Responsible AI

The Indian governance landscape has increasingly moved toward a combination of statutory safeguards, sectoral regulation, technical measures and policy guidance. The India AI Governance Guidelines released in November 2025 represent an important development. The Guidelines are framed around safe, responsible and inclusive AI adoption and recommend a coordinated governance architecture rather than relying solely on a single comprehensive AI statute.

The Guidelines identify principles including trust, people-first design, innovation, fairness and equity, accountability, understandability and safety, resilience and sustainability. They also recommend governance mechanisms and emphasise a risk-based, evidence-led and proportional approach. This is significant for privacy because AI harms cannot always be prevented through ex ante consent. Governance must also operate through organisational accountability, technical safeguards, monitoring and institutional oversight.

6.1 Interaction between the DPDP Act and AI Governance

The DPDP Act provides the rights-and-obligations foundation for digital personal data, while AI governance can address broader system-level risks. The two should not be treated as competing frameworks. For example, a high-impact AI system may require data-protection compliance because it processes personal data, while fairness, explainability, human oversight or safety may require additional governance controls. A coordinated model can avoid duplication while ensuring that privacy law does not become the sole mechanism for addressing every AI harm.

6.2 Accountability Across the AI Value Chain

Responsibility may be distributed among dataset providers, model developers, cloud providers, application developers, deployers and public authorities. A purely developer-focused liability model can therefore be inadequate. The law should identify responsibility according to control, foreseeability, risk and capacity to prevent harm. Organisations deploying high-impact AI should retain ultimate responsibility for ensuring that their systems comply with applicable law and that individuals have a meaningful avenue for redress.

6.3 Human Oversight

Human oversight should be substantive rather than symbolic. A human reviewer who merely confirms an algorithmic recommendation without access to relevant information or authority to depart from it does not provide meaningful protection. For high-impact decisions, organisations should define escalation procedures, document human review, maintain audit trails and periodically test whether human intervention is actually effective.

6.4 Algorithmic Auditing and Impact Assessment

Impact assessment can connect abstract rights to operational risk. Before deploying high-impact AI, organisations should evaluate data quality, privacy risks, discriminatory effects, security vulnerabilities, foreseeable misuse and available remedies. Independent or appropriately separated audits can provide additional assurance. The Indian policy environment already recognises algorithm auditing and privacy-preserving technologies as areas of responsible-AI development; the next step is to integrate such practices with enforceable governance duties where the risk justifies them.

7. Comparative Perspective

Comparative analysis is useful because AI challenges are not unique to India. The European Union has adopted a layered approach in which the General Data Protection Regulation (GDPR) provides broad data-protection principles and rights, while the EU Artificial Intelligence Act establishes a risk-based framework for AI systems. The EU experience illustrates the value of distinguishing general data governance from AI-specific risk regulation.

The United States has developed a more sectoral and institutionally fragmented approach, with privacy and AI issues addressed through a combination of federal and state laws, sectoral regulation, consumer-protection enforcement and standards. The NIST AI Risk Management Framework and Privacy Framework illustrate a standards-based approach that emphasises governance, risk identification, measurement and management. These approaches demonstrate that legal rules can be supported by technical and organisational standards.

7.1 Lessons for India

- A risk-based approach is preferable to treating every AI application as equally harmful.
- High-impact uses should attract stronger documentation, testing, human oversight and audit requirements.
- General data-protection law should be supplemented by AI-specific principles for automated decision-making, fairness and accountability.
- Individuals need practical remedies, not merely formal rights contained in notices.
- Regulatory coordination is essential because AI is deployed across finance, healthcare, education, telecommunications, employment and government services.
- Technical standards and privacy-enhancing technologies should complement, not replace, enforceable legal duties.

7.2 Avoiding Uncritical Transplantation

Comparative law should not lead to mechanical transplantation of foreign models. India's constitutional structure, administrative capacity, digital public infrastructure, market conditions and developmental priorities are distinct. The appropriate model is therefore one that combines rights protection with innovation, proportionality, institutional feasibility and access to justice.

7.3 The Indian Middle Path

A suitable Indian approach can be described as a rights-based and risk-sensitive techno-legal model. It need not begin with a single omnibus AI Act if existing statutes and regulators can be coordinated effectively. At the same time, the absence of a dedicated AI statute should not mean the absence of enforceable safeguards. The legal system can progressively develop AI-specific obligations through legislation, delegated rules, sectoral standards, regulatory directions and judicial interpretation.

