

International Journal Research Publication Analysis

Page: 01-12

ARTIFICIAL INTELLIGENCE AND FUNDAMENTAL RIGHTS IN INDIA: A CONSTITUTIONAL ANALYSIS OF PRIVACY, EQUALITY AND DUE PROCESS

***Mahima Yadav**

Haveli Institute of Legal Studies & Research.

Article Received: 27 July 2026

*Corresponding Author: Mahima Yadav

Article Revised: 17 August 2026

Haveli Institute of Legal Studies & Research.

Published on: 07 September 2026

DOI: <https://doi-doi.org/101555/ijrpa.4419>

ABSTRACT

Artificial Intelligence (AI) is rapidly transforming modern society. It is increasingly used in healthcare, education, finance, employment, policing, public administration, communication and commercial activities. While Artificial Intelligence provides significant opportunities for economic and social development, its increasing use also raises serious questions concerning constitutional rights. Automated decision-making, algorithmic profiling, facial recognition, predictive policing and large-scale data processing may directly affect an individual's equality, liberty, privacy and dignity.

The Constitution of India was enacted long before the emergence of modern Artificial Intelligence. However, its fundamental rights framework is sufficiently broad to address technological developments that affect constitutional values. Articles 14, 19 and 21 are particularly relevant to AI governance. Article 14 protects individuals against arbitrary and discriminatory State action; Article 19 protects important freedoms including freedom of speech and expression; and Article 21 has been judicially interpreted to protect dignity, autonomy and privacy.

This paper examines the constitutional implications of Artificial Intelligence in India with particular emphasis on privacy, equality and procedural fairness. It analyses the landmark decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, in which the Supreme Court recognised privacy as a constitutionally protected right. The paper also considers India's Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025. It argues that data protection alone cannot address all AI-related constitutional

concerns. Algorithmic transparency, accountability, human oversight, non-discrimination and effective remedies are equally important.

The paper concludes that India should adopt a rights-based approach to Artificial Intelligence in which innovation is encouraged but technological power remains subject to constitutional principles of dignity, equality, liberty, proportionality and rule of law.

KEYWORDS: Artificial Intelligence, Fundamental Rights, Article 14, Article 19, Article 21, Privacy, Equality, Algorithmic Bias, Data Protection, Due Process.

1. INTRODUCTION

Artificial Intelligence has moved rapidly from a specialised technological field into everyday life. AI systems can now analyse large quantities of information, recognise patterns, generate content, make recommendations and assist in decision-making. Governments, companies and individuals increasingly rely on AI-based systems for activities that previously required direct human involvement.

The development has significant benefits. AI can assist doctors in analysing medical information, support students through personalised learning, help businesses identify fraud, improve public administration and contribute to scientific research. For a country such as India, with a large population and rapidly expanding digital infrastructure, AI may provide important opportunities for development.

However, technological progress also creates legal risks.

An AI system may classify an individual, predict behaviour, assess risk or influence an important decision without the affected person understanding how the result was produced. Where such systems are used in employment, credit, policing, welfare or public administration, an incorrect or discriminatory result can have serious consequences.

This creates a fundamental legal question: **Can constitutional rights effectively protect individuals when decisions affecting them are increasingly influenced by algorithms?**

The answer requires an examination of India's existing constitutional framework.

The Constitution does not contain a specific provision dealing with Artificial Intelligence. Nevertheless, fundamental rights are principles designed to protect human beings against unjustified exercises of power. Therefore, technological change does not automatically place AI outside constitutional scrutiny.

Articles 14, 19 and 21 are particularly relevant. Equality, freedom, privacy, dignity and personal autonomy may all be affected by AI.

2. Research Problem

The rapid development of AI has created situations in which existing laws may not provide sufficiently specific answers to new technological problems.

The central research problem is whether India's existing constitutional and legal framework adequately protects individuals from AI-related harms, particularly algorithmic discrimination, privacy violations, surveillance and unfair automated decision-making.

The issue is especially important where AI is used by State authorities. The State cannot escape constitutional responsibility merely because a decision has been generated or assisted by a computer system.

