2026 Volume: 02 Issue: 09 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-08

DATA PRIVACY CHALLENGES IN THE USE OF ARTIFICIAL INTELLIGENCE IN INDIA

***Vayada Dixaben Kantubhai**

Haveli Institute of legal Studies and Research, Affiliated to University of Mumbai.

Article Received: 29 July 2026
Article Revised: 19 August 2026
Published on: 09 September 2026

***Corresponding Author: Vayada Dixaben Kantubhai**
Haveli Institute of legal Studies and Research, Affiliated to University of Mumbai.

DOI: https://doi-doi.org/101555/ijrpa.9966

ABSTRACT

The rapid development and use of AI raises important questions about the protection of personal data and individual privacy in India. AI systems often rely on large amounts of personal data for training, analysis and decision-making. This can lead to problems such as excessive data collection, lack of informed consent, data breaches, profiling, surveillance and lack of transparency. The main objective of this research article is to study the main challenges of data privacy arising from the use of AI in India, as well as to analyze the current legal framework for the protection of personal data and privacy. This study mainly uses doctrinal, legal research methodology, in which laws, judicial decisions, government materials, as well as other relevant secondary sources have been studied. The focus is particularly on the constitutional rights to privacy, as well as the Digital Personal Data Protection Act 2023. This study shows that despite the significant legal framework for data protection in India, some new challenges are emerging with the continued development of AI. Hence, effective consent, data security, transparency, and accountability are needed to maintain a balance between privacy and technological innovation.

KEYWORDS: Artificial Intelligence, Data Privacy, Personal Data, Data Protection, Digital Personal Data Protection Act, 2023, Privacy Rights, AI Regulation

INTRODUCTION

AI is one of the most important technological developments of recent times, and its use in India is rapidly increasing in various sectors such as education, healthcare, governance, finance, communication, and digital services. AI systems rely on large amounts of data to analyze information, make predictions, and make decisions. The excessive use of personal

information in AI is raising important questions about the privacy of individuals and the security of personal information.

AI can collect, process, store, and analyze large amounts of personal information when used. This leads to lack of informed consent, excessive data collection, data breaches, profiling, surveillance, lack of transparency, and difficulty in determining liability for misuse of personal information, as well as privacy-related issues. Such problems are becoming more important as AI technology continues to develop.

Privacy is recognized as a fundamental right in India under Article 21 of the Constitution, notably through the Supreme Court's decision in Justice K. S. Puttaswamy vs. Union of India. India has also introduced the Digital Personal Data Protection Act, 2023, which provides a legal framework for the protection of digital personal data. However, the rapid and complex development of AI raises questions as to whether the current legal framework can adequately address the new privacy risks associated with AI? The purpose of this article is to analyze the key data privacy challenges arising from the use of AI in India, as well as to study the recent legal framework applicable to such challenges.

This article focuses on the need for safeguards, transparency, and accountability to strike a balance between technological innovation and the fundamental right to privacy of individuals.

Research Objectives

1. To study the issues raised by the use of AI in India regarding data privacy challenges.
2. To analyse the current Indian legal framework for the protection of personal information and privacy in the context of AI.
3. To identify effective legal safeguards and reforms needed to strike a balance between the development of AI and the right to privacy of individuals.

Research Questions

1. What are the key data privacy challenges raised by the use of AI in India?
2. Is the current Indian legal framework adequate to address the issues and concerns raised by the use of AI regarding data privacy?
3. What legal safeguards and reforms are needed to encourage the development and use of AI in India while protecting privacy?

Research Methodology

This research article adopts a theoretical as well as a qualitative legal research methodology. The study mainly relies on the analysis of existing laws, judicial decisions, government materials and academic literature related to AI and data privacy in India. Primary sources include the Constitution of India, relevant legal provisions, especially the Digital Personal Data Protection Act, 2023, and important judicial decisions related to privacy and data security. Secondary sources include books, research articles, law journals, reports, as well as reliable, online legal, and academic resources. This research analyzes the main privacy challenges associated with the collection, processing, and use of personal information by AI systems. It also analyzes the adequacy of the current Indian legal framework to address new challenges, and identifies the need for stronger safeguards and legal reforms. This study, which is analytical in nature, aims to provide an understanding of the balance between technological innovation, protection of individual privacy, and accountability.

AI and Data Privacy: Conceptual Framework.

