Original Article
ISSN(Online): 2584-0983
https://shikshasamvad.com/

Shiksha Samvad
International Open Access, Peer Reviewed & Refereed Journal
© Shiksha Samvad|Volume-04| Issue-01| September- 2026
DOI: - https://doi.org/10.64880/shikshasamvad.v4i1.19

Predictive Policing and Constitutional Rights in India: Regulating AI-Driven Criminal Investigation

Dr. T.V.Rajput
Independent Research, Gujarat, India
Email: rajputthana010@gmail.com

Abstract

The rising use of Artificial Intelligence (AI) in criminal investigations is expanding opportunities for law-enforcement agencies to analyse vast amounts of information, discover patterns, identify suspects, and prevent future crimes. Predictive policing involves employing data-based technologies, algorithms, surveillance, facial recognition, and other computerized tools to evaluate the likelihood of crime occurring or identifying individuals and places at risk. Although such methods may be beneficial for improving criminal investigations, their increased utilization in Indian law enforcement can trigger several constitutional issues. For example, relying on historical data may lead to discriminatory practices and unequal treatment of protected classes of individuals. Moreover, incorrect results, surveillance, lack of transparency, and reduced human involvement may challenge citizens' privacy, liberty, and freedom of choice.

This paper aims to examine the constitutional issues associated with the use of AI in criminal investigations and focus on India's legal framework. The article will discuss whether the use of such technology is consistent with the Indians' rights to equality and privacy and to what extent the current laws can protect civilians from potential misconduct by law enforcers. It will also consider whether transparency and accountability mechanisms are sufficient to ensure that algorithms' decisions are not discriminatory and can be contestable by civilians. One of the critical arguments in favor of regulating AI use in criminal investigations is that it must serve as an instrument for supporting investigations but not as a primary criminal suspect identifier. Therefore, the regulation of AI in investigations must feature accountability, transparency, data privacy, human oversight, bias elimination, and accessibility to provide a sufficient level of protection and legal security for civilians in any digital environment.

Constitutional issues associated with the usage of AI in criminal investigations can emerge when using such technology in India. Although it might be helpful for analyzing and predicting the probability of crimes, it should not be utilized for making arrests or exercising coercive power over suspected criminals.

Keywords: *Predictive Policing; Artificial Intelligence; Constitutional Rights; Criminal Investigation; Data Privacy*

1. Introduction

The rapid developments in technology have transformed the criminal investigations around the globe. The law-enforcement agencies are now relying more and more on digital means for gathering, analyzing and interpreting the data for detecting the criminals and serving justice. Predictive policing is the application of data analytics and digital technologies to evaluate the patterns related to criminal activity and estimate the likelihood of the occurrence of future crime based on particular sets of circumstances.[1] Considering the rising

population, rampant cybercrimes, increased digitization and insufficient police presence in India, it may seem essential to employ such technologies to supplement the existing legal procedures.[2] Yet, there emerge several pertinent questions regarding the infringement of liberties, accountability of the State, and the limitation of power.[3]

Technology-driven policing would offer strategic advantages to the investigating agencies as compared to the traditional methods.[4] The information related to the previous convictions, geographical locations, phone records, video surveillance, and other private data may be utilized to predict the probability of a particular group of people being prone to committing certain crimes.[5] Though such data collection and analysis may help the police in investigating serious crimes, it may cause unequal targeting of specific communities based on mere statistical probabilities.[6] The data that appears neutral might have hidden prejudices that may get reflected through algorithmized responses, thus, creating adverse consequences for the socially and economically vulnerable groups.[7] At times, the opacity of such techno-police systems may deny justice to the citizens by restricting access to relevant information, and challenging the decisions reached through automated means.[8]

At the same time, the techno-police initiatives may interact with the Indian Constitution in diverse ways. The fundamental rights enshrined in the Indian Constitution and the basic structure doctrine limit the sovereignty of the country in the matters of law-making.[9] The Articles 14, 19 and 21 of the Indian Constitution safeguard the rights of equality before the law, freedom of speech and expression, and the right to life and liberty respectively.[10] The rights to autonomy and privacy have been interpreted by the Indian judiciary as a fundamental part of the Constitution.[11] Therefore, the techno-police systems may not override the judiciary and legislative domains in India. The emergence of technology-driven surveillance mechanisms has made it essential for the State to ensure that the rights to equality, autonomy, freedom of expression, and privacy are protected.[11]

