International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Predictive Policing Algorithms: The Promise and Peril of AI-Driven Crime Control

Debalina Roy

Rajiv Gandhi National University of Law, Punjab, India

Abstract: ***Predictive policing refers to the use of artificial intelligence (AI) and algorithmic models to forecast crime patterns and identify potential offenders or victims. It has emerged as a cutting-edge tool for proactive law enforcement worldwide. This approach shifts policing from a reactive response to crimes towards a proactive strategy aimed at preventing crime. By analysing historical crime patterns, predictive systems identify high-risk areas and individuals, helping police allocate resources more efficiently. In India, initiatives such as MARVEL in Maharashtra and CMAPS in Telangana exemplify this move towards data-driven policing. While these technologies hold promise for improving crime prevention and resource management, they also raise serious constitutional and ethical concerns. The key challenges stem from the reliance on historical crime data, which often contains biases that disproportionately affect marginalised communities. Such systems risk perpetuating and amplifying discrimination under the guise of scientific objectivity. Furthermore, the lack of transparency in how these predictive tools operate limits accountability and the ability of individuals to contest decisions that impact their rights. In the Indian context, these concerns highlight a pressing need to reconcile the benefits of predictive policing with constitutional protections of equality, due process, and privacy, ensuring these tools are implemented with appropriate safeguards, oversight, and fairness.***

Keywords: predictive policing, artificial intelligence, algorithmic policing, crime forecasting, due process, equality before law

1. Introduction

Predictive policing represents one of the most significant incursions of artificial intelligence (AI) into law enforcement practices, promising a shift from reactive to proactive crime control. At its core, predictive policing uses algorithmic models to forecast where crimes are likely to occur, who may commit them, or who is most at risk of victimisation. These systems draw on historical crime data and statistical correlations to identify so-called "hotspots" or "high-risk individuals." Proponents argue that such tools can enhance the efficiency of resource allocation, reduce crime rates, and assist in evidence-based decision-making within criminal justice institutions. In the United States, software such as PredPol has been deployed across several jurisdictions, while in India, state initiatives such as MARVEL (Maharashtra's AI-based crime analytics system) and CMAPS (used in Telangana) have signalled an increasing reliance on data-driven policing practices.[1]

Yet this technological promise is accompanied by profound constitutional and human rights concerns. Critics note that predictive policing systems tend to reproduce, rather than remedy, the biases embedded in historical crime datasets. Because past policing practices often disproportionately target marginalised communities, algorithms trained on such data risk entrenching systemic discrimination under a veneer of scientific objectivity.[2] This problem is not confined to foreign jurisdictions: Indian deployments such as MARVEL and CMAPS raise serious questions under Articles 14 and 21 of the Constitution, particularly regarding equality before the law, the presumption of innocence, and the right to due process.[3] Furthermore, the opacity of algorithmic systems makes it difficult for individuals to challenge adverse outcomes, undermining the principle of procedural fairness.

Accountability for harms caused by predictive policing remains unsettled. If an algorithm recommends heightened surveillance of a neighbourhood that leads to wrongful arrests or excessive policing, responsibility is diffused between multiple actors: the state, the police officers relying on algorithmic guidance, and the private companies that design and market these systems.[4] Comparative global experiences illustrate this dilemma. In *State v. Loomis*, the Wisconsin Supreme Court acknowledged the risk of bias and opacity in the COMPAS sentencing algorithm but upheld its use, depicting the judiciary's uncertainty in regulating predictive tools.[5] Similarly, experimental uses of AI in South Africa and regulatory responses in the European Union demonstrate the global contestation surrounding algorithmic crime control.[6]

In this context, predictive policing in India is at a constitutional crossroads. While the state seeks to modernise policing practices through AI-driven systems, the absence of robust legal safeguards raises the danger of normalising algorithmic surveillance without adequate oversight. This

[1] Centre for Internet and Society, *Predictive Policing in India: Towards Transparency and Accountability* (2019) https://cis-india.org/internet-governance/predictive-policing-in-india.pdf accessed 8 September 2025

[2] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press 2017)

[3] Constitution of India, arts 14 and 21

[4] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press 2018)

[5] *State v Loomis* 881 NW 2d 749 (Wis 2016)

[6] Virginia Dignum, *Responsible Artificial Intelligence: Designing AI for Human Values* (Springer 2018); European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)* COM(2021) 206 final

paper examines whether predictive policing can be harmonised with constitutional guarantees of fairness, equality, and accountability, or whether it risks entrenching a technologically reinforced regime of discrimination.

2. Statement of the Problem

The rise of predictive policing algorithms offers the promise of efficiency in crime prevention but also raises profound constitutional and ethical concerns. By relying on historical crime data, these systems risk perpetuating entrenched biases, disproportionately targeting marginalised groups. International experiences illustrate this danger: in the United States, deportation surveillance and predictive tools have been shown to disproportionately affect people of colour, while the *Loomis* case revealed how opaque algorithms can undermine due process. In South Africa, early trials depicted the tension between technology-driven policing and constitutional rights. In India, with initiatives like MARVEL and CMAPS emerging in the absence of strong data protection laws, algorithmic transparency, or independent oversight, the dangers of discrimination, wrongful arrests, and over-surveillance are magnified. The problem lies in reconciling the technological promise of predictive policing with the constitutional guarantees of equality, non-discrimination, privacy, and due process.

