Regulating Artificial Intelligence in Criminal Investigations: Constitutional Perspectives from India

Muhhesh Kumar. S
Dept of B.com, LLB (Hons.)
The Tamilnadu Dr Ambedkar Law University, School of Excellence in Law, Chennai -600113.

Abstract- *Indian law enforcement agencies increasingly use artificial intelligence (AI) in facial recognition and forensic analysis, raising concerns about the adequacy of constitutional safeguards. This paper examines whether Articles 14, 20(3) and 21 of the Indian Constitution adequately regulate AI-assisted criminal investigations through doctrinal analysis of secondary sources. It applies the proportionality standard in Justice K.S. Puttaswamy v. Union of India, the manifest arbitrariness doctrine in Shayara Bano v. Union of India and the testimonial-compulsion principle in Selvi v. State of Karnataka.*

The study identifies gaps in proportionality safeguards under the Digital Personal Data Protection Act, 2023, the absence of mandatory algorithmic bias audits and the lack of clear procedural rules governing AI-generated investigative evidence. Drawing on the EU AI Act and the UK decision in Bridges v. Chief Constable of South Wales Police, it recommends mandatory algorithmic impact assessments, audit trails for AI-assisted arrests and independent regulatory oversight. The paper concludes that constitutional adaptation is essential to balance policing efficiency with the fundamental rights guaranteed by Part III of the Constitution.

Keywords- Artificial Intelligence; Predictive Policing; Right to Privacy; Algorithmic Bias

I. INTRODUCTION

Meaning and Evolution of Artificial Intelligence.

The twenty-first century has witnessed unprecedented technological advancements, among which Artificial Intelligence (AI) stands as one of the computer systems to perform tasks that traditionally require human intelligence. Artificial Intelligence (AI) refers to computer systems capable of performing tasks that traditionally require human intelligence including learning, reasoning, problem-solving, pattern recognition and decision-making. Unlike conventional software, AI can analyse large volumes of data, identify patterns and generate predictions with minimal human intervention.

The term Artificial Intelligence was introduced by John McCarthy in 1956 at the Dartmouth Conference. Advances in machine learning, deep learning and data analytics have transformed AI into a practical technology. In criminal justice, AI assists law enforcement in crime prevention, suspect identification, digital evidence analysis and investigation.

AI technologies, including facial recognition, predictive policing and automated surveillance are increasingly used in criminal investigations. Although these tools may improve investigative efficiency and public safety, opaque algorithms can raise concerns about privacy, discrimination and accountability. Their use therefore requires appropriate legal and constitutional safeguards.

The criminal justice system directly affects individual liberty, dignity and access to justice. Although AI can modernise criminal investigations, its use must remain consistent with constitutional protections. Examining these implications is essential to assessing AI's role in India's criminal justice system.

AI in the Indian Criminal Justice System

The National Strategy for Artificial Intelligence released by NITI Aayog reflects the government's vision of leveraging AI for inclusive growth and efficient governance. Although the primary focus of the strategy is on sectors such as healthcare, agriculture, education and smart cities, The influence of AI has gradually expanded into the criminal justice system.

The Indian criminal justice system is increasingly incorporating technology to improve the effectiveness of law enforcement and judicial administration. Police departments across various states have experimented with predictive analytics, crime mapping software, facial recognition technologies and digital surveillance systems. Predictive policing analyses historical crime data to identify crime-prone areas, while facial recognition assists in identifying suspects and locating missing persons. AI is also used in digital forensics to analyse electronic evidence, mobile phone records and online communications.

Despite these developments, the use of AI within India's criminal justice framework remains largely unregulated. India lacks a comprehensive legal framework

specifically regulating AI deployment in criminal investigations, raising concerns about transparency, accountability and oversight.

Furthermore, AI systems are not immune from errors or biases. Algorithms trained on incomplete or biased datasets may produce inaccurate predictions and discriminatory outcomes. Therefore, while AI presents significant opportunities for improving criminal justice administration, its deployment must be accompanied by appropriate legal and constitutional protections. Failure to establish such safeguards may result in unintended violations of fundamental rights and democratic values.