The present study aimed to explore the interface between predictive policing, constitutional rights and crime investigations in India. Several questions related to the principles of equality, freedom of speech, right to life, and the right to privacy were raised to assess the impact of techno-police on Indian democracy. The research provides strong arguments to suggest that predictive policing should be employed cautiously in India.[12] The techno-police may offer policy advantages to the law-enforcement agencies, but it should be regulated under the framework of the Indian Constitution.[11] A comprehensive techno-legal framework should be devised to ensure that techno-police measures adhere to the established legal procedures, and protect the vulnerable groups from being targeted.[6]

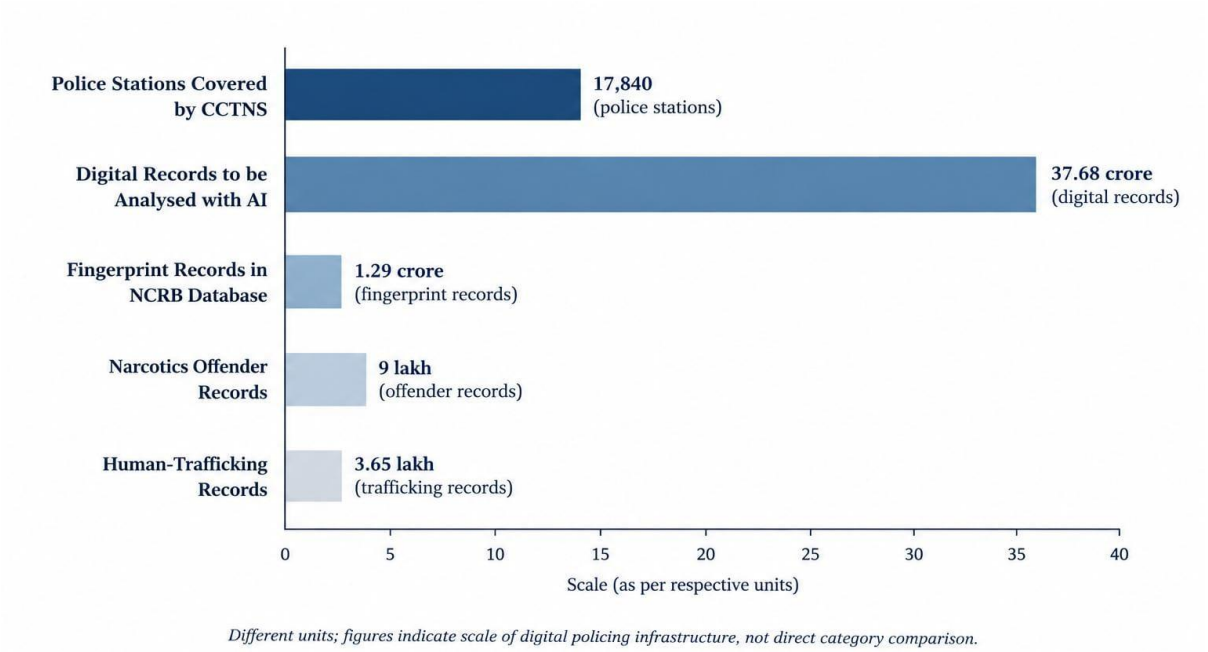

Figure 1: Scale of AI-Enabled Criminal Investigation Infrastructure in India

Source: Press Information Bureau, Government of India, 19 June 2026.

2. Research Purpose and Methodology

Research Purpose

- To evaluate the impact of predictive policing on the Indian constitution
- To highlight privacy, discrimination, and accountability problems in tech-driven investigations
- To assess the adequacy of current legal safeguards in India
- To offer recommendations on balancing factors for predictive policing.