3. Research Questions

1. What constitutional principles govern the use of Artificial Intelligence in India?
2. How can Article 14 address algorithmic discrimination?
3. How does AI affect privacy and personal autonomy under Article 21?
4. What constitutional safeguards should apply to AI-enabled surveillance?
5. How can individuals challenge harmful automated decisions?
6. Is India's existing data-protection framework sufficient to address AI-related risks?
7. What safeguards are necessary for rights-based AI governance?

4. Objectives of the Research

The objectives of this study are:

- To examine the constitutional implications of Artificial Intelligence in India.
- To analyse the relationship between AI and Articles 14, 19 and 21.
- To examine algorithmic discrimination and its relationship with equality.
- To analyse the impact of AI on privacy, dignity and autonomy.
- To examine AI-enabled surveillance.
- To study the relevance of data-protection law to AI.
- To identify gaps in the existing legal framework.
- To suggest safeguards for constitutional AI governance.

5. Research Methodology

This research adopts a doctrinal and analytical methodology. It relies primarily on constitutional provisions, judicial decisions, legislation, official government documents and academic literature.

The research examines relevant Supreme Court jurisprudence relating to privacy, equality, dignity, liberty and proportionality. It also considers India's digital personal data protection framework and contemporary technological challenges.

The study is qualitative in nature and does not involve primary empirical research.

6. Artificial Intelligence and Article 14

Article 14 guarantees equality before law and equal protection of laws. It also acts as an important constitutional safeguard against arbitrary State action.

Artificial Intelligence creates a new form of equality concern: **algorithmic bias**.

AI systems learn patterns from data. If the data used to develop an algorithm contains historical discrimination, the system may reproduce those patterns.

For example, an automated recruitment system trained on historically biased employment data could unintentionally favour one category of candidates over another. Similarly, an algorithm used for risk assessment could produce discriminatory outcomes if the underlying data reflects social or institutional bias.

The fact that discrimination is produced through technology does not make it constitutionally acceptable.

6.1 Algorithmic Bias

Algorithmic bias may arise from:

- Biased training data;
- Incomplete data;
- Incorrect assumptions;
- Unequal representation;
- Flawed design;
- Inappropriate variables; or
- Discriminatory historical patterns.

The constitutional problem becomes more serious when the State relies upon such systems.

A government authority cannot avoid Article 14 scrutiny by transferring part of its decision-making process to an algorithm.

6.2 Transparency

Equality requires individuals to have a meaningful opportunity to challenge discriminatory treatment.

If an AI system is completely opaque, an affected person may not know why a decision was made. Therefore, transparency becomes an important component of constitutional accountability.

Where AI is used for high-impact decisions, sufficient information should be available to enable meaningful review.

7. Artificial Intelligence and Article 19

AI can affect freedom of speech and expression in several ways.

Social-media platforms use automated systems to recommend, rank and sometimes remove content. These systems can significantly influence the information individuals see.

AI-generated misinformation and deepfakes create genuine challenges for public discourse. At the same time, excessive regulation of AI-generated content may interfere with legitimate expression.

Therefore, AI regulation must balance the prevention of serious harm with constitutional protection of free expression.

Any restriction on speech must remain consistent with Article 19(2) and established constitutional principles.

The key concern is transparency. Users should, where appropriate, know when automated systems significantly influence the visibility or removal of content.

8. Artificial Intelligence and Article 21

Article 21 provides that no person shall be deprived of life or personal liberty except according to procedure established by law.

Judicial interpretation has transformed Article 21 into a broad protection of human dignity and personal liberty.

AI may affect Article 21 through:

- Collection of personal information;
- Biometric identification;
- Facial recognition;
- Digital surveillance;
- Automated profiling;
- Predictive policing;
- Automated decision-making; and
- Misuse of personal data.

The constitutional significance of AI therefore extends beyond technology and enters the domain of individual liberty.

9. Right to Privacy and AI

The most important constitutional authority in this area is *Justice K.S. Puttaswamy (Retd.) v. Union of India*.

The Supreme Court recognised privacy as a fundamental right and connected it with dignity, liberty and autonomy. The Court identified, among other dimensions, informational privacy and privacy of choice. (SCI API)

This principle has direct relevance to Artificial Intelligence.

