INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 3 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 3 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-3-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

ARTIFICIAL INTELLIGENCE AND LAW: IS THE INDIAN LEGAL FRAMEWORK READY?

AUTHOR – TEJAS R GOWDA, STUDENT AT CHRIST DEEMED TO BE UNIVERSITY

BEST CITATION – TEJAS R GOWDA, ARTIFICIAL INTELLIGENCE AND LAW: IS THE INDIAN LEGAL FRAMEWORK READY?, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (3) OF 2026, PG. 617-628, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/JPRB7370

ABSTRACT

Artificial Intelligence (AI) is increasingly transforming governance, public administration, and law enforcement across the globe. Governments are integrating algorithmic systems into decision-making processes in order to improve efficiency, optimize resource allocation, and enhance security mechanisms. In India, artificial intelligence technologies such as facial recognition systems, predictive policing tools, and advanced data analytics platforms are gradually becoming embedded within law enforcement frameworks. While these technological innovations promise enhanced public safety and improved efficiency in criminal investigations, they simultaneously raise significant legal, ethical, and constitutional concerns.

Despite the rapid adoption of AI technologies, India currently lacks a comprehensive legal framework governing the development, deployment, and accountability of artificial intelligence systems. Existing legislation such as the Information Technology Act, 2000, the Consumer Protection Act, 2019, and the Digital Personal Data Protection Act, 2023 provide only fragmented regulatory oversight. These statutes were enacted before the widespread emergence of sophisticated algorithmic systems and therefore fail to address the complex legal challenges associated with modern AI technologies.

This research paper examines the readiness of the Indian legal framework to regulate artificial intelligence technologies used in law enforcement, with particular emphasis on facial recognition systems. The study evaluates the constitutional implications of AI-based surveillance technologies under Articles 14 and 21 of the Constitution of India, focusing on the protection of equality, privacy, and personal liberty. Through doctrinal legal analysis and comparative evaluation of international regulatory models—particularly the European Union's proposed Artificial Intelligence Act—the paper identifies significant gaps in India's regulatory approach.

The research argues that the absence of comprehensive legal safeguards governing artificial intelligence creates a regulatory vacuum that may facilitate arbitrary state action and undermine fundamental rights. To address these concerns, the paper proposes the enactment of dedicated artificial intelligence legislation, the establishment of independent oversight authorities, and the implementation of transparency and accountability mechanisms governing algorithmic systems. Ultimately, the paper concludes that India must urgently develop a balanced regulatory framework that promotes technological innovation while safeguarding constitutional freedoms and democratic values.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Chapter 1: Introduction

1.1 Background and Emergence of Artificial Intelligence

Artificial Intelligence has emerged as one of the most significant technological innovations of the modern era. The concept of artificial intelligence refers to computer systems designed to perform tasks that typically require human intelligence, including learning, reasoning, problem-solving, and decision-making. With advancements in machine learning, neural networks, and computational infrastructure, artificial intelligence systems have become capable of processing vast volumes of data and generating predictions with remarkable accuracy.

The increasing digitization of modern societies has provided the necessary foundation for the development of artificial intelligence. Governments, corporations, and individuals generate enormous amounts of data through digital interactions, online platforms, and automated systems. Artificial intelligence technologies utilize this data to identify patterns, make predictions, and automate decision-making processes.

In governance, artificial intelligence has emerged as a tool capable of enhancing efficiency, reducing administrative burdens, and improving public service delivery. Governments across the world increasingly rely on AI-driven technologies for a variety of purposes, including tax administration, welfare distribution, transportation planning, disaster management, and healthcare monitoring.

Artificial intelligence technologies allow governments to analyze complex datasets and generate insights that can inform policymaking. For example, machine learning algorithms can identify trends in economic activity, public health patterns, and environmental changes, enabling policymakers to design more effective policies.

However, the integration of artificial intelligence into governance structures also raises important questions regarding accountability and transparency. When decisions affecting individuals are made by automated systems, it becomes necessary to examine how such systems operate and whether they comply with constitutional and legal safeguards.

1.2 Artificial Intelligence in Law Enforcement

The use of artificial intelligence in law enforcement represents one of the most significant technological developments in modern policing. Law enforcement agencies increasingly rely on advanced technological tools to combat crime, enhance surveillance capabilities, and analyze criminal data.