AI provides a framework for technologies and computer systems that can perform tasks that are specifically human-like, such as learning, analyzing information, recognizing patterns, making predictions, and assisting in decision-making. AI systems often rely on large amounts of data to train algorithms and improve their performance. This data can include a person's name, contact details, location, online activities, preferences, and other personal information about an individual.

Data privacy is the protection of an individual's personal information, as well as the individual's proper control over how such information is collected, used, stored, and shared. Data privacy is an important part of the digital environment, as personal data can be stored and processed in large quantities.

Therefore, there is an important relationship between AI and data privacy. AI systems can collect and process large amounts of personal data for activities such as automated decision-making, recommendation systems, profiling, and predictions. Such data processing can provide technological as well as societal benefits, but it can also pose privacy risks. Individuals may not always be fully aware of how their information is being used, or may find it difficult to fully understand the consequences of AI processing their data.

The key challenges of AI are to strike the right balance between the benefits and the protection of individual privacy. Effective data protection principles such as transparency with informed consent, purpose limitations, data protection, and accountability are therefore

important for the responsible use of AI. Understanding this relationship between AI and its data privacy can help better analyze the legal as well as practical data privacy challenges that arise from the use of AI in India.

Legal Framework for Data Privacy in India

The legal framework governing data privacy in India is based on constitutional principles, statutory provisions and judicial decisions. Legal safeguards have become more important due to the rapid development of AI, as AI systems can collect and analyze personal data on a large scale.

8.1. Right to Privacy under the Constitution of India.

The right to privacy has been recognized as a fundamental right under Article 21 of the Constitution of India. The Supreme Court in the case of Justice K. S. Puttaswamy vs. Union of India considered privacy as an important part of the right to life and personal liberty. This decision recognized the right of an individual to protect his personal information and autonomy. These constitutional safeguards are especially important in the context of the processing of personal data by AI systems.

8.2. Digital Personal Data Protection Act, 2023.

Digital Personal Data Protection Act, 2023 is the main law related to the processing of digital personal data in India. This Act provides a legal framework for the processing of personal data and recognizes the need to protect the privacy of individuals. This Act sets out certain responsibilities for entities processing personal data and certain rights for individuals with respect to their personal data. This Act becomes an important part when personal data is collected and processed by AI systems.

8.3. Information Technology Act, 2000.

The Information Technology Act, 2000 and its related rules also play an important role in regulating electronic data and protecting certain types of personal data. Although this Act was enacted before the advent of modern AI, it is part of India's dual digital and data security framework.

8.4. Importance of Judicial Decisions

Indian courts have played a significant role in the development of privacy principles. Various judicial decisions have emphasized the importance of privacy, dignity, autonomy, and protection of personal information. These principles provide guidance for understanding the lawfulness of data processing through emerging technologies such as AI.

8.5. Relevance for AI

Currently, the Indian legal framework provides important safeguards for privacy, as well as personal data. However, the use of AI raises new and complex issues related to automated processing, profiling, transparency, consent, and liability. Therefore, proper application of existing privacy principles for AI systems and further legal and regulatory development, where necessary, are required.

(9) Key Data Privacy Challenges in the Use of Artificial Intelligence

The excessive use of AI in India has raised several challenges regarding the collection, processing, and security of personal data.

• The main data privacy challenges are as follows:

9.1. Lack of informed consent.

AI systems can collect and process large amounts of personal data, while the individual has no knowledge of how their information will be used. Complicated privacy policies, as well as unclear information, can make it difficult for an individual to give proper informed consent.

9.2. Excessive collection and use of personal data

AI systems often require large amounts of data sets for training and improving performance. Collecting more personal data than necessary can increase privacy risks, as well as create possibilities for data misuse or unauthorized processing.

9.3. Lack of transparency.

AI systems are often based on complex, algorithms that can be difficult for the average person to understand. This makes it difficult for individuals to understand what data is being processed, why it is being processed, and how AI-based decisions are being made.

9.4. Data security and data breaches.

AI systems can store and process large amounts of personal information. Weak security measures, cyberattacks, or unauthorized access can lead to data breaches, causing serious harm to individuals.

9.5. Profiling and surveillance.

AI can analyze personal data to identify patterns, make predictions about individuals, and create profiles of individuals. Excessive profiling and surveillance can impact an individual's autonomy and privacy, especially when the individual is unaware of such practices.

9.6. Bias and Discrimination

AI systems trained on incomplete or biased data sets can produce unfair results. When personal data is used for automated decision-making, such results can affect individual rights and raise concerns about fairness and privacy.

