IMPLEMENTATION CHALLENGES OF PREDICTIVE POLICING IN INDIA

***MS. SUSHREE SASWATI MISHRA**
****PROF. (DR.) ARPITA MITRA**

ABSTRACT

Predictive policing involves the use of data analytics, machine learning, and algorithmic modelling on past criminal data to forecast future criminal activity to identify hotspots in crimes and to allocate law enforcement resources in a proactive manner. While countries like the United States and the United Kingdom have been using the tools of predictive policing for more than two decades, India is now at an inflection point where a number of states in the country are piloting systems like CMAPS of Delhi Police, while the national Crime and CCTNS are supporting the tools with the digital infrastructure. This paper takes a critical look into multifaceted implementation challenges that face predictive policing in India. The analysis is organised around five central themes-not only infrastructural and data quality deficiencies are discussed but also algorithmic bias and the entrenchment of caste and religious, as well as socioeconomic discrimination; constitutional and human rights issues (with a particular focus on the right to privacy under Article 21); inadequate legal and regulatory framework (including the Digital Personal Data Protection Act 2023 and its limited application to law enforcement), and institutional capacity, accountability and transparency deficits within Indian policing. The paper contends that unless India overcomes these structural issues with the help of purpose-built legislations, proper oversight structure and inclusive algorithmic governance, predictive policing will end up perpetuating the existing inequities instead of bringing in its claimed public safety benefits. The paper concludes with some recommendations for a rights respecting framework through which the responsible deployment of predictive policing in India can be guided.

Keywords: Predictive Policing, Algorithmic Bias, Data Governance, Privacy Rights, Accountability

*University Junior Research Fellow, The West Bengal National University of Juridical Sciences, (WBNUJS)
**Professor in Criminology, The West Bengal National University of Juridical Sciences (WBNUJS)

I. INTRODUCTION

The combination of artificial intelligence (AI), big data analytics, and law enforcement has led to a new paradigm in crime prevention dubbed predictive policing. At its most basic, predictive policing involves the application of statistical algorithms and machine learning model to big data sets composed of historical data on criminal incidents, arrest records, and demographic data to predict the time, place, and manner of future crimes and to identify potentially likely offenders and/or victims.[1] While the prospect of proactive, data-driven policing has been met with much enthusiasm by law enforcement agencies worldwide, it has also been met with vigorous criticism from civil society, legal scholars and technologists who wonder whether it is accurate, fair and compatible with fundamental rights.

India is an especially complex and consequential environment to consider the prospects of predictive policing. With a population of over 1.4 billion, a turbulent social texture characterized by deep-rooted inequalities of caste, religion, and class, and a law enforcement machinery whose resource limitations and defects of accountability are well-documented, the costs of getting predictive policing wrong are huge indeed. The National Crime Records bureau (NCRB) reported a total of six point two four million cases that occurred in 2023 and with a 7.2 per cent increase since 2022 and cyber-crime surged around 31.2 per cent in the same period.[2] The sheer scale of crime data in India, and the insufficiency of traditional reactive policing, has encouraged policymakers to consider technological ways to solve problems, generally called predictive analytics.

This paper is not written from a simplistically sceptical or enthusiastic viewpoint to predictive policing. Rather, it aims to give a nuanced, evidence-based analysis of the unique challenges that India must face thus far if it is to implement predictive policing in a way that is effective, equitable and constitutionally valid. The analysis continues in five main fields of inquiry, concerning the state of digital infrastructure and data quality; algorithmic bias & outcomes of discrimination; constitutional and human rights implications; adequacy of legal and regulatory

[1] George R, “Predictive Policing: What is it, How it Works, and its Legal Implications' (Centre for Internet and Society, 24 November 2015) <https://cis-india.org/internet-governance/blog/predictive-policing-what-is-it-how-it-works-and-it-legal-implications\> accessed 20 February 2026

[2] National Crime Records Bureau, *Crime in India 2023 Report* (Ministry of Home Affairs, Government of India 2025) <https://ncrb.gov.in\> accessed 20 February 2026; Vision IAS, 'NCRB Releases Crime in India 2023 Report' (30 September 2025) <https://visionias.in/current-affairs/news-today/2025-09-30/social-issues/national-crime-records-bureau-ncrb-releases-crime-in-india-2023-report\> accessed 20 February 2026

framework; and institutional accountability. The paper concludes by providing a suggestion of structural recommendations.