8. Critical Evaluation of the Indian Framework

The Indian framework has several strengths. First, constitutional recognition of privacy provides a rights-based foundation. Second, the DPDP Act supplies a dedicated statutory framework for digital personal data. Third, the 2025 Rules add operational detail and establish a pathway toward implementation. Fourth, the India AI Governance Guidelines recognise that AI governance requires institutional

coordination, risk mitigation and accountability. Together, these developments indicate a transition from reactive cyber regulation toward a more structured digital-governance ecosystem.

Nevertheless, significant limitations remain. The first is the gap between general data protection and AI-specific harms. Data protection rules may address collection, use, security and individual rights without fully resolving whether an automated outcome is fair or intelligible. The second is the difficulty of meaningful consent where individuals cannot realistically anticipate downstream inferences or model uses. The third is the challenge of allocating responsibility across complex AI supply chains.

The fourth concern is transparency. Transparency should not be reduced to disclosure of source code. For legal purposes, the more relevant question is whether an affected person can understand the nature and significance of automated processing sufficiently to exercise a right. This may require information about the purpose of processing, categories of data, material factors, responsible entity, avenues for human review and remedies.

The fifth concern is the tension between data minimisation and AI development. AI systems often benefit from large and diverse datasets, but collecting data merely because it may be useful later is inconsistent with strong purpose limitation. The law should encourage privacy-preserving approaches such as carefully governed synthetic data, federated learning, secure computation and other techniques where appropriate.

The sixth concern is institutional capacity. Rights are meaningful only when regulators, courts and affected individuals can enforce them. A technically complex dispute involving an AI system may require expertise in law, statistics, machine learning, cybersecurity and sector-specific regulation. Strengthening institutional expertise is therefore as important as drafting new legal provisions.

8.1 The Right to be Forgotten and AI

The proposal specifically identifies the 'right to be forgotten'. In India, correction and erasure are addressed within the DPDP Act, but the practical application of erasure to AI models presents difficult questions. If personal data has been used for training, removing the original record may not automatically remove all statistical influence from a model. A future-oriented framework should clarify when retraining, deletion from associated datasets, suppression, output filtering or other technical measures are appropriate.

8.2 The Need for Effective Remedies

A rights framework should provide accessible grievance mechanisms, timely investigation, appropriate compensation or corrective measures where legally available, and judicial review where constitutional rights are implicated. For high-impact AI, affected individuals should not be required to prove technical details that are exclusively controlled by the deploying organisation. Evidentiary rules and disclosure procedures should therefore be designed to prevent information asymmetry from defeating legitimate claims.

9. Suggested Legal and Institutional Reforms

The following reforms are proposed in light of the research questions and hypotheses in the underlying proposal:

- AI-specific risk classification: High-impact AI applications should be identified through criteria based on potential effects on rights, safety, access to essential services and vulnerable groups.

- **Mandatory AI impact assessments for high-risk uses:** Assessments should cover privacy, security, bias, accuracy, human rights and foreseeable misuse before deployment and periodically thereafter.
- **Meaningful automated-decision safeguards:** Where AI materially affects a person's rights or significant interests, the person should, subject to legitimate exceptions, receive appropriate notice and access to meaningful human review.
- **Clear allocation of responsibility:** Deployers and other actors should have documented responsibilities according to their control and role in the AI lifecycle. Contractual allocation should not eliminate statutory accountability.
- **Algorithmic audit mechanisms:** High-risk systems should be subject to independent or appropriately controlled audits covering data governance, performance, discrimination, security and compliance.
- **Enhanced transparency duties:** Organisations should maintain records of AI systems, purposes, categories of data, significant risks, testing and incident response, with appropriate disclosure to regulators and affected persons.
- **Protection against AI surveillance:** Public-sector AI surveillance should be governed by clear legal authority, necessity, proportionality, independent oversight, retention limits and effective remedies.
- **Strengthening data-subject rights in model ecosystems:** The law and regulatory guidance should address correction, erasure, derived data, model training and technically feasible machine-unlearning practices.
- **Privacy by design and security by design:** Privacy should be incorporated at the system-development stage rather than treated as a post-deployment compliance exercise.
- **Regulatory coordination:** The Data Protection Board, sectoral regulators and proposed AI-governance institutions should coordinate to avoid overlapping or contradictory requirements.
- **Special protection for vulnerable persons:** Children and other vulnerable groups should receive enhanced safeguards where AI systems create elevated risks of profiling, manipulation or discrimination.
- **Institutional capacity building:** Regulators and courts require interdisciplinary expertise in AI, data science, cybersecurity, constitutional law and sector-specific regulation.
- **Regulatory sandboxes with rights safeguards:** Controlled innovation environments can permit experimentation while imposing measurable privacy, safety and accountability conditions.
- **Periodic review:** AI governance should include scheduled review because technological capabilities and risks evolve faster than conventional legislative cycles.