Research Methodology

This research uses a doctrinal and qualitative research method. The study focuses on the Constitution, statutes, case laws, legal journals, policies, reports, and other relevant materials. The paper examines the issue of predictive policing and lays down the measures that can protect the rights of citizens in a democracy like India during technology-assisted crime investigations.

3. Literature Review

Recent studies on predictive policing in India bring to light various issues regarding the tensions between advancements in criminal investigations through technology and the protections of constitutional rights. Specifically, **Antara Vats (2022)** investigated predictive policing practices in India. Her research identified concerns regarding the dependability of data, the risks of errors, and the difficulties in contesting decisions made by these technologies. **Vats's (2022)** study concluded that the use of historical data in predictive policing could result in the replication of existing social inequalities and discrimination.

Meanwhile, **Kavidharani R. (2025)** undertook a constitutional morality perspective of predictive policing. In his work, he discussed the ethical implications of crime mapping, facial recognition technology, and surveillance in light of constitutional rights. He argued that the

effectiveness of these technologies should not come at the expense of equality, privacy, liberty, and dignity. Similarly, **Apoorva Roy, Neetu Neetu, and Ajay Raj Singh (2025)** explored predictive policing through a legal lens. The article identified the challenges of algorithmic bias, discrimination, privacy, fairness, and accountability in predictive policing. Overall, the study emphasized the need for human factors in policing criminal investigations to avert social injustices.

On the other hand, **Sahil and Dr. Shobhna Jeet (2025)** focused on predictive policing and India's data-protection laws. Their research highlighted concerns over personal-data profiling, surveillance, and State monitoring and the need for accountability. **Debalina Roy (2026)** identified tensions between the efficacy of predictive policing and the risks of using data profiling, including discriminatory data and the limitations of challenging such information. **Harinath Reddy G. and Manne Sainath (2026)**, in turn, investigated predictive policing in the context of India's criminal justice system. Their work stressed the need to consider constitutional morality, including factors such as accountability and human oversight.

4. Laws, Amendments and Judicial Decisions

4.1 Constitution of India, 1950

The Constitution of India, 1950 lays the foundational principles relating to the legality of predictive policing and technology-facilitated criminal investigation. **Article 14** provides for the equality before law and prohibits discrimination by the State, which becomes pertinent while utilising predictive systems with historical crime data that may reflect social or systemic biases. **Article 19** safeguards fundamental freedoms, which can be impacted by pervasive surveillance and monitoring. Significantly, **Article 21** safeguards the life and personal liberty and was interpreted to include the right to privacy and dignity. Therefore, the exercise of predictive policing must be consistent with the principles of fairness, reasonableness, necessity and proportionality.[11]

4.2 Information Technology Act, 2000

The Information Technology Act, 2000 along with amendments provides an important legal framework relating to electronic information and technology-related offences. Its provisions relating to electronic records, interception, surveillance and cybersecurity become relevant while addressing the collection and analysis of digital information by police authorities. However, the Act was enacted before the emergence of predictive policing and does not address algorithmic profiling, automated risk assessment and technological bias in detail. This creates a lacunae necessitating stricter legal safeguards in the context of policing decisions influenced by technology.[14]

4.3 Digital Personal Data Protection Act, 2023

The **Digital Personal Data Protection Act, 2023** is particularly pertinent as predictive policing involves the collection, storage and analysis of vast volumes of personal information. The Act offers a legal framework for processing digital personal data and becomes relevant while addressing aspects of lawful processing, data security, purpose of collecting information,

retention and accountability in the context of criminal investigation. Simultaneously, the treatment of State functions and exemptions requires careful contemplation so as to not unnecessarily impact privacy.[15]

4.4 Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam, 2023

The **Bharatiya Nyaya Sanhita, 2023 (BNS)** replaced the Indian Penal Code, 1860 while the **Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)** replaced the **Code of Criminal Procedure, 1973**. The **Bharatiya Sakshya Adhiniyam, 2023 (BSA)** replaced the Indian **Evidence Act, 1872.** These statutes provide a comprehensive legal overhaul of India's criminal justice system. The BNSS affords wider recognition of electronic methods while the BSA addresses electronic and digital evidence. Their relevance to predictive policing stems from their ability to ensure that technology-assisted investigation facilitates investigation without replacing the evidentiary, procedural and fairness-related requirements. A prediction by a computer system should not be used as evidence of crimes.[16]