3. Literature Review

Angwin, Julia, and colleagues widely cited ProPublica's investigation *Machine Bias* provides compelling empirical evidence that the COMPAS risk-assessment tool disproportionately classified Black defendants as high-risk while underestimating the risk posed by White defendants, highlighting systemic racial bias in algorithmic decision-making and demonstrating how predictive tools can replicate and entrench structural inequalities.[7]

Citron, Danielle and Pasquale, Frank, in *The Scored Society: Due Process for Automated Predictions*, underline serious due process concerns, explaining that so-called ‘black box’ algorithms deny defendants meaningful opportunities to understand or contest the logic behind adverse outcomes, thereby undermining procedural fairness and constitutional protections.[8]

Centre for Internet and Society (CIS), in its report *Predictive Policing in India: Towards Transparency and Accountability*, critiques Indian predictive policing programmes such as the Maharashtra Advanced Research and Vigilance for Enhanced Law Enforcement (MARVEL) and the Crime Mapping, Analytics and Predictive System (CMAPS). The report emphasises the absence of statutory safeguards, independent audits, and clear accountability mechanisms, warning that such opacity threatens fundamental rights and constitutional guarantees.[9]

Dignum, Virginia, in *Responsible Artificial Intelligence*, draws attention to debates in South Africa and other jurisdictions about accountability and oversight in experimental applications of AI policing. Dignum argues that responsible AI deployment requires clear norms of transparency, explainability, and human control, which remain largely absent in many countries, including India.[10]

Eubanks, Virginia, in *Automating Inequality*, examines how predictive policing technologies perpetuate what she terms a ‘digital poorhouse,’ whereby marginalised communities are subjected to heightened surveillance and intervention, while accountability is diffused across state agencies and private contractors. Eubanks’ work reveals the risk of algorithmic systems reproducing historical injustices under the guise of technological neutrality.[11]

European Union, through its proposed *Artificial Intelligence Act*, explicitly designates predictive policing as a ‘high-risk application of AI, mandating rigorous standards of transparency, auditability, and continuous human oversight. This legislative approach illustrates how technological innovation can be aligned with fundamental rights protections and offers a potential regulatory model for jurisdictions such as India.[12]

Ferguson, Andrew Guthrie, in *The Rise of Big Data Policing*, argues that predictive policing is far from a neutral innovation. Instead, it embeds and magnifies historical patterns of discrimination, with data-driven tools often reflecting the biased practices of past policing, thereby perpetuating inequalities while presenting an appearance of scientific objectivity.[13]

Judicial perspectives reinforce these scholarly concerns. In *State v Loomis*, the Wisconsin Supreme Court acknowledged the opacity of the COMPAS algorithm but nevertheless allowed its use in sentencing, illustrating the judiciary’s struggle to balance efficiency with fairness and due process.[14] The Supreme Court of India in *Justice K.S. Puttaswamy v. Union of India* recognised privacy as a fundamental right and stressed the necessity of

[7] Julia Angwin and others, ‘Machine Bias’ *ProPublica* (23 May 2016) https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing accessed 15 September 2025

[8] Danielle Keats Citron and Frank Pasquale, ‘The Scored Society: Due Process for Automated Predictions’ (2014) 89 *Washington Law Review* 1

[9] Centre for Internet and Society (n 1)

[10] Virginia Dignum, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way* (Springer 2019)

[11] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin’s Press 2018)

[12] European Commission, ‘Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)’ COM (2021) 206 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 accessed 15 September 2025

[13] Ferguson (n 2)

[14] *Loomis* (n 5)

proportionality in state surveillance, a principle highly relevant to predictive policing in the Indian context.[15]

Across these strands of scholarship and jurisprudence, a broad consensus emerges: predictive policing, while offering promises of efficiency and crime reduction, risks undermining constitutional rights unless supported by robust safeguards of transparency, accountability, and oversight. Claims of algorithmic neutrality often conceal embedded biases that produce discriminatory outcomes under the veneer of objectivity. The Indian experience with MARVEL and CMAPS illustrates these risks, where weak regulatory oversight and opacity threaten due process and equality. In contrast, the European Union's rights-based framework demonstrates that technological innovation can be harmonised with fundamental rights. This paper examines whether India's adoption of predictive policing can be reconciled with constitutional guarantees of fairness, equality, and human dignity, and what regulatory frameworks are required to prevent algorithmic policing from exacerbating systemic discrimination.

Research Gap

Although significant research confirms the bias and constitutional concerns of predictive policing internationally, there is a lack of focused doctrinal and comparative legal analysis on India's specific socio-legal context. Existing studies often overlook India's constitutional protections under Articles 14 and 21 in relation to the opacity and accountability of systems like MARVEL and CMAPS. Moreover, there is a limited examination of the regulatory gaps concerning transparency, liability, and oversight. This paper addresses these gaps by providing a detailed constitutional critique and proposing tailored policy recommendations for India.

Research Objectives

1) To critically analyse the constitutional and legal implications of predictive policing in India.
2) To examine how historical crime data and algorithmic design affect fairness, accuracy, and non-discrimination.
3) To investigate accountability gaps in cases of wrongful arrests, surveillance, or bias caused by predictive policing.
4) To conduct a comparative study of international experiences to identify lessons for India.
5) To propose regulatory safeguards and policy frameworks ensuring the ethical and rights-compliant use of AI in law enforcement.

Research Questions

1) Does predictive policing undermine constitutional guarantees such as equality, due process, and the presumption of innocence?
2) How do biases in historical crime data affect the accuracy and fairness of predictive policing algorithms?
3) Who should be held accountable for violation of rights caused by algorithmic predictions - the state, police officers, or software developers?
4) What regulatory or policy measures can ensure that predictive policing in India operates transparently, fairly, and in line with human rights obligations?