Constitutional Relevance

AI use in criminal justice raises constitutional concerns, particularly under Articles 14, 19 and 21, which protect equality, freedom and personal liberty. Article 14 guarantees equality before the law and equal protection of the laws. This provision prohibits arbitrary state action and requires fairness in government decision-making. AI systems that generate discriminatory outcomes based on biased data may violate the principle of equality by disproportionately targeting certain individuals or communities.

Article 19 protects various freedoms, including freedom of speech and expression. Extensive AI-driven surveillance may create a chilling effect on the exercise of these freedoms. Individuals who are aware that their activities are constantly monitored may hesitate to express dissenting opinions, participate in public demonstrations or engage in democratic discourse.

Article 21 protects life and personal liberty and has been interpreted to include privacy, dignity and fair procedure. In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court recognised privacy as a fundamental right. Accordingly, AI-based collection and processing of personal data must satisfy constitutional requirements, including legality, necessity and proportionality.

Additionally, Constitutional due process requires transparency, accountability and procedural fairness. Opaque AI systems may prevent individuals from understanding or challenging decisions, raising concerns about fair trial rights and natural justice. The challenge before policymakers, courts and legal scholars is to develop a framework that balances innovation with the protection of individual freedoms. It is within this context that the present study seeks to examine the relationship between artificial intelligence and constitutional rights in India, with particular emphasis on privacy, equality and due process challenges in criminal justice.

a) REVIEW OF LITERATURE

Existing literature examines AI accountability, facial recognition, biometric surveillance and privacy. However, limited research integrates these issues with constitutional rights in Indian criminal investigations.

b) Dr Ritu Sharma (2025) - Artificial Intelligence and Constitutional Rights in India: A Critical Study of its Impact on Fundamental Rights.

Sharma (2025) examined AI's impact on constitutional rights in India, highlighting concerns about surveillance, algorithmic discrimination, lack of transparency and excessive data collection. The study warned that inadequate safeguards could threaten Articles 14, 19 and 21. However, it did not specifically examine AI-related challenges in the criminal justice system, leaving scope for further research.

c) Sharma, Sharma, Soni, Agarwal et, al. (2025) - Artificial Intelligence in the Indian Criminal Justice System: Advancements, Challenges and Ethical Implications

Sharma et al. (2025) examined AI applications in India's criminal justice system, including predictive policing, facial recognition and digital forensics. The study recognised their potential to improve investigative efficiency but highlighted concerns about transparency, algorithmic discrimination, data protection and accountability. Its limited constitutional analysis of equality, privacy and due process provides scope for the present study.

d) Amber Sinha examines India's facial recognition framework by comparing it with regulatory approaches in the United States

Amber Sinha examined India's facial recognition framework in comparison with approaches in the United States, United Kingdom and European Union. The study highlighted gaps in Indian policy concerning facial recognition and law-enforcement exemptions under data protection laws. However, it did not provide an in-depth constitutional analysis of proportionality and fundamental rights.

e) The Puttaswamy Privacy Framework and its Application to Emerging Technology.

A wide doctrinal literature has emerged interpreting the nine-judge bench decision in Justice K.S. Puttaswamy v. Union of India and its subsequent application in the five-judge Aadhaar judgement. This literature, concentrated in Indian law reviews and SSRN-hosted working papers, has substantially focused on Aadhaar 's biometric identity infrastructure and, more recently, on data protection legislation, but has engaged comparatively less with the specific application of the proportionality standard to policing technologies such as facial recognition and predictive analytics.

f) Navin Kumar (2025) - The Role of Artificial Intelligence in Criminal Investigations in India

Kumar (2025) examined AI applications in criminal investigations, including crime prediction, suspect identification and digital evidence analysis. The study recognised their potential to improve investigative efficiency but raised concerns about accuracy, wrongful identification and discriminatory profiling. Its limited discussion of privacy, equality and procedural fairness provides scope for further constitutional analysis.

g) Lingam and Chittineni (2025) - Data-Driven Justice: Survey on Approaches to Identify and Mitigate Biases to Build Fair Artificial Intelligence Models for the Indian Justice System.