Artificial intelligence technologies have introduced new approaches to policing that emphasize predictive analysis and data-driven decision-making. These systems analyze historical crime data, geographic information, and demographic patterns in order to identify areas where criminal activity is likely to occur.

One widely discussed application of artificial intelligence in policing is predictive policing. Predictive policing systems use machine learning algorithms to analyze past crime data and generate predictions regarding future criminal activity. Law enforcement agencies can use these predictions to allocate police resources more efficiently.

Artificial intelligence is also used in criminal investigations, where machine learning algorithms assist investigators in analyzing digital evidence, identifying suspicious patterns, and linking criminal networks.

Another important application of artificial intelligence in law enforcement is facial recognition technology. Facial recognition systems enable authorities to identify individuals by analyzing facial features captured through surveillance cameras or digital images.

The increasing adoption of these technologies

reflects a broader shift toward technological policing strategies that rely on automated systems to support law enforcement decision-making.

1.3 Facial Recognition Technology

Facial recognition technology is one of the most widely used forms of biometric identification. The technology operates by analyzing unique facial characteristics and comparing them with stored images in databases.

Facial recognition systems typically involve three key stages. The first stage involves detecting a face within an image or video frame. Once a face is detected, the system extracts unique facial features such as the distance between eyes, nose structure, and jawline shape. These features are then converted into a digital representation known as a facial template.

In the final stage, the system compares the facial template with existing images stored in databases to identify potential matches. Advanced facial recognition systems can process large volumes of images in real time, enabling authorities to identify individuals quickly.

In law enforcement contexts, facial recognition technology can be used for several purposes. Authorities may use these systems to identify criminal suspects, locate missing persons, verify identities during investigations, and monitor public spaces for security threats.

In India, facial recognition technologies have been deployed by several state police departments during large public events and security operations. Authorities have also experimented with these technologies to identify individuals involved in criminal activities or to track missing children.

While the use of facial recognition technology may enhance investigative capabilities, it also raises significant legal and constitutional concerns.

1.4 The Problem of Mass Surveillance

One of the most controversial aspects of facial recognition technology is its potential to enable mass surveillance. When combined with extensive networks of CCTV cameras and government databases, facial recognition systems can allow authorities to monitor individuals in public spaces continuously.

Mass surveillance technologies can significantly alter the relationship between citizens and the state. Individuals may become subject to constant monitoring without their knowledge or consent. This raises concerns regarding the erosion of privacy and personal autonomy in democratic societies.

Surveillance technologies may also create a chilling effect on civil liberties. Citizens who believe that their activities are constantly monitored may hesitate to participate in protests, political demonstrations, or other forms of civic engagement.

The potential for misuse of surveillance technologies has raised concerns among civil liberties organizations and legal scholars. Without proper legal safeguards, facial recognition technologies may be used in ways that undermine fundamental rights.

1.5 Algorithmic Bias and Discrimination

Artificial intelligence systems are heavily dependent on the datasets used to train them. If these datasets contain biases or fail to represent diverse populations, the resulting algorithms may produce discriminatory outcomes.

Several studies conducted internationally have revealed that facial recognition systems often exhibit higher error rates when identifying individuals belonging to certain demographic groups. In particular, facial recognition algorithms have been shown to perform less accurately when identifying women and individuals with darker skin tones.

These biases arise because many training

datasets are dominated by images of certain demographic groups, resulting in algorithms that are more accurate at identifying individuals from those groups.

In law enforcement contexts, algorithmic bias can have serious consequences. Misidentification by facial recognition systems may lead to wrongful arrests, unjustified surveillance, or discriminatory targeting of certain communities.

Such outcomes may violate constitutional principles of equality and non-discrimination. Ensuring fairness and accountability in artificial intelligence systems therefore represents an important challenge for policymakers.

Chapter 2: Literature Review

2.1 Scholarly Perspectives on Artificial Intelligence Governance

The rapid development of artificial intelligence has generated extensive academic debate regarding its legal and ethical implications. Scholars across disciplines such as law, computer science, and political science have examined the impact of AI technologies on governance and society.

Early research on artificial intelligence primarily focused on technological capabilities and economic benefits. Scholars emphasized the potential of AI to drive economic growth, improve productivity, and transform industries.