Hypothesis

While predictive policing algorithms promise efficiency and proactive crime prevention, their reliance on biased historical data risks reinforcing systemic discrimination and undermining constitutional safeguards. India's existing legal framework is insufficient to address accountability and rights violations arising from AI-driven policing.

4. Research Methodology

This paper has adopted a doctrinal research methodology. Primary sources such as constitutional provisions, statutes, case laws (both Indian and international), and official reports have been analysed. Secondary sources, including scholarly articles, policy papers, and critiques of AI in law enforcement, have informed the study. Comparative analysis of case studies like the U.S. Loomis decision and South Africa's AI policing trials has provided insights into the successes, failures, and safeguards adopted elsewhere. The Indian context has been examined through existing initiatives like MARVEL and CMAPS, evaluating their design, data use, and transparency.

4.1 Predictive Policing: Concepts and Context

Predictive policing refers to the application of data analytics, artificial intelligence, and algorithmic models to anticipate where crimes are likely to occur, who might commit them, or who is at greatest risk of victimisation. It represents a fundamental shift in criminal justice strategy, moving from reactive law enforcement towards a more proactive model. By leveraging statistical correlations and patterns in large datasets, predictive policing aims to guide the deployment of police resources with greater efficiency than traditional methods. While crime forecasting is not entirely new, the integration of machine learning and AI has dramatically increased the scale and speed of prediction, raising both possibilities and constitutional concerns.

4.1.1 Concept and Evolution of Predictive Policing

The origins of predictive policing can be traced to criminological theories of the 20th century, particularly the "broken windows" theory and hot-spot policing, which emphasised the concentration of criminal activity in certain geographic areas. The advancement of computational power and access to large digital datasets in the early 2000s provided a technological basis for developing algorithms that could detect patterns in past crime data. One of the earliest and most prominent systems was PredPol, developed through a collaboration between the Los Angeles Police Department and academic researchers, which sought to predict crime hotspots using statistical modelling akin to earthquake aftershock predictions.[16]

This innovation was followed by risk-assessment tools designed to evaluate the likelihood of recidivism, such as the

[15] *Justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

[16] Ferguson (n 2)

Paper ID: SR26325204616 DOI: https://dx.doi.org/10.21275/SR26325204616

Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) algorithm in the United States. Originally designed to assist parole and sentencing decisions, COMPAS relied on multiple data points, ranging from criminal history to socio-economic background, to generate "risk scores."[17] Although COMPAS was not a policing tool per se, its predictive logic significantly influenced law enforcement practices and provided a template for integrating AI into judicial and policing systems.

In India, predictive policing has more recently become part of crime-control strategies, particularly through the Crime and Criminal Tracking Network and Systems (CCTNS) and state-level AI-driven platforms. Maharashtra's AI-based crime analytics system 'MARVEL' and Telangana's Crime Mapping, Analytics and Predictive System 'CMAPS' exemplify the integration of predictive models in policing at the state level.[18] These systems, though less publicised than their Western counterparts, mark a clear transition towards data-driven law enforcement within the Indian criminal justice landscape.

4.1.2 Technologies and Algorithms: COMPAS, PredPol, MARVEL, CMAPS

Predictive policing technologies generally fall into two broad categories: place-based algorithms and person-based algorithms. Place-based systems such as PredPol focus on geographical areas with high crime risk, whereas person-based tools such as COMPAS assess the likelihood of individuals reoffending.

PredPol was designed to forecast the locations and times where crimes were most likely to occur, primarily for property and drug-related offences. It uses three key variables: the type of crime, location, and time of day.[19] The output is a map with designated "hotspot boxes," allowing police officers to increase patrols in those areas. Despite its promise, studies have revealed that PredPol disproportionately targeted minority neighbourhoods, leading to concerns of discriminatory policing disguised as scientific neutrality.[20]

COMPAS, by contrast, is a person-based risk assessment algorithm. It calculates an individual's probability of reoffending using a questionnaire of over 100 variables.[21] The tool gained global attention after the ProPublica investigation 'Machine Bias', which showed that COMPAS falsely labelled African-American defendants as high-risk at nearly twice the rate of Caucasian defendants.[22] This raised concerns that predictive algorithms were replicating systemic racial biases embedded in historical data, while simultaneously obscuring them under a veneer of objectivity.

In the Indian context, CMAPS in Telangana and Andhra Pradesh integrates GIS mapping, CCTV feeds, and historical data to identify vulnerable zones and track offenders. It reportedly allows police to 'geo-tag' crime incidents and analyse patterns for future predictions. MARVEL, launched in Maharashtra, operates as a data-driven crime analytics system combining AI with state police databases. Both systems, however, lack publicly available details on their algorithmic design, transparency mechanisms, or safeguards against bias. The opacity of these platforms poses significant challenges for accountability and constitutional scrutiny.[23]

4.1.3 Claimed Benefits: Efficiency, Prevention, and Crime Control

The promise of predictive policing lies in its potential to enhance law enforcement efficiency and enable proactive crime prevention. Proponents argue that by directing resources to the most crime-prone areas, predictive policing can reduce response times, deter offences, and optimise manpower allocation.[24] In an era of limited police resources, such targeted deployment is seen as a rational and evidence-based approach.

In addition to efficiency, predictive policing is promoted as a crime-prevention tool. The logic is that visible police presence in predicted hotspots acts as a deterrent to would-be offenders. Similarly, person-based tools like COMPAS claim to assist in parole decisions, theoretically reducing the risk of releasing high-risk offenders while facilitating the reintegration of low-risk individuals.[25] Advocates further suggest that predictive tools can reduce subjective bias by relying on data rather than individual police discretion.