9.7. Responsibilities

Determining liability for AI-related privacy violations can be difficult, as it can involve multiple actors, such as AI developers, service providers, and organizations using AI systems. Hence, clear responsibilities are needed for effective protection of personal data. These challenges highlight the need for strong privacy, security measures, responsible data processing, and effective accountability mechanisms for the use of AI.

Therefore, there is a need to properly implement the current legal framework in India, keeping in mind the evolving privacy risks associated with AI, and to further develop it where necessary.

Critical Analysis of the Current Indian Legal Framework:

India has developed a significant legal framework for privacy, as well as the protection of personal data, notably through the constitutional recognition of the right to privacy and the Digital Personal Data Protection Act, 2023. However, the rapid development of AI has raised some challenges that the existing legal framework cannot necessarily address.

The existing legal framework provides important principles such as consent, protection of personal data, and responsibilities. But these principles can be difficult to apply in practice to AI systems. AI can process large amounts of data, make predictions, and create profiles of individuals, processes that can be difficult for ordinary individuals to understand.

As a result, meaningful consent, as well as transparency, can be difficult to maintain. Accountability also poses a significant concern. When privacy is breached by AI-based systems, it can be difficult to determine liability between the organisations using the system, the developer, and other entities involved in the data processing. Similarly, profiling, as well as automated decision-making, can also pose a risk of unfair or discriminatory outcomes.

Thus, the current Indian legal framework provides a strong basis for data privacy protection, but may require further development to address the new and evolving risks associated with AI. Greater transparency, meaningful consent, data protection obligations, and additional safeguards may be necessary for high-risk AI applications.. A balanced approach is needed to ensure that technological innovation is not necessarily inhibited while protecting individual privacy.

Instructions and Recommendations

1. Strengthen informed consent.

There should be a clear, simple, and meaningful consent mechanism for data processing through AI. So that the individual is aware of how their personal data will be used.

2. Improve transparency.

Organizations using AI should provide simple, understandable information about data collection, processing, and, where necessary, AI-based decision-making.

3. Ensure strong data security.

Appropriate technical and organizational security measures should be adopted to prevent unauthorized access, misuse, and data breaches.

4. Define clear responsibilities.

Responsibilities should be clearly defined between organizations involved in the processing of personal data, AI developers, and other relevant entities.

5. Protection against profiling and bias.

High-risk AI applications should have appropriate safeguards in place to mitigate excessive profiling, as well as unfair or discriminatory outcomes.

6. Develop AI-specific privacy protections.

India should continue to develop clear legal and regulatory safeguards to address the unique and evolving privacy risks of AI, while also promoting responsible innovation.

CONCLUSION

The widespread use of AI in India has created many opportunities for technological development, but it can also raise important questions about the protection of personal data and personal privacy.. AI systems rely heavily on data for training, analysis, predictions, and decision-making, which can lead to risks such as lack of informed consent, excessive data collection, data breaches, profiling, lack of transparency, and difficulty in determining responsibilities.

India has taken important steps to protect privacy and personal data by constitutionally recognizing the right to privacy and through the Digital Personal Data Protection Act, 2023. However, the ever-changing nature of AI is giving rise to new and complex privacy concerns, which may require more specific and effective safeguards. The legal framework in recent times provides a basis for data protection, but its effective application to AI-based data processing is still a major step.

The study concludes that privacy protection and the development of AI, rather than being seen as conflicting objectives, need to strike a balance between the two. India should promote technological innovation while ensuring responsible collection and processing of personal data. Strong consent mechanisms, transparency, data protection, accountability, as well as privacy protections against harmful profiling and biased outcomes can make protection more effective.

Finally, effective regulation of AI should not necessarily hinder technological progress while protecting individual rights. A flexible, and ever-evolving legal framework will be required to address new privacy risks related to AI, and to maintain public trust in the responsible use of AI in India.

REFERENCES

1. The Constitution of India, art. 21.
2. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
3. The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023.
4. The Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000.
5. Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Act, 2023, Government of India, 2023.
6. United Nations Educational, Scientific and Cultural Organization (UNESCO), Recommendation on the Ethics of Artificial Intelligence (2022).
7. UNESCO, “Ethics of Artificial Intelligence,” UNESCO, 2026.
8. India Code, The Information Technology Act, 2000, Government of India.
9. Ministry of Electronics and Information Technology, Government of India, Acts and Policies, Government of India.