However, as artificial intelligence systems became integrated into decision-making processes that affect individuals, scholars began to examine the ethical and legal implications of algorithmic governance.

Legal scholars have highlighted several concerns associated with artificial intelligence, including lack of transparency, algorithmic bias, accountability gaps, and privacy violations.

2.2 Algorithmic Transparency and Accountability

One of the most important issues identified in academic literature is the lack of transparency in artificial intelligence systems. Many machine learning algorithms operate as "black box" systems, meaning that their decision-making processes are not easily understood.

The lack of transparency creates challenges for accountability. When an AI system produces a harmful outcome, it may be difficult to determine who is responsible for that outcome.

Some scholars argue that algorithmic decision-making should be subject to transparency requirements that allow individuals and regulators to understand how decisions are produced.

Others propose the development of explainable artificial intelligence systems that provide clear explanations for automated decisions.

2.3 Artificial Intelligence Regulation in India

In the Indian context, discussions surrounding artificial intelligence governance have largely focused on technological innovation and economic development. Government policy initiatives emphasize the importance of artificial intelligence in sectors such as healthcare, agriculture, and smart cities.

However, legal scholars have raised concerns regarding the absence of comprehensive regulatory frameworks governing artificial intelligence technologies.

Existing laws in India were enacted before the widespread emergence of modern AI systems and therefore fail to address issues such as algorithmic accountability, automated decision-making, and biometric surveillance.

The literature therefore highlights the urgent need for regulatory mechanisms that ensure responsible use of artificial intelligence while protecting fundamental rights.

Chapter 3: Research Objectives

The increasing integration of artificial intelligence technologies into law enforcement activities raises important legal and constitutional questions. Despite the rapid deployment of these technologies, there remains considerable uncertainty regarding their regulation within the Indian legal framework. This research therefore aims to examine the legal implications of artificial intelligence technologies used in law enforcement and to assess the adequacy of existing regulatory mechanisms.

The primary objective of this research is to analyze the extent to which Indian law is prepared to regulate the use of artificial intelligence technologies in policing and criminal investigations.

While artificial intelligence offers several potential benefits in enhancing law enforcement efficiency, its deployment also raises significant concerns regarding privacy, discrimination, and accountability. This research therefore seeks to evaluate the compatibility of such technologies with constitutional principles.

A second objective of this research is to examine the constitutional implications of facial recognition technology under Articles 14 and 21 of the Constitution of India. Facial recognition systems rely on biometric identification and automated decision-making processes that may significantly affect individual rights. By examining relevant judicial precedents and constitutional doctrines, this research aims to evaluate whether such technologies comply with the constitutional guarantees of equality, privacy, and personal liberty.

A third objective is to identify the gaps that exist within India's current legal framework governing artificial intelligence technologies. Although several statutes address aspects of digital governance and data protection, none of these laws provide a comprehensive framework for regulating algorithmic decision-making systems used by public authorities. This research therefore seeks to highlight the regulatory vacuum that currently exists in this area.

Another objective of this study is to examine international regulatory approaches to artificial intelligence governance. Several jurisdictions have begun developing legal frameworks to address the risks associated with artificial intelligence technologies. By examining these international models, particularly the European Union's proposed Artificial Intelligence Act, this research aims to identify best practices that may inform the development of AI regulation in India.

Finally, this research seeks to propose policy recommendations and legal reforms that can ensure responsible use of artificial intelligence technologies in law enforcement. The goal is to develop a regulatory framework that balances the benefits of technological innovation with the protection of fundamental rights and democratic values.

Chapter 4: Research Methodology

This research adopts a doctrinal legal research methodology, which involves the systematic analysis of legal texts, statutes, judicial decisions, and scholarly commentary. Doctrinal research is widely used in legal scholarship because it focuses on examining existing legal principles and evaluating how these principles apply to emerging issues.

The primary sources used in this research include constitutional provisions, statutory legislation, and judicial precedents. The Constitution of India serves as the foundation for the legal analysis in this study, particularly Articles 14 and 21 which guarantee equality before the law and the right to life and personal liberty. These constitutional provisions play a central role in determining the legality of surveillance technologies deployed by the state.