Another benefit often cited is the ability of predictive policing to provide strategic insights into broader crime trends. Large-scale data analysis can help identify emerging crime patterns, such as cybercrime or organised theft networks, which might otherwise go undetected.[26] In countries like India, where police forces are often

---

[17] Sarah Brayne, 'Big Data Surveillance: The Case of Policing' (2017) 82(5) *American Sociological Review* 977 https://pmc.ncbi.nlm.nih.gov/articles/PMC10846878/ accessed 10 September 2025

[18] 'MARVEL: Maharashtra Unveils India's First AI Crime-Fighting Initiative' (Mumbai Live, 18 July 2024) https://www.mumbailive.com/en/civic/maharashtra-unveils-india's-first-ai-crime-fighting-initiative-85015 accessed 10 September 2025

[19] PredPol, 'How Predictive Policing Works' (PredPol) https://www.predpol.com/how-predictive-policing-works/ accessed 10 September 2025

[20] Kristian Lum and William Isaac, 'To Predict and Serve?' (2016) *Significance* 14 https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x accessed 10 September 2025

[21] Angwin and others (n 7).

[22] Ibid

[23] gana State Police, 'Crime Mapping, Analytics and Predictive System (CMAPS)' (Telangana Police) https://www.tspolice.gov.in/cmaps accessed 10 September 2025

[24] Centre for Internet and Society (n 1)

[25] Telangana State Police, 'Crime Mapping, Analytics and Predictive System (CMAPS)' (Telangana Police) https://www.tspolice.gov.in/cmaps accessed 10 September 2025

[26] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press 2018)

overburdened, algorithmic analysis is touted as a way to modernise law enforcement and align it with ‘smart city’ governance initiatives.

Yet these claimed benefits must be approached with caution. As scholars such as Andrew Ferguson have argued, predictive policing is not a neutral technology but one embedded in social, political, and historical contexts.[27] Efficiency claims often ignore the fact that the underlying data reflect patterns of over-policing in marginalised communities. Similarly, the deterrence effect is difficult to measure empirically, and algorithmic predictions often lack the transparency required to validate their accuracy.

Understanding predictive policing requires situating its technological promise within broader debates on fairness, discrimination, and accountability. On one hand, predictive tools offer law enforcement agencies new means of allocating scarce resources, potentially reducing crime and improving public safety. On the other, these very tools risk entrenching historical injustices by reproducing biased datasets and concealing them behind the authority of “scientific” prediction.

The case of COMPAS illustrates how algorithms may reinforce racial disparities, while PredPol demonstrates the risks of discriminatory targeting in urban policing. In India, MARVEL and CMAPS raise similar issues, compounded by the absence of strong data protection laws or algorithmic transparency mandates. Without robust oversight, predictive policing risks becoming a tool for normalising surveillance and arbitrary decision-making.

Thus, while predictive policing may promise efficiency, its adoption cannot be divorced from constitutional and ethical considerations. Rather than assuming neutrality, predictive algorithms must be critically examined as part of a wider system of power relations, with implications for fundamental rights, equality before law, and the presumption of innocence.

4.2 Predictive Policing Algorithms in India

India’s embrace of data-driven governance has accelerated the adoption of predictive policing, a practice that employs algorithmic models to forecast the likelihood of crime in particular locations or by particular individuals. While the promise of improved efficiency and proactive crime prevention attracts policymakers, the constitutional and human-rights implications are profound.

4.2.1 CMAPS and MARVEL: Design and Functionality

The Crime Mapping, Analytics and Predictive System (CMAPS) was first piloted in the state of Andhra Pradesh and later adopted by the Telangana Police. It integrates historical crime records, geographic information systems, and extensive networks of CCTV cameras to create real-time “heat maps” identifying zones of heightened criminal risk.[28] The platform can issue immediate alerts to field officers, allowing patrols to be redeployed dynamically.

Maharashtra’s MARVEL (Maharashtra Advanced Research and Vigilance for Enhanced Law Enforcement) similarly combines large datasets of First Information Reports (FIRs), prior criminal records and live surveillance feeds.[29] The system uses pattern-recognition techniques and natural-language processing to draw links between incidents and to suggest possible hotspots for preemptive policing.

Despite their sophistication, both projects remain opaque. Neither has released its algorithmic architecture, weighting of variables or data-cleaning methods.[30] Independent academic or judicial audits have not been conducted, and internal police documentation is largely inaccessible through public-information requests. This opacity inhibits assessment of accuracy and of compliance with constitutional rights.

4.2.2 Data Quality, Transparency, and Bias Concerns

Predictive algorithms inevitably reflect the quality and distribution of their input data. Indian crime statistics are shaped by socio-economic realities, including under-reporting in rural districts, selective registration of FIRs, and historic patterns of caste- and community-based policing.[31] Dalit and Adivasi communities, for example, experience disproportionate surveillance and arrest rates.[32] Training an algorithm on such data risks reinforcing these inequities, presenting them as neutral ‘scientific’ predictions while masking structural discrimination.

The lack of algorithmic transparency compounds the problem. Public access to the training data, the criteria for data exclusion, or the statistical models used is non-existent. Without such disclosure, it is impossible to evaluate whether CMAPS or MARVEL satisfy constitutional requirements of equality before the law (Article 14) and protection of life and personal liberty (Article 21).[33]

The Supreme Court in *Justice K.S. Puttaswamy v. Union of India* held that any state surveillance must meet the tests of legality, necessity and proportionality.[34] Predictive policing projects launched through executive action, with neither legislative authorisation nor independent oversight, are unlikely to meet these standards. Citizens flagged by an algorithm have no clear avenue to contest their inclusion in ‘high-risk’ categories, creating a de facto system of unreviewable state surveillance.