II. PREDICTIVE POLICING INITIATIVES IN INDIA

India's involvement with predictive policing has developed due to a mix of the country's national infrastructure initiatives, and state-level pilot projects. The "Crime and Criminal Tracking Network and Systems" (CCTNS), a Mission Mode Project by the Ministry of Home Affairs project launched in 2009 under the ambit of the National e-Governance Plan is the digital backbone behind India's ecosystem of crime data. The NCRB being the nodal agency has linked more than 15,000 police stations and 6,000 higher police offices in the country through CCTNS and have enabled electronic registration of FIR and maintain the criminal records which is accessible across the state boundaries.[3]

Building on this infrastructure, Delhi Police made an interesting first in India when the police announced the launch of its own predictive policing tool when it unveiled the Crime Mapping, Analytics and Predictive System (CMAPS) in 2015. CMAPS is aimed at live spatial hot spot mapping of crime, criminal behaviour pattern analysis and suspect profiling using data collected by Dial-100 emergency calls, and collected by the CCTNS and data archived from crime. The system updates its crime hotspot predictions every one to three minutes and ranks the police districts based on the intensity of crimes.[4] By 2019, the Digital Police Portal, integrated with CCTNS, extended the reach of such analytics capabilities nationally.[5]

Beyond Delhi, some other states have considered or put in place similar systems. Telangana Police set up 30,000 community-supported CCTV cameras in the surveillance and analytics network. Himachal Pradesh installed more than 19000 CCTVs in January 2020 as part of a CCTVs Surveillance Matrix which will be the foundation of predictive policing. Maharashtra was able to bag a budget for Rs 850 Crore towards developing a safe cyber emergency response system using AI encompassing analytics. Madhya Pradesh, Jharkhand, and Uttar Pradesh have separately discussed/piloted the data analytics in crime prevention. At the national level, plans for the National Automated Facial Recognition System (NAFRS) were unveiled by the

[3] National Crime Records Bureau, 'CCTNS – Crime and Criminal Tracking Network and Systems' (Ministry of Home Affairs, Government of India) <https://ncrb.gov.in/en\> accessed 18 February 2026
[4] Delhi Police / BW Police World, 'Delhi Police Implements Crime Mapping Analytics and Predictive System (CMAPS)' <https://www.bwpoliceworld.com/article/delhi-police-implements-crime-mapping-analytics-predictive-system-cmaps-134283\> accessed 19 February 2026
[5] Saikia N, 'Predictive Policing and the Future of Law Enforcement' (*The Dialogue*, 20 September 2023) <https://thedialogue.co/predictive-policing-and-the-future-of-law-enforcement/\> accessed 19 February 2026

Ministry of Home Affairs in 2019, which aims to identify criminals by using images from the scene of crime and matching them with the records stored in the CCTNS.+

Table 1: Key Predictive Policing Initiatives in India

State/Body	Initiative	Features	Year
Delhi Police	CMAPS	Hotspot mapping, criminal profiling, Dial-100 integration	2015
National (MHA/NCRB)	CCTNS / Digital Police Portal	15,000+ police stations linked; national crime database	2009/2019
Telangana	HydCop App & CCTV Network	30,000 cameras; community-supported surveillance analytics	2017
Himachal Pradesh	CCTV Surveillance Matrix	19,000+ cameras; predictive patrol planning	2020
Maharashtra	Cyber Emergency Response System	Rs 850 Cr AI-driven analytics; cyber task force	2020+
National (MHA)	NAFRS	Facial recognition integrated with CCTNS for criminal ID	2019

Source: Compiled by author from NCRB, BW Police World, PIB, and LSE Human Rights Blog (2015–2026).