4.5 Indian Telegraph Act, 1885

The Indian Telegraph Act, 1885 comprises provisions relating to interception of communication in permissible circumstances. Though it precedes modern digital technologies, its surveillance-related provisions have historically been pertinent to communications monitoring. Predictive policing may involve analysing communication-related information and thus lawful authority and procedural safeguards assume critical importance. Any augmentation of surveillance capabilities should be balanced vis-a-vis constitutional privacy safeguards.[17]

4.6 Aadhaar Act, 2016

The Aadhaar Act, 2016 regulates the use of Aadhaar information and biometric identity data. Its relevance emerges as contemporary investigations may employ identification and verification technologies. The use of biometric information for policing purposes must be regulated since biometric data is highly sensitive and its misuse or disclosure can have deleterious consequences for privacy and security.[18]

4.7 Right to Information Act, 2005 and Protection of Human Rights Act, 1993

The Right to Information Act, 2005 enhances transparency and accountability in public administration and is relevant in comprehending government policies and practices related to technology-based policing though statutory exemptions may limit access to information pertaining to investigations and national security. The Protection of Human Rights Act, 1993 provides a broader legal framework for addressing violations of human rights and affirms the principle that policing must uphold individual dignity and liberty.[19]

4.8 Justice K.S. Puttaswamy v. Union of India, 2017

The Supreme Court's verdict in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) is one of the most significant judgments for the application of technology and policing in India.

A nine-judge Bench declared privacy as a fundamental right under the Constitution. The Court drew a connection between privacy and dignity, autonomy, liberty and individual choice. The judgment is particularly pertinent to predictive policing as the collection and analysis of personal information entails serious privacy concerns. State action with respect to privacy must have a lawful basis and satisfy constitutional requirements.[11]

4.9 Anuradha Bhasin v. Union of India, 2020

The Supreme Court in Anuradha Bhasin v. Union of India (2020) examined restrictions on fundamental rights and stressed upon the requirement for legality and proportionality. The judgment reinforces the notion that restrictions imposed by the State cannot be excessive and lack sufficient legal justification. As applied to predictive policing, this judgment implies that surveillance, data collection or technological monitoring must have a legitimate aim and should not encroach upon individual rights to an unwarranted extent.[21]

Table1: NCRB data relevant to predictive policing

NCRB indicator	**Recent data**	**Relevance to your study**	**Source**
Total cognisable crimes	**6,237,582 cases (2023)**	Demonstrates the scale of criminal cases potentially requiring data-assisted investigation.	NCRB, *Crime in India 2023*
Cybercrime cases	**86,420 cases (2023)**	Supports the argument that increasing digital crime creates a need for technologically capable investigation.	NCRB, *Crime in India 2023*
Cybercrime growth	**Increase over previous years**	Demonstrates the growing importance of digital evidence and technology-assisted policing.	NCRB, *Crime in India 2023*
Latest NCRB edition	**Crime in India 2023**	Establishes that 2023 is the latest NCRB crime data	

Source: National Crime Records Bureau, *Crime in India 2023*; Ministry of Home Affairs, Government of India. The MHA states that **2023 is the latest published NCRB Crime in India report**.

5. Critical Analysis and Challenges

A predictive policing technology can be applied in a manner that supports police investigations by recognizing patterns, focusing resources, and responding to impending dangers. At the same time, the technology can create constitutional and practical problems in India because of possible algorithmic bias, privacy concerns, reduced transparency, false accusations, and a lack of remedies. The technology can reinforce discrimination if it is based on past experiences of the police. The tool can also learn totarget individuals on irrelevant characteristics such as race, ethnicity, or religion. Moreover, predictive policing software may require law enforcement officers to process and store private information about citizens, which

constitutes a privacy issue. Investigation software may also generate unproven accusations against civilians, who may not have adequate remedies against potential government violations of their privacy or rights. Overall, predictive policing can and should be used in India with proper oversight, standardization, transparency, proportionality, and remedies.