---

[27] Ferguson (n 2)
[28] K Natwar Singh, ‘AI Integration in Telangana Police: Analyzing Efficiency and Ethical Dimensions’ (2024) 28(1) Museonaturalistico 3378, 3383-3390 https://www.museonaturalistico.it/index.php/journal/article/download/710/557/1328 accessed 10 September 2025
[29] Centre for Internet and Society (n 1)
[30] ibid
[31] National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs 2024)
[32] National Campaign on Dalit Human Rights, *Police Discrimination and Dalit Vulnerability* (2021) https://www.ncdhr.org/publications accessed 12 September 2025
[33] Constitution of India 1950, arts 14 and 21
[34] *Puttaswamy* (n 15)

Furthermore, the deployment of CMAPS and MARVEL occurs against the backdrop of India's ambitious smart city initiatives, where municipal governance increasingly depends on integrated data platforms. Predictive policing thereby risks normalising continuous surveillance in urban centres, encouraging pre-emptive police action and blurring the distinction between preventive and punitive state power. Cultural analogies such as the film *Minority Report* (2002), which depicts a 'pre-crime' unit arresting individuals before any offence occurs, illustrate the dystopian potential of such logic when unchecked by legal safeguards.

4.2.3 Towards a Rights-Based Approach

A rights-compliant framework for predictive policing must therefore include: (i) independent algorithmic audits to assess bias and accuracy; (ii) publication of impact assessments and model documentation; (iii) clear legislative authorisation establishing necessity and proportionality; and (iv) remedies for individuals adversely affected. Absent these safeguards, predictive policing threatens to entrench technologically reinforced discrimination and erode public trust in law enforcement.

India's legal system has not kept pace with the technological complexity of predictive policing. Although various statutes touch on data protection and electronic surveillance, none directly regulates algorithmic decision-making in law enforcement.

4.2.4 Legal and Regulatory Framework for Predictive Policing in India

The Digital Personal Data Protection Act 2023 (DPDP Act) is India's principal privacy statute. It introduces consent-based processing and establishes a Data Protection Board.[35] Yet section 17(2)(a) exempts *"functions of the State,"* including policing and public-order maintenance, from key safeguards such as purpose limitation and prior authorisation.[36] Consequently, systems like CMAPS and MARVEL may collect and analyse vast quantities of personal data without individual consent or meaningful external scrutiny.

The Information Technology Act 2000, supplemented by the 2011 Rules on Reasonable Security Practices, focuses mainly on private intermediaries and offers no requirements for algorithmic audits or transparency in state use of AI.[37] Neither the Code of Criminal Procedure 1973 nor the Indian Evidence Act 1872 addresses the evidentiary status of algorithmic risk assessments or the procedural rights of persons identified by predictive tools.

The responsibility for accountability in predictive policing within India is dispersed among three primary groups. The State and Police Agencies oversee the implementation and management of predictive systems and hold a constitutional obligation to protect fundamental rights. Nevertheless, there is currently no specific law that imposes strict liability for harms such as wrongful arrests or discriminatory practices. Individual officers may shift accountability by citing algorithmic outputs as 'objective' data that guide decisions, thereby minimising their personal discretion. Private vendors develop and maintain proprietary algorithms that are often safeguarded by trade-secret protections, restricting transparency and external scrutiny. This fragmented accountability structure complicates the clear assignment of responsibility and creates significant challenges to effective oversight and remedy in the use of AI-powered policing tools. This diffusion creates a responsibility gap, leaving individuals harmed by algorithmic error without a clear path to redress.[38]

The Supreme Court's decision in *Justice K.S. Puttaswamy v Union of India* mandates that any surveillance satisfy tests of legality, necessity and proportionality.[39] Predictive policing systems implemented through executive orders and shielded from public oversight cannot easily meet these requirements. Potential violations of Articles 14 and 21 thus remain a persistent risk.

To reconcile predictive policing with constitutional guarantees, India requires a dedicated legislative framework that mandates independent algorithmic impact assessments and periodic audits, defines liability regimes allocating responsibility among the state, police officers, and private developers, provides for judicially reviewable authorisation before deployment, and ensures notice and remedy for individuals adversely affected. Without such reforms, predictive policing will continue to operate as a technologically advanced yet legally under-regulated practice, undermining public trust and constitutional rights.[40]

4.3 Constitutional Validity of Predictive Policing

Predictive policing integrates algorithmic decision-making into core law enforcement activities. Although it promises enhanced efficiency and crime prevention, its constitutional validity in India rests on compliance with fundamental rights, including equality before the law, the presumption of innocence and due process, and the right to privacy as affirmed by the Supreme Court in the Justice K.S. Puttaswamy case.