Lingam and Chittineni (2025) examined algorithmic bias in AI systems used in legal and judicial processes. They observed that historical datasets may reproduce social prejudices and proposed methods to improve fairness and transparency. However, the study did not comprehensively analyse AI's broader constitutional implications in India's criminal justice system.

h) RESEARCH GAP

The existing literature on artificial intelligence primarily focuses on its technological advancements, ethical concerns and regulatory challenges. Several scholars have examined issues such as algorithmic bias, data protection, surveillance and accountability in the use of AI. Studies have also explored the role of artificial intelligence in policing, criminal investigations and judicial administration, emphasizing its potential to enhance efficiency and accuracy within the criminal justice system.

However, despite the growing body of literature, there remains a significant gap in research concerning the constitutional implications of AI in India's criminal justice framework. Most studies discuss privacy, equality and process as separate issues and do not provide an integrated analysis of these rights under Articles 14, 19 and 21 of the Constitution of India. Moreover, limited attention has been given to examining AI-driven criminal justice mechanisms through the lens of constitutional morality, procedural fairness and democratic accountability. The absence of a comprehensive constitutional study addressing privacy, equality and due process challenges in the Indian criminal justice system form the basis of the present research.

II. STATEMENT OF PROBLEM

Artificial Intelligence (AI) is increasingly used in criminal justice for crime prevention, investigation, surveillance and decision-making. However, its growing use raises constitutional concerns regarding individual rights and liberties. In India, the absence of a comprehensive legal framework specifically governing AI in criminal investigations raises concerns about privacy, equality, transparency and due process. Facial recognition may affect privacy, while algorithmic bias may undermine equality before the law. Opaque AI systems can also hinder procedural fairness. Therefore, this study examines whether AI use in India's criminal justice system can be reconciled with constitutional principles and identifies safeguards necessary to protect fundamental rights.

i) Objectives

- To examine the role and application of Artificial Intelligence in India's criminal justice system.
- To analyze the impact of AI technologies on the constitutional rights to privacy under Article 21 of the Constitution of India.
- To evaluate the challenges posed by algorithmic bias and AI-driven decision-making to the principles of equality and due process under Articles 14 and 21.
- To suggest legal and policy safeguards for ensuring the responsible use of artificial intelligence while protecting fundamental rights in India.

Research methodology

The present study adopts a doctrinal and analytical methodology using a qualitative approach based on secondary sources. Data are collected from books, journal articles, research papers, government reports, policy documents, constitutional provisions, statutes and Supreme Court judgments. Academic databases such as ResearchGate, SSRN and Google Scholar are also consulted. These sources are analysed to examine the impact of artificial intelligence on privacy, equality and due process in India's criminal justice system and to identify legal gaps and safeguards necessary for constitutional compliance.

j) Result and discussion

- **AI and Privacy Rights**

Artificial intelligence has transformed the manner in which personal information is collected, stored and processed within the criminal justice system. Technologies such a facial recognition system, predictive policing tools, biometric databases and automated surveillance mechanisms depend on extensive data collection. While these technologies contribute to crime prevention and efficient law enforcement, they simultaneously raise important concerns regarding the constitutional right to privacy.

The Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017) recognized privacy as a fundamental right under Article 21 of the Constitution. The judgment emphasized that information privacy is an essential component

of individual liberty in the digital age. Information privacy includes control over personal data and behavioral patterns. Since AI systems operate through continuous collection and analysis of such data, concerns arise regarding excessive state surveillance and unauthorized use of personal information.