More recently, IPS officer Navdeep Aggarwal came up with Smart Prahari - a predictive patrol routing system on the basis of AI developed using open source tools but at zero cost. Smart Prahari anonymises a crime data, places it on encrypted server, generates patrol routes which can be completely auditable and provides a privacy sensitive model for a predictive policing. The range of such policies speaks to the hunger for technological solutions to Indian policing even as much as the lack of a coherent and law based national government policy. [6]

III. INFRASTRUCTURAL AND DATA QUALITY CHALLENGES

The reliability of any predictive policing system is fundamentally dependent on the quality, completeness and representativeness of the underlying data. In India, however, these fundamental requirements are broken by a number of systemic deficiencies. The NCRB itself

[6] Indian Masterminds, 'When AI Becomes the Policeman's Sixth Sense: Smart Prahari' (29 November 2025) <https://indianmasterminds.com/feature-stories-on-bureaucrats-changemakers/when-ai-becomes-the-policemans-sixth-sense-163800/\> accessed 20 February 2026

has pointed out that exchange of information between the neighbouring police stations, districts or states was historically "next to impossible" before the advent of CCTNS. Although CCTNS has produced a lot of improvement in connectivity, data entry quality and uniformity is inconsistent across states and districts.[7]

A huge percentage of data related to crime in India are not digitised. Under-reporting of crimes especially those concerning women, marginalised communities and rural populations causes systematics gaps. When the process of First Information Report (FIR) is not registered, then no crime goes into the system, and the algorithmic model is in effect working on data that is skewed by past patterns of police inaction and is not representative of the actual incidence of crimes. The NCRB's report on Crime in India in 2023 said the charge-sheeting rate among ignoratio مساعد for Dengue crimes in India was 72.7 per cent while conviction rate was only 54 per cent-this indicates deep inefficiencies in our crime justice system, which the algorithmic tools alone will not be able to remedy.

Table 2: India Crime Statistics 2022–2023 (NCRB)

Indicator	2022	2023	Change (%)
Total Crimes Registered	5.82 million	6.24 million	+7.2%
IPC Crimes	3.56 million	3.76 million	+5.7%
Cybercrimes	65,893	86,434	+31.2%
Charge-sheeting Rate (IPC)	71.3%	72.7%	+1.4 pp
Conviction Rate (IPC)	54%	54%	No change
Crime Rate (per lakh population)	422.2	448.3	+6.2%

Source: National Crime Records Bureau, Crime in India 2022 and 2023 Reports[8], Ministry of Home Affairs, Government of India.

Furthermore, the data feeding predictive models is far from being gathered through automated processes, i.e. human judgment is embedded in the decision to register an FIR, then registering the complainant's account, then the class of offences and even the recording of arrest. Each one

[7] Saikia N, 'Predictive Policing and the Future of Law Enforcement' (*The Dialogue*, 20 September 2023) <https://thedialogue.co/predictive-policing-and-the-future-of-law-enforcement/\> accessed 19 February 2026
[8] Drishti IAS, *'Crime in India 2023 Report'* https://www.drishtiias.com/daily-news-analysis/crime-in-india-2023-report accessed 20 February 2026

of these steps is open to the biases, discretionary decisions and corruption that have been a hallmark of Indian policing for so long. An ethnographic study of Delhi Police's CMAPS by Marda and Narayan (2020) found that the representational, historical, and measurement biases in data collection practices of Delhi Police's get transferred directly toCMAPS predictive model.[9]

The inequality of digital infrastructure is also a major challenge. Police stations in rural and semi-urban areas often do not have the hardware and internet connectivity and the trained personnel needed for proper data entry. As of 2023 India has 236 State based training centres, covering around 2.2 million police personnel equivalent to one training centre per almost 9,300 officers. This ratio is not sufficient for imparting the specialised skills required for AI-driven data collection and interpretation. The risk, therefore, is that predictive policing will effectively be reserved for a handful of technologically advanced urban police departments, and that this will create a disjunct and inequitable system.

IV. ALGORITHMIC BIAS AND DISCRIMINATORY OUTCOMES

The issue of algorithmic bias involving predictive policing has received ongoing interest from legal academics and technologists worldwide, and it becomes acute in the Indian context because of the complex social stratification of Indian society. Predictive policing algorithms identify patterns in historical crime data; but if that historical data reflects discriminatory policing practices of: too much surveillance of Muslim, Dalit and Adivasi communities; selective policing in poor urban neighbourhoods; or persistent under-reporting of crimes in rich neighbourhoods then the algorithm will perpetuate and enthrench these discriminatory patterns.[10]

Research into Delhi's CMAPS specifically shows that places with higher concentration of caste and religious minorities are disproportionately flagged as areas with high crime, not necessarily due to a higher rate of crime in those areas, but because of the historical over-policing in those areas.[11] This creates what researchers call a "discriminatory feedback loop": the more a