---

[35] Government of India, The Digital Personal Data Protection Act 2023 (2023) https://egazette.nic.in/WriteReadData/2023/250813.pdf accessed 14 September 2025

[36] Ibid

[37] Information Technology Act 2000 (India); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 https://www.meity.gov.in/writereaddata/files/it_act2000/it_amendment_act2008.pdf accessed 14 September 2025

[38] D K Basu, 'Liability and Accountability in AI-driven Policing' (2025) 11 Law Journals 78 https://lawjournals.org/assets/archives/2025/vol11issue5/11111.pdf accessed 14 September 2025

[39] *Puttaswamy* (n 15)

[40] K Natwar Singh, 'AI Integration in Telangana Police: Analyzing Efficiency and Ethical Dimensions' (2024) 28(1) Museonaturalistico 3378 https://www.museonaturalistico.it/index.php/journal/article/download/710/557/1328 accessed 14 September 2025

Paper ID: SR26325204616 DOI: https://dx.doi.org/10.21275/SR26325204616

4.3.1 Equality Before Law and Non-discrimination (Article 14)

Article 14 of the Constitution mandates that the State shall not deny any person equality before the law or the equal protection of the laws.[41] Within this framework, Indian courts have consistently affirmed that any state action must be founded on reasonable classification and must avoid arbitrariness.[42] Predictive policing systems rely on historical crime data which often reflects entrenched social inequities such as the disproportionate policing of Dalit and Adivasi communities.[43] the over-representation of religious minorities in arrest statistics, and the under-reporting of crimes in affluent areas Algorithms trained on such biased datasets therefore risk producing predictions that disproportionately target already marginalised groups.[44]

The opacity of systems like the Crime Mapping, Analytics and Predictive System (CMAPS) and Maharashtra's MARVEL makes it difficult to determine whether the models incorporate safeguards against bias or whether their outputs have disparate impacts.[45]

Where a facially neutral algorithm leads to disproportionate surveillance of specific communities, the state action implementing those outputs risks being manifestly arbitrary and thus violative of Article 14.[5] The Supreme Court has repeatedly held that arbitrariness is antithetical to equality, most notably in *E.P. Royappa v State of Tamil Nadu* and later in *Shayara Bano v Union of India*.[46] Predictive policing without demonstrable fairness metrics or independent audits cannot easily satisfy these constitutional standards.

4.3.2 Presumption of Innocence and Due Process (Article 21)

Article 21 protects the right to life and personal liberty except according to a procedure established by law that is fair, just and reasonable.[47] Predictive policing challenges this guarantee by shifting the focus from past conduct to anticipated future behaviour.

Individuals or neighbourhoods labelled 'high-risk' may experience intensified surveillance, frequent stops, or even pre-emptive detention, effectively punishing them for crimes not yet committed.

The presumption of innocence, though not explicitly stated in the Constitution, is a core component of Article 21 and the criminal justice system. In *Maneka Gandhi v. Union of India*, the Supreme Court expanded Article 21 to require fairness and non-arbitrariness in any state action affecting liberty.[48] When police officers rely on opaque algorithmic risk scores, individuals may be subjected to adverse action without notice, disclosure of the underlying data, or an opportunity to contest the basis of the prediction. Such practices compromise both procedural due process and the substantive guarantee of liberty.[49]

Moreover, Indian evidentiary law has yet to recognise or regulate algorithmic predictions. The Indian Evidence Act 1872 provides no framework for admitting or challenging AI-generated risk assessments, leaving affected individuals without effective procedural safeguards.

4.3.3 Privacy and Surveillance Concerns

The nine-judge bench in *Justice K.S. Puttaswamy v. Union of India* declared privacy a fundamental right and articulated the triple test of legality, necessity and proportionality for any state intrusion.[50] Predictive policing initiatives such as CMAPS and MARVEL operate primarily through executive orders and internal police directives, lacking clear statutory authorisation. This absence of a legislatively enacted, narrowly tailored law fails the first prong of the *Puttaswamy* test.[51]

Even if legality were established, the state must show that predictive policing is necessary for a legitimate aim and that less intrusive measures would not suffice. Given that conventional crime-prevention strategies exist and the empirical effectiveness of predictive policing remains contested, demonstrating necessity is difficult. Finally, proportionality requires a balance between the extent of the privacy infringement and the importance of the objective.

Continuous surveillance and mass data collection inherent in predictive policing, often of individuals with no criminal record, pose a significant and arguably disproportionate intrusion into personal autonomy and informational privacy.

Predictive policing, as presently practised in India, faces formidable constitutional hurdles. Its reliance on biased historical data threatens equality under Article 14; its focus on forecasting potential offences undermines the presumption of innocence and the due-process guarantees of Article 21; and its pervasive surveillance contravenes the privacy protections set out in *Puttaswamy*.

Absent explicit legislative authorisation, transparent algorithmic auditing, and enforceable procedural safeguards, the deployment of predictive policing cannot be reconciled with India's constitutional framework.

---

[41] Constitution of India 1950, art 14

[42] *State of West Bengal v Anwar Ali Sarkar* AIR 1952 SC 75 at 78

[43] Over half of prisoners in India are Muslims, Dalits and Adivasis. Newsclick, 2023 https://www.newsclick.in/over-half-prisoners-india-are-muslims-dalits-and-adivasis accessed 14 September 2025

[44] National Campaign on Dalit Human Rights, *Police Discrimination and Dalit Vulnerability* (2021) https://www.ncdhr.org/publications accessed 12 September 2025

[45] Centre for Internet and Society (n 7)

[46] *E P Royappa v State of Tamil Nadu* (1974) 4 SCC 3 at 38; *Shayara Bano v Union of* India AIR 2017 SC 4609

[47] Constitution of India, Article 21

[48] *Maneka Gandhi v Union of India* AIR 1978 SC 597

[49] Bikram Singh Goraya, 'Judicial Approach to Predictive Policing and Electronic Surveillance in India vis-à-vis Right to Privacy' (2023) 10 Indian Journal of Law & Technology 45

[50]

[51] D K Basu, 'Liability and Accountability in AI-Driven Policing' (2025) 11 Law Journals 78

4.4 Comparative Perspectives on Predictive Policing

While India's engagement with predictive policing is relatively recent, other jurisdictions have grappled with similar technologies for over a decade. Examining global experiences provides insight into regulatory options, accountability models, and constitutional safeguards that may guide Indian policy.