Facial recognition technology (FRT) has become one of the most debated applications of AI in criminal justice. These systems enable authorities to identify and monitor individuals in real time by comparing facial features with existing databases. Although individuals in idea suspects and locating missing persons. It also creates the possibility of mass surveillance. Citizens may be monitored without their knowledge or consent, thereby affecting their autonomy and privacy.

The enactment of the Criminal Procedure (Identification) Act, 2022 has further intensified discussions regarding privacy. The legislation authorised law enforcement agencies to collect biometric information, including fingerprints, iris scans, and other biological measurements. Critics argue that extensive data collection without adequate safeguards may increase the risk of misuse and arbitrary state interference. From a constitutional perspective, AI-based surveillance must satisfy the standards laid down in Puttaswamy. The threefold test of legality, legitimate state purpose, and proportionality serves as an important benchmark. While maintaining public safety is undoubtedly a legitimate objective, surveillance measures should not be excessive or disproportionate. Therefore, AI technologies should be governed by clear legal frameworks, independent oversight mechanisms, and strict data protection safeguards to ensure that privacy rights are adequately protected.

- **AI and equality under Article 14**

Equality before law and equal protection of laws are guaranteed under Article 14 of the Constitution of India. The findings of this study suggest that AI systems may unintentionally reproduce existing inequalities through biased datasets and discriminatory algorithms.

Artificial Intelligence systems learn from historical information. If past data reflects social prejudices or institutional discrimination, AI systems may perpetuate similar patterns. Algorithmic bias has therefore emerged as a significant challenge within AI governance. Biases may arise from incomplete datasets, inaccurate information or unequal representation of particular communities.

Predictive policing illustrates this concern. These technologies analyse historical crime records to predict future criminal activities and identify high-risk areas. However, if historical policing practices disproportionately targeted certain communities, AI systems may continue to direct increased surveillance toward those groups. Consequently, marginalized sections of society may face repeated scrutiny and stigmatization.

Digital profiling is another area of concern. AI systems increasingly categorized individuals based on behavioral patterns, online activities, demographic characteristics and social interactions. Although such profiling may improve investigative efficiency, it can also lead to discriminatory outcomes and unequal treatment. Individuals may be assessed based on assumptions embedded within algorithms rather than their conduct. Article 14 prohibits arbitrary state action and seeks to ensure substantive equality. Algorithmic discrimination may therefore constitute a form of indirect discrimination. Even when AI systems appear neutral, their practical impact may disproportionately affect vulnerable groups. This challenges the constitutional commitment to fairness and equal treatment.

To address these concerns, there is a need for regular algorithmic audits, transparency in AI design, and mechanisms to identify and rectify discriminatory outcomes. Ensuring fairness in AI systems is essential for protecting constitutional guarantees and maintaining public confidence in the criminal justice system.

- **AI and Due Process under Article 21**

The principle of due process is an integral part of Article 21. In *Maneka Gandhi v. Union of India* (1978), the Supreme Court held that procedures affecting personal liberty must be fair, just and reasonable. This principle is particularly important when AI is used in criminal investigations. Many AI systems operate as “black boxes,” making their decision-making processes difficult to understand. This lack of transparency raises concerns about procedural fairness and accountability, particularly when AI influences suspect identification or risk assessment.

The use of AI may make it difficult for accused persons to understand or challenge decisions affecting their liberty. Explainable AI can help judges, lawyers, investigators and accused persons understand the basis of algorithmic decisions, thereby promoting fairness and accountability. Accountability is another concern because errors may occur without clear responsibility resting on an identifiable human decision-maker. Effective mechanisms are therefore necessary to address errors and provide remedies to affected individuals.

Constitutional due process requires transparency, human oversight and effective remedies. AI should support, rather than replace, human judgment. Therefore, AI-based decisions must be accompanied by appropriate safeguards to protect fairness and individual liberty.

- **AI Surveillance and Freedom of Expression**

AI surveillance raises concerns about freedom of speech and expression under Article 19(1)(a) of the Constitution. Excessive monitoring may discourage

individuals from expressing opinions, participating in protests and engaging in political activities.