[9] Marda S and Narayan S, 'Data in New Delhi's Predictive Policing System' Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM, 2020) <https://dl.acm.org/doi/abs/10.1145/3351095.3372865\> accessed 20 February 2026

[10] Bhandari V, 'Building the Case for Restricted Use of Predictive Policing Tools in India' (2022) 19 International Review of Information Ethics <https://informationethics.ca/index.php/irie/article/view/487\> accessed 20 February 2026

[11] Singh T, 'Predictive Policing in India: Deterring Crime or Discriminating Minorities?' (LSE Human Rights Blog, 16 April 2021) <https://blogs.lse.ac.uk/humanrights/2021/04/16/predictive-policing-in-india-deterring-crime-or-discriminating-minorities/\> accessed 20 February 2026

particular group is policed, the more crime data is generated about them; the more crime data is generated about them, the higher their algorithmic risk score; the higher their risk score, the more policing they attract and so the cycle perpetuates itself.[12]

This phenomenon is not specific to India. In the United States, the recidivism predictive algorithm, or COMPAS, turned out to be twice as likely to falsely identify a future defendant as black than white, as ProPublica revealed. According to a study by the UK government, police officers sent to hotspots identified by data analytics were more likely to make an arrest based on bias than on probable cause. However, the stakes are arguably higher in India considering that in contrast to more legally advanced jurisdictions, India has no dedicated AI legislation, binding standards of algorithmic accountability, or systems of judicial review of automated law enforcement decisions.

The "black box" nature of a number of commercial predictive policing tools compounds the problem. When algorithms are treated as proprietary trade secrets as frequently is the case with privately developed systems neither law enforcement agencies nor affected citizens would be able to scrutinise the assumptions, weightings or training data embedded in the model.[13] In a country like India, where goonda registers and police registers have been used for history to harass and collect information on notoriously marginalised communities through special laws like the National Security Act 1980 or the Maharashtra Control of Organised Crime Act 1999, the black-boxing of algorithmic decision making is especially troubling.

The Internet Freedom Foundation's Panoptic Tracker, tracking the use of facial recognition technology (FRT), had identified at least 168 FRT systems across the country including at least 43 that were being used for security and surveillance. An audit of commercial FRT systems in India revealed that they are biased against minority groups and have produced results that are a cause for grave concern about fairness and political abuse. Given that FRT is recently being incorporated in conjunction with predictive policing platforms, this structural bias in recognition systems replicates into the wider predictive analytics ecosystem.

V. CONSTITUTIONAL AND HUMAN RIGHTS IMPLICATIONS

[12] Barocas S and Selbst AD, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.
[13] OxJournal, 'Predictive Policing or Predictive Prejudice? A Study of the Legal, Historical and Ethical Implications of AI in Policing' <https://www.oxjournal.org/predictive-policing-or-predictive-prejudice/\> accessed 21 February 2026

The constitutional validity of predictive policing in India must be possessed between the framework of fundamental rights which are secured by Part III of the Constitution of India, in particular articles 14 (right to equality), 19 (freedom of expression and movement), and 21 (right to life and personal liberty). The pious judgement of the supreme court of India in the landmark nine-judge bench in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, held that privacy is a fundamental right under Article 21. f it is found that a particular law resorts to state interference with privacy, the court determines whether the interference is held to be proportionate and legitimately achieved.[14]

The Puttaswamy proportionality test requires that any action by the state which violates privacy has to meet four cumulative criteria: (i) it has to be sanctioned by law; (ii) it has to be necessary in a democratic society; (iii) it has to be proportionate to the object sought to be achieved; and (iv) there have to be procedural guarantees against abuse. Current implementations of predictive policing in India do not meet these requirements. There is no legislation expressly authorising predictive policing, no definition of the categories of data which might be collected and no independent oversight. The use of CMAPS data to create suspect profiles and make preventive detentions, without this type of legal grounding, is vulnerable to a constitutional challenge.

Article 14's guarantee of equality before the law and equal protection of laws are also at stake. Policies that are neutral on its face but discriminatory as applied, what US constitutional law calls "disparate impact", violate anti-discrimination principles. As the High Court in Delhi held in the case of Madhu vs Northern Railways - 247 (2018) DLT 198 that policies which are facially neutral but have a disproportionate discriminatory effect against identifiable groups are constitutionally suspect.[15] Predictive policing algorithms which systematically over-police communities on the basis of their caste or religious identity even if not explicitly designed to do so, may well be violations of Article 14.