6. Finding and Discussion

The study concludes that predictive policing can help Indian law enforcement agencies to detect crime patterns, assign resources, and expedite investigations. Yet, it is of crucial importance to consider various factors, beginning with the accuracy and validity of information used for predictions, and ending with possible adverse effects on the rights and freedoms of Indians. Predictive policing requires a comprehensive legal framework to clarify the responsibilities of all sides participating in such operations, as well as to ensure the accessibility of redress for all persons that have been brought in any way into the sphere of predictive policing. Moreover, the study reveals that technology-driven predictions should not replace evidence, policing discretion, and judicial oversight. Therefore, technology-assisted policing solutions should be based on constitutional rights, including the right to equality and legal protection, the right to privacy, and the right to liberty and security of person. It is essential to ensure effective human oversight, proper collection and processing of data, and the observance of legal standards and accountability in order to optimize investigative procedures and achieve the best outcomes in terms of crime reduction and citizens' safety.

7. Conclusion and Suggestions

Conclusion

The implementation of predictive policing can improve the investigative practices in India by supporting the law-enforcement agencies to gain knowledge about the occurrence patterns of criminal behaviours, assess risks, and optimize their investigative capacities. However, as India's progressive technology should not undermine the rights protected by its constitution, the application of such strategies as predictive policing should not violate the privacy, equality, discrimination, transparency, and freedom issues.

Suggestions

- Legal framework for predictive policing in India should be created for data use, surveillance, accountability, and human rights.
- Technology should not be used to predict and then act on without human involvement.
- Lawful personal data collection and protection should be promoted and protected to prevent discrimination and the use of sensitive information.
- Transparency, accountability, and legal resources should be available to the public and required for those misusing the system.

References

1. Richard A Berk, 'Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement' (2021) 4 *Annual Review of Criminology* 209, 209–237.

2. Vivek Sreehari and others, 'Artificial Intelligence and Predictive Policing in the Indian Criminal Justice System: Methods, Applications and Constitutional Concerns' (2026) 3(7s) *Journal of Intelligent Decision Making and Information Science*.
3. T-W Hung and C-P Yen, 'Predictive Policing and Algorithmic Fairness' (2023) 201 *Synthese* 206.
4. Berk (n 1).
5. Berk (n 1); Sreehari and others (n 2).
6. Hung and Yen (n 3).
7. T-W Hung and C-P Yen, 'Predictive Policing and Algorithmic Fairness' (2023) 201 *Synthese* 206; A S Almasoud and J A Idowu, 'Algorithmic Fairness in Predictive Policing' (2025) 5 *AI and Ethics* 2323.
8. B Perego, 'Predictive Policing: Transparency of Algorithms, Impact on Privacy and Discriminatory Implications' (2020) 2020(2) *BioLaw Journal – Rivista di BioDiritto* 447.
9. *Kesavananda Bharati v State of Kerala* (1973) 4 SCC 225.
10. Constitution of India 1950, arts 14, 19 and 21.
11. *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
12. Berk (n 1); Hung and Yen (n 3); Sreehari and others (n 2).
13. Information Technology Act 2000, ss 43, 43A, 69 and 69B.
14. Berk RA, 'Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement' (2021) 4 *Annual Review of Criminology* 209.
15. Digital Personal Data Protection Act 2023, ss 4–13.
16. Bharatiya Sakshya Adhiniyam 2023, ss 3 and 61–63.
17. *People's Union for Civil Liberties (PUCL) v Union of India* (1997) 1 SCC 301; *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
18. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, ss 2(k), 28 and 29.
19. Right to Information Act 2005, ss 4 and 8.
20. Protection of Human Rights Act 1993, ss 2(d), 12 and 13.
21. *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.

Cite the Article:

Rajput, Dr. T.V.(2026). Predictive Policing and Constitutional Rights in India: Regulating AI-Driven Criminal Investigation. Shiksha Samvad International Open Access Peer-Reviewed & Refereed Journal of Multidisciplinary Research, 4(1) 173-180, ISSN: 2584-0983 (Online), Volume 04, Issue 01, September-2026., **DOI: -** https://doi.org/10.64880/shikshasamvad.v4i1.19