Statutory legislation such as the Information Technology Act, 2000, the Consumer Protection Act, 2019, and the Digital Personal Data Protection Act, 2023 are also examined in order to understand the extent to which existing laws regulate artificial intelligence technologies. These statutes provide the legal framework governing digital technologies, data protection, and consumer rights in India.

Judicial precedents delivered by the Supreme Court of India are another important source for this research. Decisions such as Justice K.S. Puttaswamy (Retd.) v. Union of India and Anuradha Bhasin v. Union of India provide important guidance regarding privacy rights and the constitutional limits of state surveillance.

In addition to primary legal sources, this research also relies on secondary sources such as academic articles, policy reports, and international regulatory frameworks. Scholarly literature provides insights into the ethical and legal implications of artificial intelligence technologies and highlights the need for regulatory safeguards.

A comparative legal approach is also employed in this research. By examining regulatory frameworks developed in other jurisdictions, particularly the European Union and the United States, the study identifies potential models that could inform the development of AI regulation in India.

Chapter 5: Existing Legal Framework in India

5.1 Information Technology Act, 2000

The Information Technology Act, 2000 represents India's primary legislation governing electronic communications and cybercrime. The Act was enacted to provide legal recognition to electronic transactions and to address issues relating to cyber offences. It contains provisions addressing unauthorized access to computer systems, data breaches, identity theft, and hacking.

One of the relevant provisions within the Act is Section 43A, which imposes liability on corporate entities that fail to implement reasonable security practices while handling sensitive personal data. This provision seeks to ensure that organizations adopt adequate safeguards when processing personal information.

However, the Information Technology Act was enacted at a time when modern artificial intelligence technologies had not yet emerged. As a result, the Act does not address issues such as algorithmic decision-making, automated surveillance systems, or facial recognition technologies. The absence of specific provisions regulating these technologies highlights the limitations of the existing legal framework.

5.2 Consumer Protection Act, 2019

The Consumer Protection Act, 2019 introduced important reforms aimed at strengthening consumer rights in India. One of the key features of the Act is the introduction of product liability provisions, which allow consumers to seek compensation for harm caused by defective products or services.

Artificial intelligence-based products may potentially fall within the scope of product liability provisions if they cause harm to individuals. For example, if an AI-driven system produces an incorrect identification that results in harm, it may theoretically give rise to liability claims.

However, the Consumer Protection Act does not address the broader governance challenges associated with artificial intelligence technologies. Issues such as algorithmic transparency, accountability for automated decisions, and regulation of biometric surveillance remain outside the scope of this legislation.

5.3 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 represents India's most recent effort to regulate the processing of personal data. The legislation introduces several important principles including consent-based data

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

processing, data minimization, and accountability obligations for data fiduciaries.

The Act establishes rights for individuals regarding the processing of their personal data and imposes obligations on organizations that collect and process such data. These provisions represent an important step toward strengthening privacy protections in India.

However, the legislation does not specifically regulate the use of artificial intelligence technologies by government authorities. In particular, the Act does not address the deployment of facial recognition systems by law enforcement agencies.

Consequently, the use of AI-driven surveillance technologies often occurs through administrative decisions rather than explicit legislative authorization. This regulatory gap raises concerns regarding transparency, accountability, and democratic oversight.

Chapter 6: Constitutional Implications – Articles 14 and 21

6.1 Article 14: Equality Before the Law

Article 14 of the Constitution of India guarantees equality before the law and equal protection of the laws. The Supreme Court has consistently interpreted this provision as prohibiting arbitrary state action. When artificial intelligence systems are used in law enforcement, there is a risk that algorithmic biases may produce discriminatory outcomes. If facial recognition technologies disproportionately misidentify individuals belonging to certain demographic groups, their deployment may violate the constitutional guarantee of equality.

The use of biased algorithms in law enforcement may therefore raise serious constitutional concerns. Ensuring fairness in algorithmic decision-making is essential to protecting the principle of equality before the law.

6.2 Article 21: Right to Privacy and Personal Liberty

Article 21 guarantees the right to life and personal liberty. Over time, the Supreme Court has interpreted this provision broadly to include several derived rights including privacy, dignity, and autonomy.

In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court recognized privacy as a fundamental right protected under Article 21. The Court held that privacy is intrinsic to human dignity and personal liberty.