The right to movement is also under Article 19(1)(d) in the cases where the predictive systems intrude upon the persons by generating individual risk scores or labelling them as potential offenders, which can, as a result, have them subjected to the practices of stop and frisk, preventive detention under Section 107 or 151 of the Code of Criminal Procedure (now the Bharatiya Nagarik Suraksha Sanhita 2023), or entry into watch lists. The lack of an explanation

[14] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1
[15] *Maneka Gandhi v Union of India* (1978) 1 SCC 248; Constitution of India, arts 14, 19, 21

or contestation of algorithmic decisions right that exists on the basis of the European Union's General Data Protection Regulation (GDPR) means that individuals in India do not, as of this writing, have an effective legal mechanism to challenge erroneous algorithmic classifications.

The constitutional challenge obviously becomes all the more complicated given the Right to Information Act 2005 which includes very broad exemptions for law enforcement agencies. A study on Delhi police's CMAPS revealed that it is almost impossible to get details on the functioning of the system, data sources, or outputs of the tool by applying RTIs, in effect plugging the tool out of public accountability.[16]

VI. INADEQUACY OF THE LEGAL AND REGULATORY FRAMEWORK

India's current legal architecture for governing predictive policing is fragmented, reactive, and inadequate. The principal legislative instruments in this space are the Information Technology Act 2000, the Digital Personal Data Protection Act 2023 (DPDPA), and the constitutional provisions discussed above.[17]

The DPDPA, enacted by Parliament in August 2023 and operationalised through the Digital Personal Data Protection Rules 2025 (notified on 13 November 2025), represents India's first comprehensive data protection legislation. It establishes rights for data principals including rights to access, correction, erasure, and grievance redressal, and imposes obligations on data fiduciaries in relation to consent, data minimisation, and security safeguards.[18] However, crucially, Section 17(1)(b) of the DPDPA exempts the processing of personal data for the purpose of "prevention, detection, investigation, or prosecution of any offence or contravention of any law" from the Act's core data principal rights and data fiduciary obligations.[19]

This broad law enforcement exemption effectively places predictive policing systems outside the ambit of the DPDPA's most protective provisions. Critics have noted that the Act lacks requirements for algorithmic accountability, any legal basis for challenging automated law

[16] Marda S and Narayan S, 'Data in New Delhi's Predictive Policing System' Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM, 2020) <https://dl.acm.org/doi/abs/10.1145/3351095.3372865\> accessed 20 February 2026
[17] Information Technology Act 2000 (India); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (India)
[18] Hogan Lovells, 'India's Digital Personal Data Protection Act 2023 Brought into Force' (2025) <https://www.hoganlovells.com/en/publications/indias-digital-personal-data-protection-act-2023-brought-into-force-\> accessed 20 February 2026
[19] Digital Personal Data Protection Act 2023 (India), s 17(1)(b)

enforcement decisions, or liability standards for AI-driven bias.[20] Unlike the EU's GDPR, which includes a right not to be subject to solely automated decisions with legal or similarly significant effects (Article 22), or the proposed EU AI Act, which classifies real-time remote biometric identification and predictive policing as high-risk AI systems requiring conformity assessment, India has no analogous legal framework.

Table 3: Comparative Legal Framework India vs. EU

Legal Issue	India (DPDPA 2023)	EU (GDPR / AI Act)
Law enforcement exemption	Broad s 17(1)(b) exempts prevention, detection, investigation	Limited must be proportionate and lawful under LE Directive
Right to explanation of automated decisions	Absent	Article 22 GDPR right not to be subject to solely automated decisions
Algorithmic accountability standards	None	EU AI Act classifies predictive policing as high-risk AI
Consent in law enforcement context	Not required	Not applicable but procedural safeguards apply
Data Protection Authority oversight of police AI	No explicit mandate	Supervisory authorities oversee law enforcement processing
Penalties for AI bias / misuse	None AI-specific	GDPR fines up to €20M / 4% global turnover

Source: Compiled by author from DPDPA 2023; EU GDPR Regulation (EU) 2016/679; EU AI Act Regulation (EU) 2024/1689.