AI systems frequently require large quantities of data. Information about an individual's location, communication, preferences, financial behaviour and online activities may be collected and analysed.

The concern is not merely that information may be disclosed. AI can also generate new conclusions from information.

For example, seemingly ordinary data may be combined to create a detailed profile of an individual. This creates what may be described as an **inference problem**: information that an individual never consciously disclosed may nevertheless be predicted from other data.

Therefore, privacy protection must address both collection and inference.

10. Informational Privacy

Informational privacy concerns an individual's ability to exercise control over personal information.

The Supreme Court's privacy jurisprudence recognises informational privacy as a constitutionally significant interest. (SCI API)

In the AI environment, informational privacy is challenged by:

- Extensive data collection;
- Profiling;
- Data aggregation;
- Automated inference;
- Cross-platform data processing; and
- Long-term retention.

The individual may not always know how information provided for one purpose is later used for another.

Therefore, purpose limitation, transparency and meaningful control become important principles.

11. AI-Enabled Surveillance

AI has greatly increased the capacity of surveillance systems.

Facial recognition, biometric identification and automated analytics can enable authorities to monitor and identify individuals at large scale.

Surveillance may serve legitimate objectives such as preventing crime or protecting national security. However, surveillance can also interfere with privacy and create a chilling effect on individual behaviour.

A person who believes that every movement or communication is being monitored may become less willing to express opinions or participate freely in society.

Therefore, surveillance must be governed by clear legal authority and constitutional safeguards.

The principle should be simple: **the existence of technological capability does not itself create legal authority.**

12. Proportionality and AI

The principle of proportionality is especially relevant where AI interferes with fundamental rights.

A restriction should have a legitimate objective and should use means reasonably connected to that objective. The interference should not be excessive.

For example, if facial recognition is used for a legitimate security purpose, the law must consider:

- Whether the use is authorised by law;
- Whether the objective is legitimate;
- Whether the technology is necessary;
- Whether less intrusive alternatives exist;
- How accurate the technology is;
- How data is stored;
- Who can access it; and
- What remedy exists for wrongful identification.

Proportionality prevents technological convenience from becoming an excuse for excessive interference with rights.

13. AI and Due Process

Automated decision-making creates a procedural fairness problem.

Suppose an AI system produces an adverse decision against an individual. The individual may want to know:

- What information was used?
- Why was the decision made?
- Was the information accurate?
- Was the algorithm biased?
- Who is responsible?
- Can the decision be reviewed?

If there is no meaningful answer, the individual may have no effective way to challenge the decision.

Therefore, high-impact AI systems should include:

1. Meaningful human review;
2. Mechanisms for correction of inaccurate data;
3. Explanations appropriate to the circumstances;
4. Complaint mechanisms; and
5. Accessible remedies.

Technology should not eliminate procedural fairness.

14. Digital Personal Data Protection Framework

India enacted the Digital Personal Data Protection Act, 2023 to establish a statutory framework relating to digital personal data. The Ministry of Electronics and Information Technology maintains the Act and related materials on its official website. (MeitY)

The framework is highly relevant to AI because AI systems often depend upon personal data. The Digital Personal Data Protection Rules, 2025 were officially notified on 14 November 2025. MeitY also published an enforcement timeline and material concerning the Data Protection Board. (MeitY)

The data-protection framework is an important development, but it should not be treated as a complete AI law.

Data protection primarily concerns processing of personal data, while AI creates additional issues involving:

- Algorithmic bias;
- Explainability;
- Automated decisions;
- Ai-generated content;
- Accountability;
- Safety; and
- High-risk uses.

Therefore, India may require complementary principles specifically addressing high-risk AI applications.

15. AI in Criminal Justice

AI may be used in criminal investigation and law enforcement for facial recognition, pattern analysis and other forms of technological assistance.

These technologies may improve efficiency, but errors can have serious consequences.

An incorrect identification may affect an innocent person's liberty and reputation.

AI output should therefore not automatically be treated as conclusive evidence.

Human verification, corroboration and judicial scrutiny remain essential.