The judgment established a three-part test for evaluating state actions that restrict privacy rights:

1. The restriction must have a legal basis.
2. The restriction must pursue a legitimate state objective.
3. The restriction must satisfy the principle of proportionality.

Facial recognition technologies involve the collection and analysis of biometric data, which constitutes highly sensitive personal information. The deployment of such technologies without adequate legal safeguards may therefore violate constitutional protections relating to privacy and personal liberty.

Chapter 7: Comparative International Approaches

Several jurisdictions around the world have begun developing regulatory frameworks to address the risks associated with artificial intelligence technologies. As AI systems become increasingly integrated into public governance, economic activities, and law enforcement operations, governments have recognized the need to establish legal mechanisms capable of managing the potential harms associated with these technologies. Issues such as algorithmic bias, lack of transparency, privacy violations, and misuse of surveillance technologies have prompted policymakers to consider specialized regulatory approaches tailored to

artificial intelligence systems.

Among global regulatory efforts, the European Union has taken one of the most comprehensive and proactive approaches to AI governance through the development of the proposed Artificial Intelligence Act. The EU framework adopts a risk-based approach to regulation, which classifies artificial intelligence systems according to the level of risk they pose to individuals, society, and fundamental rights. This approach recognizes that not all AI systems pose the same level of danger, and therefore different regulatory standards are applied depending on the potential harm associated with specific applications.

Under the EU's regulatory framework, artificial intelligence systems are divided into several categories, including minimal-risk, limited-risk, high-risk, and unacceptable-risk systems.

Systems that are considered to pose unacceptable risks, such as certain forms of social scoring and manipulative AI technologies, may be prohibited entirely. High-risk AI systems, including biometric identification technologies used in law enforcement and border control, are subject to strict regulatory requirements. These requirements include mandatory risk assessments, transparency obligations, human oversight mechanisms, and compliance with strict data governance standards.

The European Union's approach also emphasizes accountability and transparency in algorithmic decision-making. Developers and deployers of high-risk AI systems are required to provide clear documentation regarding how their systems operate, including the datasets used to train them and the potential risks associated with their deployment. These measures are designed to ensure that artificial intelligence technologies operate in a manner consistent with fundamental rights, including privacy, non-discrimination, and human dignity.

In contrast, the regulatory approach adopted in the United States has been more fragmented and decentralized. Rather than implementing a comprehensive national regulatory framework, regulation of artificial intelligence technologies in the United States has often occurred at the state and municipal levels. Several cities have introduced restrictions or outright bans on the use of facial recognition technologies by law enforcement agencies due to concerns regarding privacy and racial bias.

For instance, cities such as San Francisco, Boston, and Portland have implemented regulations that limit the use of facial recognition technologies by government authorities. These measures reflect growing public concern that facial recognition systems may enable intrusive forms of surveillance and disproportionately affect minority communities. Studies conducted in the United States have indicated that certain facial recognition systems demonstrate higher error rates when identifying individuals belonging to racial minorities, which raises concerns regarding discriminatory policing practices.

The differing regulatory approaches adopted by the European Union and the United States highlight the broader global debate regarding how artificial intelligence technologies should be governed. While some jurisdictions favor comprehensive legislative frameworks, others rely on sector-specific regulations and local restrictions to address the risks associated with AI systems.

These international developments demonstrate a growing recognition among policymakers that artificial intelligence technologies require specialized regulatory oversight. Traditional legal frameworks governing data protection, consumer rights, and telecommunications may not be sufficient to address the unique challenges posed by AI-driven systems. As artificial intelligence technologies continue to evolve, governments will increasingly need to develop regulatory frameworks that balance technological innovation with the protection of fundamental rights and democratic values.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

For countries such as India, these international experiences provide valuable insights into the development of effective AI governance frameworks. By studying these global regulatory models, policymakers can identify best practices and adapt them to the specific legal, social, and institutional context of the country.

Chapter 8: Challenges in Regulating Artificial Intelligence in India

Regulating artificial intelligence technologies presents several significant challenges for policymakers. As artificial intelligence continues to evolve and become increasingly integrated into governance, law enforcement, and commercial sectors, legislators face difficulties in developing regulatory frameworks that are both effective and adaptable. The rapid advancement of AI technologies, combined with their technical complexity and societal implications, makes regulation particularly challenging.