4.4.1 United States: State v. Loomis and Debates on COMPAS

The United States pioneered predictive policing through both place-based and person-based systems. One of the most influential person-based tools is the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), which assesses the likelihood of recidivism using variables such as prior arrests, socio-economic factors, and behavioural questionnaires.[52]

The constitutional tension surrounding COMPAS surfaced in *State v. Loomis*, where the Wisconsin Supreme Court considered whether a sentencing judge's reliance on a COMPAS risk score violated due process.[53] The Court acknowledged the algorithm's proprietary nature and the inability of defendants to challenge its methodology, yet upheld its use with cautionary instructions. Critics argue that this decision entrenched opacity and allowed racially biased data to influence sentencing.[54]

Parallel concerns surround place-based tools such as PredPol, which use historical crime data to identify 'hotspots.' Investigations show that these systems disproportionately direct police patrols toward predominantly Black and Latino neighbourhoods, reinforcing racial disparities in arrests and, indirectly, immigration-enforcement and deportation processes.[55] U.S. civil-rights advocates contend that such tools, when deployed without rigorous audits, perpetuate structural racism under the guise of objectivity.

4.4.2 South Africa: Experimental AI Policing Trials and Judicial Oversight

South Africa offers a contrasting example of early engagement combined with constitutional vigilance. Pilot programmes in Johannesburg and Cape Town have experimented with predictive analytics to address high rates of violent crime.[56] Civil-society groups quickly raised concerns about privacy, racial profiling, and the potential for over-policing historically disadvantaged communities. South Africa's Constitution guarantees robust rights to equality, dignity, and privacy, prompting calls for judicial review and legislative safeguards. The South African Human Rights Commission has emphasised the need for explicit statutory authorisation, independent impact assessments, and community consultation before deploying predictive tools.[57] Although comprehensive national legislation has yet to be enacted, these oversight efforts highlight a proactive approach to balancing technological innovation with constitutional rights.

4.4.3 European Union: The AI Act and Emerging Regulatory Safeguards

The European Union has adopted a detailed, risk-based regulatory approach in its Artificial Intelligence Act, classifying predictive policing as a 'high-risk' application. This designation imposes rigorous obligations on predictive policing systems, including comprehensive documentation of training data and model design, mandatory independent conformity assessments, and the requirement for human oversight in decision-making processes. Further, the Act establishes a framework for post-market monitoring to identify and mitigate unforeseen harms. Regulators are empowered to levy administrative fines on entities that fail to comply, and individuals adversely affected by violations of fundamental rights under the EU Charter may seek legal remedies. This framework aims to ensure accountability, transparency, and the protection of fundamental rights in the deployment of AI technologies in law enforcement.[58]

Member states are supplementing this framework with national initiatives. For example, the Netherlands requires privacy impact assessments for algorithmic policing, while Germany's federal data-protection authorities have issued guidance demanding transparency and auditability of predictive tools.[59] These measures aim to ensure that algorithmic innovation proceeds only within a rights-respecting framework.

The comparative analysis brings to light three recurring concerns in the regulation of algorithmic governance: the risk of entrenching historical biases, the opacity of proprietary systems, and the difficulty of allocating accountability between state actors and private developers. The United States illustrates the dangers of deploying predictive technologies in the absence of robust transparency requirements, while South Africa demonstrates the value of instituting early rights-based scrutiny. The European Union, through its comprehensive legislative framework, offers the most rigorous model by requiring algorithmic audits, risk

---

[52] Angwin and others (n 7)
[53] *Loomis* (n 5)
[54] Danielle K Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Wash L Rev 1
[55] Kristian Lum and William Isaac, 'To Predict and Serve?' (2016) *Significance* 14 https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x accessed 12 September 2025
[56] Virginia Dignum, *Responsible Artificial Intelligence* (Springer 2019) 142–144.
6 South African Human Rights Commission, *Technology and Human Rights: Annual Report* (2022) https://sahrc.org.za accessed 12 September 2025
[57] European Commission, 'Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' COM (2021) 206 final https://artificial-intelligence-act.eu/ accessed 12 September 2025
[58] Charter of Fundamental Rights of the European Union [2012] OJ C326/391
[59] European Union Agency for Fundamental Rights, *Getting the Future Right: AI and Fundamental Rights* (2022) https://fra.europa.eu/en/publication/2022/artificial-intelligence-fundamental-rights accessed 12 September 2025

categorisation, and human oversight as conditions of deployment.

For India, these global experiences highlight the urgency of enacting a dedicated statutory regime that imposes mandatory impact assessments, public-facing audits, and clearly delineated liability provisions. Such a framework would align algorithmic governance with constitutional protections under Articles 14, 19, and 21, ensuring that fundamental rights are not compromised by technological opacity or unchecked private innovation. Without these safeguards, India risks replicating the controversies over racial bias that have plagued the United States and forfeiting the proactive, rights-driven protections now emerging in Europe and South Africa.

5. Conclusion

The accelerating adoption of predictive policing technologies in India represents both an opportunity and a profound constitutional challenge. On one hand, data-driven tools promise more efficient law enforcement by anticipating crime trends and guiding police deployment. On the other hand, these technologies exacerbate concerns around embedded bias, unchecked surveillance, and erosion of due process.

Key Insights and Concerns

Predictive policing depends heavily on historical crime data that, in India, reflects caste- and community-based disparities. Algorithms run the risk of encoding such systemic prejudice as ostensibly objective outputs.[60] Leading predictive systems in India, such as CMAPS and MARVEL, currently operate without statutory authorisation, transparency about their design or data, or independent audits.[61] This opacity prevents meaningful examination of fairness, accuracy, and compatibility with constitutional protections under Articles 14 and 21.