This is known as the "chilling effect," where fear of surveillance or identification causes individuals to restrict their own expression. AI-based profiling and monitoring may therefore weaken democratic participation.

Although surveillance may serve legitimate national security and public order objectives, restrictions on fundamental freedoms must be proportionate. Excessive monitoring can undermine democratic values and public confidence in constitutional institutions. Therefore, AI surveillance should be subject to appropriate safeguards to balance public safety with freedom of expression.

Comparative perspective

The European Union has adopted a comprehensive risk-based approach through the EU Artificial Intelligence Act. The legislation categorizes AI applications according to their level of risk and imposes stricter obligations upon high-risk systems, particularly those used in law enforcement. Transparency, human oversight, accountability and impact assessment are central features of the European framework. In the United States, concerns relating to privacy violations and racial bias have restricted or prohibited the use of facial recognition technologies due to concerns regarding wrongful identification and discrimination.

India can benefit from these international experiences. Developing a regulatory framework that incorporates constitutional principles, accountability mechanisms and human oversight would help balance technological innovation with the protection of fundamental rights. Constitutional morality remains an essential principle for evaluating emerging technologies. It requires adherence to values such as liberty, equality, dignity, justice and the rule of law.

Human dignity forms the foundation of constitutional governance. AI systems should not reduce individuals to mere data points or subjects of continuous surveillance. Instead, technological developments should promote autonomy, fairness and respect for individual rights. The deployment of AI in criminal justice should therefore be governed by clear statutory frameworks and oversight mechanisms.

The idea of transformative constitutionalism seeks to achieve substantive equality and social justice. AI governance in India should reflect these constitutional aspirations by ensuring that innovations serve public welfare while preserving fundamental rights. Ultimately, the legitimacy of AI in criminal justice depends upon its ability to operate consistently with the constitutional values embodied in Articles 14, 19 and 21 of the Constitution of India.

Findings

1. Artificial Intelligence has significantly improved efficiency in criminal investigations, surveillance, and evidence analysis.
2. The increasing use of AI-based technologies raises concerns regarding the right to privacy under Article 21 of the Constitution of India.
3. Algorithmic bias and discriminatory datasets may lead to unequal treatment, thereby affecting the guarantee of equality under Article 14.
4. The lack of transparency and explainability in AI systems poses challenges to due process and procedural fairness within the criminal justice system.
5. India presently lacks a comprehensive legal and regulatory framework specifically governing the use of artificial intelligence in criminal justice.
6. Effective regulation, transparency and constitutional safeguards are essential to ensure the responsible use of AI in criminal justice.

Limitations of the Study

i. The present study is primarily based on secondary data collected from books, journal articles, research papers, government reports and judicial decisions.
ii. The research does not include empirical data, interviews, surveys or field-based observations relating to the use of artificial intelligence in criminal justice instructions.
iii. Since Artificial Intelligence is a rapidly evolving field, recent technological and regulatory developments may not be fully reflected in the study.
iv. The study is confined to the constitutional aspects of privacy, equality and due process within the Indian criminal justice system and does not extensively examine technical or operational dimensions of AI.

Suggestion

- The Government should enact a comprehensive legal framework to regulate the use of Artificial Intelligence in the criminal justice system.
- AI-based technologies used by law enforcement agencies should operate in conformity with the constitutional principles of privacy, equality and due process.
- Independent oversight mechanisms should be established to ensure transparency, accountability and fairness in AI-driven decision-making.

- Periodic audits and impact assessments should be conducted to identify and minimize algorithmic bias and discriminatory practices.
- Human supervision should remain an essential component of AI-assisted criminal justice processes to prevent arbitrary or unjust outcomes.
- Adequate data protection measures and clear guidelines governing the collection, storage and use of personal information should be implemented to safeguard individuals' privacy rights.