9.1 Balancing Innovation and Rights

The objective of regulation should not be to prohibit beneficial AI. A rights-protective framework can increase trust and create conditions for sustainable innovation. Clear rules can reduce uncertainty for responsible developers while discouraging harmful practices. The proper balance is therefore not 'innovation versus regulation' but responsible innovation through proportionate regulation.

9.2 From Notice to Accountability

A central reform principle is to move from a notice-and-consent model toward a broader accountability model. Notice and consent remain important, but they should operate

alongside organisational duties, risk assessment, data governance, security, fairness testing, human oversight and remedies. This is particularly important where the individual cannot realistically predict how an AI system will transform raw data into consequential inferences.

10. Findings and Conclusion

10.1 Major Findings

- Privacy in the AI era is both an informational and constitutional concern involving dignity, autonomy, liberty and equality.
- The DPDP Act, 2023 materially strengthens India's data-protection framework, but it is not a complete AI-governance statute.
- The Digital Personal Data Protection Rules, 2025 represent an important implementation development and must be considered in any current analysis of Indian data protection.
- AI creates distinctive problems involving inference, profiling, opacity, bias, automated decisions and distributed responsibility that cannot always be solved through conventional consent.
- AI-enabled State surveillance raises constitutional questions that require legality, necessity, proportionality and procedural safeguards.
- The India AI Governance Guidelines provide an important principle-based governance layer and support a risk-sensitive, accountable approach.
- Effective protection depends not only on legal rights but also on institutional capacity, technical standards, auditability and accessible remedies.

Conclusion

Artificial Intelligence is transforming the relationship between individuals, institutions and information. Its capacity to process enormous volumes of personal data can generate substantial public and private benefits, but it also creates the possibility of pervasive profiling, opaque decision-making, discrimination, surveillance and loss of individual control. The legal response must therefore recognise that the AI privacy problem is not simply a question of keeping data secret; it is a question of preserving human agency in an environment in which data can continuously generate new predictions and classifications.

India has established important foundations. The constitutional recognition of privacy in Puttaswamy provides a rights-based standard. The DPDP Act, 2023 provides a dedicated statutory framework, while the Digital Personal Data Protection Rules, 2025 provide implementation detail. The India AI Governance Guidelines add a broader policy architecture for safe, responsible and inclusive AI. These developments demonstrate substantial progress.

At the same time, the research supports the first hypothesis in a qualified form: the Indian framework, considered as a whole, is evolving but does not yet provide a fully comprehensive answer to every AI-specific challenge. In particular, automated decision-making, inferential profiling, algorithmic bias, model accountability and effective contestability require further legal and institutional development. The second hypothesis is also supported: stronger safeguards, risk-sensitive oversight, meaningful human review, auditing and effective remedies can improve rights protection without requiring a blanket prohibition on AI innovation.

The future of Indian AI governance should therefore be based on a balanced techno-legal model. Data protection should be integrated with constitutional rights, equality principles, sectoral regulation, cybersecurity and responsible-AI practices. High-impact AI should attract stronger safeguards than low-risk applications. Organisations should be accountable throughout the lifecycle of AI systems, and individuals should have realistic mechanisms to challenge harmful or inaccurate outcomes.

Ultimately, technological progress is compatible with fundamental rights only when institutions remain capable of supervising technology and individuals remain capable of exercising meaningful control over decisions that affect them. The success of India's digital future will depend not merely on how rapidly AI is adopted, but on whether that adoption is trusted, accountable, inclusive and consistent with human dignity.

References

A. Primary Legal Sources

1. Constitution of India, 1950.
2. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
3. Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.
4. Information Technology Act, 2000.
5. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
6. India AI Governance Guidelines, Ministry of Electronics and Information Technology/IndiaAI Mission, November 2025.

B. Selected Cases

1. Justice KS. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. K.S. Puttaswamy (Retd.) v. Union of India, (2018) 1 SCC 809.
3. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
4. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
5. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
6. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
7. Selvi v. State of Karnataka, (2010) 7 SCC 263.

C. Books and Academic Sources

1. Solove, Daniel J., Understanding Privacy, Harvard University Press.
2. Kulshreshtha, V.D., Data Protection Law in India.
3. Relevant peer-reviewed scholarship on artificial intelligence, algorithmic accountability, privacy, data protection and digital constitutionalism.
4. Indian Journal of Law and Technology and other specialist technology-law literature.

D. Government and Institutional Materials

1. Ministry of Electronics and Information Technology (MeitY), Government of India, Digital Personal Data Protection framework and related notifications.
2. Principal Scientific Adviser/India AI Mission materials concerning AI governance and responsible AI.
3. NIST, Privacy Framework and related AI risk-management materials, used for comparative analytical context.
4. Supreme Court of India judgments and official case materials.