The legislative framework remains fragmented. The Digital Personal Data Protection Act 2023 grants broad state exemptions, while the Information Technology Act 2000, the Indian Evidence Act 1872, and the Code of Criminal Procedure 1973 do not address algorithmic governance or AI-generated evidence.[62] Comparative experiences illustrate that the U.S. has faced repeated controversies due to lack of regulation,[63] South Africa stresses early rights-based oversight,[64] and the European Union advances a risk-based statutory model mandating transparency, audits, and human oversight.[65] Accountability in India is unclear: state agencies avoid strict liability, police officers face a 'human-in-the-loop' paradox, and vendors protect proprietary systems through trade secrets.

6. Policy and Legal Recommendations: Towards a Rights-Based Framework

India should enact a dedicated Predictive Policing Regulation Act containing the following core statutory principles:

1) **Legality and Authorisation:** No predictive policing system may be deployed without explicit statutory approval, subject to parliamentary oversight and periodic review.
2) **Algorithmic Transparency and Audits:** Mandatory disclosure of datasets, modelling techniques, and error margins, with independent audits before deployment and periodically thereafter.
3) **Necessity and Proportionality:** Deployment is permitted only when strictly necessary for legitimate aims and where no less intrusive alternatives exist.
4) **Due Process Protections:** Affected individuals must be notified of algorithmic reliance, granted access to relevant data, and afforded the ability to appeal decisions before an independent authority or court.
5) **Liability and Vendor Accountability:** State agencies bear strict liability for violations, supported by vendor obligations to cooperate with audits and litigation. Officers remain bound by professional misconduct standards.
6) **Democratic Oversight:** Implementation of regular impact assessments, civil society consultations, and publication of transparency reports submitted to Parliament.

The future of AI-driven policing in India hinges on such safeguards. Without them, there is a real risk of entrenching bias, institutionalising surveillance, and eroding the presumption of innocence. With them, predictive analytics can enhance public safety while upholding India's

[60] R Murugesan, 'Predictive Policing in India: Deterring Crime or Discriminating Minorities?' (LSE Human Rights Blog, 15 April 2021) https://blogs.lse.ac.uk/humanrights/2021/04/16/predictive-policing-in-india-deterring-crime-or-discriminating-minorities accessed 14 September 2025

[61] Surabhi Agarwal, 'AI Policing Systems in India Lack Oversight' *Economic Times* (New Delhi, 12 December 2023) https://economictimes.indiatimes.com/news/india/ai-policing-systems-lack-oversight/articleshow/XXXXX.cms accessed 14 September 2025

[62] *Digital Personal Data Protection Act 2023*; *Information Technology Act 2000*; *Indian Evidence Act 1872*; *Code of Criminal Procedure 1973*

[63] Rashida Richardson, Jason Schultz, and Kate Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice' (2019) 94 *New York University Law Review Online* 192 https://www.nyulawreview.org/online-feature/dirty-data-bad-predictions accessed 14 September 2025

[64] South African Human Rights Commission, *Report on Human Rights and Technology in South Africa* (2021) https://www.sahrc.org.za/home/21/files/Tech%20Report%202021.pdf accessed 14 September 2025

[65] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM (2021) 206 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A206%3AFIN accessed 14 September 2025

constitutional values of equality, liberty, and dignity. Technology must remain accountable to the citizenry, ensuring predictive policing is governed by law, oversight, and rights.[66]

References

[1] Andrew Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York University Press 2017)
[2] Danielle Citron and Frank Pasquale, *The Scored Society: Due Process for Automated Predictions* (Washington University Press 2019)
[3] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press 2018)
[4] Centre for Internet and Society, *Predictive Policing in India: Towards Transparency and Accountability* (Centre for Internet and Society 2020) https://cis-india.org/internet-governance/predictive-policing-in-india.pdf accessed 14 September 2025
[5] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM (2021) 206 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A206%3AFIN accessed 14 September 2025
[6] Amnesty International, *Automated Racism: The UK's Use of Predictive Policing* (Amnesty International 2025) https://www.theguardian.com/uk-news/2025/feb/19/uk-use-of-predictive-policing-is-racist-and-should-be-banned-says-amnesty accessed 14 September 2025
[7] NAACP, *Artificial Intelligence and Predictive Policing: Issue Brief* (NAACP 2024) https://naacp.org/resources/artificial-intelligence-predictive-policing-issue-brief accessed 14 September 2025
[8] Sarah Brayne, 'Big Data Surveillance: The Case of Policing' (2020) 38 *Journal of Law, Technology & Policy* 1 https://jltp.uchicago.edu/content/big-data-surveillance-case-policing accessed 14 September 2025
[9] A Vats, 'Building the Case for Restricted Use of Predictive Policing' (2022) *Information Ethics* https://informationethics.ca/index.php/irie/article/view/487 accessed 14 September 2025
[10] Almasoud AS, 'Algorithmic Fairness in Predictive Policing' (2024) *AI and Ethics* https://link.springer.com/article/10.1007/s43681-024-00541-3 accessed 14 September 2025
[11] Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, *Machine Bias*, ProPublica (23 May 2016) https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing accessed 14 September 2025
[12] *State v Loomis*, 881 NW 2d 749 (Wisconsin Supreme Court 2016)
[13] *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1

[66] Saptarshi Mandal, 'AI, Rights, and the Indian Constitution' (2024) *India Law Review* 3(1) 45 https://indialawreview.in/2024/01/ai-rights-indian-constitution accessed 14 September 2025