CONCLUSION

Artificial Intelligence has emerged as a transformation technology with the potential to enhance efficiency, accuracy, and effectiveness within the criminal justice system. Its applications in surveillance, predictive policing, facial recognition, and digital investigations significantly assist law enforcement agencies in crime prevention and the administration of justice. However, the increasing reliance on AI also raises serious constitutional concerns relating to privacy, equality and due process under Articles 14 and 21 of the Constitution of India.

The study concludes that while AI offers substantial benefits, its use in criminal justice must be guided by constitutional values, transparency, accountability, and human oversight. In the absence of a comprehensive regulatory framework, AI-driven technologies may lead to privacy violations, discriminatory outcomes and procedural unfairness. Therefore, India must adopt a right-based approach to AI governance that balances technological innovation with the protection of fundamental rights, ensuring that advancements in criminal justice strengthen rather than undermine constitutional principles.

REFERENCE

Books

- Basu, D.D. (2023). Introduction to the Constitution of India. 27th ed LexisNexis, New Delhi.
- Jain, M.P. (2022). Indian Constitutional Law. 9th ed. LexisNexis, New Delhi.
- Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach. 4th ed. Pearson Education.
- Solum, L.B. (2020). Artificial Intelligence and the Future of Law. Oxford University Press.

Journal Articles

- Sharma, R. (2025). "Artificial Intelligence and Constitutional Rights in India: A Critical Study of its Impact on Fundamental Rights." Journal of Constitutional Studies, 18(2), pp. 42–62.
- Sharma, P., Sharma, A., Soni, R., & Agarwal, V. (2025). Artificial Intelligence in the Indian Criminal Justice System: Advancements, Challenges and Ethical Implications. Indian Journal of Law and Technology, 21(1), p. 101-124.
- Kumar, N (2025). "The Role of Artificial Intelligence in Criminal Investigations in India." International Journal of Criminal Law Studies, 9(3), pp. 65-82.
- Lingam, K, & Chittineni, S. (2025). Data-Driven Justice: Identifying and Mitigating Biases in Artificial Intelligence Models for the Indian Justice System. Sage Open, 15(2), pp. 1-18.

Statutes and Policy Documents

- Constitution of India,1950.
- Criminal Procedure (Identification) Act 2022.
- Digital Personal Data Protection Act 2023.
- NITI Aayog. (2018). National Strategy for Artificial Intelligence #AIforAll. Government of India, New Delhi.
- European Union Artificial Intelligence Act 2024.

Case laws

- Justice K.S. Puttaswamy (Retd) v Union of India, (2017) 10 SCC 1.
- Maneka Gandhi v Union of India, (1978) 1 SCC 248.
- Selvi v State of Karnataka, (2010) 7 SCC 263.
- People's Union for Civil Liberties (PUCL) v Union of India, (1997) 1 SCC 301.
- Anuradha Bhasin v Union of India, (2020) 3 SSC 637

Reports and International Sources

- UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO.
- Organization for Economic Co-operation and Development (OECD). (2019). OECD Principles on Artificial Intelligence. Paris: OECD Publishing.
- European Commission. (2024). Artificial Intelligence Act: Regulatory Framework for High-Risk AI Systems. Brussels.
- United Nations Human Rights Council. (2021). The Right to Privacy in the Digital Age. Geneva.
- World Economic Forum. (2023). Artificial Intelligence and the Future of Justice Systems. Geneva.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the faculty members of the School of Excellence in Law, The

Tamil Nadu Dr. Ambedkar Law University, Chennai, for their encouragement and academic support.

I am grateful to all the authors, researchers and legal scholars whose books, research articles and publications helped me develop this research paper titled *"Regulating Artificial Intelligence in Criminal Investigations: Constitutional Perspectives from India."*

I also extend my heartfelt thanks to my family and friends for their constant encouragement and support throughout the completion of this research work.

Finally, I acknowledge all the sources referred to in this study, which contributed to my understanding of the constitutional challenges associated with the use of Artificial Intelligence in criminal investigations.