The criminal justice system must preserve the presumption of innocence and procedural fairness even when advanced technology is used.

16. AI and Children

Children are particularly vulnerable to digital technologies.

AI-powered platforms may collect information about children's activities and preferences.

Children may also lack the maturity necessary to understand long-term privacy consequences.

Therefore, stronger safeguards are necessary for children's personal data.

AI systems directed towards children should be designed with privacy, safety and age-appropriate protections.

17. Challenges in the Existing Framework

Several challenges remain.

17.1 Absence of a Comprehensive AI Law

India's legal framework is developing, but AI-specific regulation remains an evolving area.

17.2 Algorithmic Opacity

Individuals may find it difficult to understand automated decision-making.

17.3 Accountability Gap

It may be unclear whether responsibility lies with the developer, deployer or institution using the AI system.

17.4 Bias

AI can reproduce discriminatory patterns in training data.

17.5 Privacy

Large-scale data processing creates significant informational privacy concerns.

17.6 Lack of Effective Remedies

Individuals may struggle to challenge automated decisions.

18. Recommendations

18.1 Human Oversight

AI should not be allowed to make final high-impact decisions affecting fundamental rights without meaningful human review.

18.2 Algorithmic Impact Assessments

High-risk AI systems should undergo assessments concerning privacy, equality and discrimination.

18.3 Transparency

Individuals should receive sufficient information to understand significant automated decisions.

18.4 Accountability

Responsibility for AI-related harm should be clearly allocated.

18.5 Anti-Discrimination Testing

AI systems should be tested for discriminatory outcomes before and after deployment.

18.6 Privacy by Design

Privacy safeguards should be incorporated during the design stage rather than added after deployment.

18.7 Effective Remedies

Affected individuals should have accessible complaint and review mechanisms.

18.8 Judicial Oversight

Use of AI by public authorities should remain subject to constitutional review.

19. FINDINGS

The research establishes that Artificial Intelligence can significantly affect fundamental rights.

First, AI can create new forms of discrimination, making Article 14 highly relevant.

Second, large-scale data processing and profiling create serious privacy concerns under Article 21.

Third, AI-enabled surveillance can affect liberty and create a chilling effect.

Fourth, automated decision-making creates procedural fairness concerns.

Fifth, the Digital Personal Data Protection framework provides an important foundation but does not by itself resolve all AI-related constitutional issues.

Finally, constitutional principles must remain applicable irrespective of whether a decision is made by a human being, an algorithm or a combination of both.

20. CONCLUSION

Artificial Intelligence has the potential to transform India. Its applications may improve public administration, healthcare, education, commerce and criminal investigation.

However, technological progress must remain consistent with constitutional democracy.

The Constitution does not become irrelevant because decision-making becomes automated.

On the contrary, constitutional principles become more important when technological systems acquire greater power over individual lives.

Article 14 can provide protection against discriminatory and arbitrary algorithmic outcomes.

Article 19 remains relevant where AI affects freedom of expression. Article 21 provides a strong foundation for protecting privacy, dignity and autonomy.

The Supreme Court's privacy jurisprudence, particularly *Justice K.S. Puttaswamy (Retd.) v. Union of India*, demonstrates that constitutional rights can respond to changing technological realities. (SCI API)

India's data-protection framework is an important step, but future AI governance should go further by addressing algorithmic bias, transparency, accountability, human oversight and effective remedies.

The objective should not be to stop innovation. It should be to ensure responsible innovation. **Artificial Intelligence may be capable of making predictions, identifying patterns and processing enormous quantities of information, but it must remain subject to human dignity, constitutional liberty and the rule of law.**

The future of AI governance in India should therefore follow one central principle:

Technology must serve constitutional democracy, and not replace it.

REFERENCES

1. Constitution of India, Articles 14, 19 and 21.
2. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. (Supreme Court of India)
3. Digital Personal Data Protection Act, 2023. (MeitY)
4. Digital Personal Data Protection Rules, 2025. (MeitY)
5. Ministry of Electronics and Information Technology, Government of India, official materials on data protection. (MeitY)
6. Supreme Court of India, judgments concerning privacy, dignity, autonomy and fundamental rights. (SCI API)