One of the primary challenges is the rapid pace of technological innovation. Artificial intelligence technologies are developing at an unprecedented rate, often advancing faster than legislative processes can respond. Governments typically require considerable time to draft, debate, and enact legislation. By the time regulatory frameworks are implemented, the technology they were designed to regulate may already have evolved significantly. This creates a persistent gap between technological development and legal oversight. In the context of AI, innovations such as machine learning models, autonomous systems, and biometric identification technologies are constantly improving, making it difficult for lawmakers to create regulations that remain relevant over time. As a result, policymakers must design flexible regulatory frameworks capable of adapting to evolving technologies.

Another major challenge arises from the technical complexity of artificial intelligence systems. Many AI models operate through advanced machine learning techniques that analyze vast datasets and generate predictions or decisions through intricate computational processes. These processes are often difficult for non-technical regulators to understand. Many algorithms function as opaque "black box" systems, meaning that even developers may not fully understand how specific outputs are produced. This lack of transparency creates significant difficulties for regulators attempting to assess whether AI systems are fair, accurate, or free from bias. Without sufficient technical expertise, regulatory bodies may struggle to monitor AI systems effectively or identify potential risks associated with their deployment.

Furthermore, policymakers must address the challenge of algorithmic bias and discrimination. Artificial intelligence systems rely on training data to learn patterns and make predictions. If the datasets used to train these systems contain historical biases or incomplete information, the resulting algorithms may produce discriminatory outcomes. In the context of law enforcement, biased AI systems could disproportionately target certain communities, leading to unjust surveillance or wrongful identification. Preventing such outcomes requires careful oversight of the data used to train AI systems as well as continuous monitoring of their performance.

Another key difficulty in regulating artificial intelligence involves balancing technological innovation with the protection of fundamental rights. Governments often promote AI development as a driver of economic growth, innovation, and global competitiveness. Overly restrictive regulations may discourage investment in emerging technologies and slow technological progress. On the other hand, insufficient regulation may expose individuals to serious risks, including mass surveillance, privacy violations, and discrimination.

Achieving the appropriate balance between

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

innovation and rights protection is therefore a complex task. Policymakers must ensure that regulatory frameworks encourage technological development while simultaneously safeguarding constitutional principles such as privacy, equality, and accountability. This requires a nuanced approach that combines legal safeguards, technical standards, and institutional oversight mechanisms.

In conclusion, the regulation of artificial intelligence technologies involves navigating multiple challenges, including rapid technological advancement, technical complexity, potential bias, and competing policy priorities. Addressing these challenges requires proactive policymaking, interdisciplinary collaboration, and continuous evaluation of regulatory frameworks to ensure that AI technologies develop in a manner consistent with democratic values and fundamental rights.

Chapter 9: Recommendations for Legal Reform

The growing integration of artificial intelligence technologies in law enforcement presents both opportunities and risks. While AI systems such as facial recognition technologies may enhance investigative efficiency and improve public security, their deployment also raises significant legal and constitutional concerns. India's current legal framework remains inadequate to address these challenges, as existing statutes governing digital technologies were enacted before the widespread adoption of advanced artificial intelligence systems. Consequently, there is an urgent need for comprehensive legal reforms that ensure responsible use of AI technologies while safeguarding fundamental rights.

9.1 Enactment of Dedicated Artificial Intelligence Legislation

One of the most significant reforms required in India is the enactment of a comprehensive legislative framework specifically governing artificial intelligence technologies. At present, the regulation of AI is fragmented across multiple statutes, including the Information Technology Act, the Consumer Protection Act, and the Digital Personal Data Protection Act. Although these laws address certain aspects of digital governance and data protection, they do not directly regulate algorithmic decision-making systems or biometric surveillance technologies used in law enforcement.

Dedicated AI legislation would provide a coherent legal framework governing the development, deployment, and accountability of artificial intelligence systems. Such legislation should establish guiding principles for responsible AI governance, including transparency, accountability, fairness, and respect for human rights. It should also define key concepts such as automated decision-making systems, biometric identification technologies, and algorithmic risk assessments.

Furthermore, the legislation should adopt a risk-based regulatory approach, similar to frameworks being developed in the European Union. Under this approach, artificial intelligence systems would be categorized according to the level of risk they pose to individuals and society. High-risk systems, such as facial recognition technologies used by law enforcement agencies, should be subject to stricter regulatory oversight, including mandatory risk assessments and clear limitations on their use.

9.2 Ensuring Transparency and Explainability in Algorithmic Systems

Transparency is a crucial principle in the regulation of artificial intelligence technologies. Many AI systems operate as complex machine-learning models that are difficult to interpret, often functioning as so-called "black box" systems. This lack of transparency creates serious challenges for accountability, as it may be difficult to determine how a particular algorithmic decision was produced. To address this issue, regulatory frameworks should require that artificial intelligence systems used in law enforcement be designed in a manner that

allows for explainability and scrutiny. Authorities deploying such systems should disclose information regarding how the systems operate, including the datasets used for training, accuracy rates, and potential risks associated with their use.

Additionally, independent audits of algorithmic systems should be conducted to identify potential biases or discriminatory outcomes. Regular evaluations would ensure that AI technologies used in public administration remain consistent with constitutional principles of fairness and equality. Human oversight should also be maintained in decision-making processes to ensure that automated systems do not replace human judgment entirely.

9.3 Establishment of Independent Regulatory Authorities

Another important reform involves the establishment of independent regulatory institutions responsible for overseeing artificial intelligence technologies. Effective regulation requires specialized expertise and institutional capacity to monitor complex technological systems.

India currently lacks a dedicated authority responsible for regulating artificial intelligence governance. The creation of an independent Artificial Intelligence Regulatory Authority would help address this gap. Such an authority could develop regulatory guidelines, monitor compliance with AI laws, and investigate potential misuse of artificial intelligence technologies.

The regulatory authority could also maintain a registry of high-risk AI systems deployed by government agencies and private organizations. Entities deploying such technologies would be required to provide information regarding their design, functionality, and intended use.

Independent oversight would help ensure that artificial intelligence systems are deployed responsibly and in accordance with legal safeguards.

9.4 Strengthening Data Protection and Biometric Safeguards

Facial recognition technologies rely heavily on biometric data, which constitutes highly sensitive personal information. The collection and processing of biometric identifiers raise significant privacy concerns because such data is unique to each individual and cannot easily be changed if compromised.

Although the Digital Personal Data Protection Act, 2023 provides a general framework for regulating personal data processing, it does not specifically address the use of biometric surveillance technologies by law enforcement agencies. Stronger legal safeguards are therefore necessary.

India should establish strict rules governing the collection, storage, and use of biometric data. Such rules should ensure that biometric information is collected only for legitimate purposes and that its use is proportionate to the objective being pursued. Clear limitations should also be imposed on the retention and sharing of biometric data to prevent misuse.

9.5 Promoting Public Awareness and Digital Literacy

Legal reforms must be accompanied by increased public awareness regarding the implications of artificial intelligence technologies. Many individuals remain unaware of how AI systems operate and how these technologies may affect their privacy and civil liberties.

Governments should therefore promote digital literacy initiatives aimed at educating citizens about emerging technologies and their legal implications. Educational institutions, civil society organizations, and research bodies can play an important role in fostering public discussion about artificial intelligence governance.

Greater public awareness would empower individuals to exercise their rights and hold authorities accountable for the use of AI technologies.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Chapter 10: Conclusion

Artificial intelligence technologies are rapidly transforming governance and law enforcement practices across the world. While these technologies offer significant benefits in improving efficiency and enhancing security capabilities, they also raise profound legal and constitutional concerns.

Facial recognition systems, in particular, present serious risks relating to privacy, discrimination, and mass surveillance. Without appropriate safeguards, the deployment of such technologies may undermine fundamental rights guaranteed by the Constitution of India.

India's current legal framework remains inadequate to address these challenges. Existing laws governing digital technologies were enacted before the emergence of modern artificial intelligence systems and therefore fail to regulate algorithmic decision-making effectively.

To ensure that technological advancement does not come at the expense of constitutional freedoms, India must urgently develop a comprehensive regulatory framework governing artificial intelligence. Such a framework must strike a careful balance between promoting innovation and protecting the fundamental rights of individuals.