Beyond the DPDPA, the Police Acts governing state police forces most of which are modelled on the colonial Police Act of 1861 contain no provisions specifically addressing the use of AI or predictive analytics in law enforcement.[21] The absence of a dedicated statute regulating the collection, storage, processing, and use of crime data in predictive systems means that police agencies are currently deploying significant surveillance and prediction capabilities without

[20] Cyberlawconsulting, 'AI and Data Privacy in India: Emerging Legal and Ethical Challenges' <https://www.cyberlawconsulting.com/ai_and_data_privacy_in_india.php\> accessed 20 February 2026

[21] Ministry of Home Affairs, Government of India, *'Digital Transformation of Justice: Integrating AI in India's Judiciary and Law Enforcement'* (Press Information Bureau, 2024) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2106239 accessed 20 February 2026

any legislative authorisation or independent judicial oversight, a situation that is constitutionally questionable in light of the Puttaswamy judgment.[22]

VII. INSTITUTIONAL ACCOUNTABILITY, TRANSPARENCY, AND CAPACITY DEFICITS

Even where predictive policing systems are technically functional and legally grounded, their efficacy and legitimacy depend critically on the institutional culture, accountability mechanisms, and human capacity of the deploying organisation. On all three dimensions, Indian policing presents significant challenges.[3]

Police accountability in India is structurally weak. Despite the Supreme Court's landmark directions in Prakash Singh v. Union of India[23] mandating the establishment of Police Complaints Authorities and State Security Commissions, implementation has been patchy and, in many states, superficial. Internal accountability mechanisms often don't work and officers rarely face consequences for misconduct or arbitrary exercise of power. When law enforcement agencies use predictive tools that produce potentially life-changing results like preventive detention recommendations, suspect lists, and surveillance targeting without any civilian oversight, the likelihood of abuse is high.

Transparency is an associated and equally pressing issue. Predictive policing systems in India work without any publicly available documentation of their methodologies, training data, error rates or impact assessments. The proposal for the application of the technology for Network Access For Forensic Recorder of Sexuality (NAFS) presented by the Ministry of Home Affairs, for instance, failed to address any issues related to the ethical, legal and privacy implications of this technology.[24] The combination of RTI exemptions for law enforcement, and algorithmic systems being proprietary systems deployed by private vendors, leaves law enforcement with little to no transparency around some of the most important policing decisions.

Human capacity is also a third key challenge. As was mentioned above, the ratio of training infrastructure against the police personnel in India is deeply lacking. Training programmes for police officers do not even include modules on algorithmic systems, AI ethics, or data literacy.

[22] FICCI and EY, 'Predictive Policing and Way Forward' (FICCI-EY Report, 2018) <https://ficci.in/spdocument/23009/FICCI_EY_Predictive_Policing_.pdf\> accessed 20 February 2026
[23] (2006) 8 SCC 1
[24] Oxford BSG (Blavatnik School of Government), 'India: Increasing Use of AI Across the Justice System" (Oxford Institute of Technology and Justice) <https://www.techandjustice.bsg.ox.ac.uk/research/india\> accessed 19 February 2026

Without officers who are aware of the probabilistic and contextual limitations of predictive outputs and who are trained to use the results of algorithms as sources of information instead of substitutes for human judgment logically employing black-box algorithms the potential for mechanical over-reliance on algorithmic outputs is significant. The NCRB National Workshop on Crime Data Analytics directly acknowledged the fact that even though the deployment of analytics tools such as PredPol was said to have led to a 25 per cent reduction in crime in Los Angeles, its deployment requires institutional investment in data analysis ecosystems in police forces across states.[25]

The issue of vendor dependency should be given particular attention. Where predictive policing tools are acquired from private technology companies domestic or foreign law enforcement agencies may not have the technical expertise to audit the contracts, modify them or terminate them. This introduces a dependence of structures, which can harm both operational sovereignty and accountability. The experience of the United States where several cities including: Santa Cruz, California and Portland, Oregon banned predictive policing tools after it was found that commercial vendors were unable to ensure non-discriminatory outcomes should serve as cautionary tale for India.[26]

VIII. RECOMMENDATIONS TOWARDS A RIGHTS-RESPECTING FRAMEWORK

The challenges documented in this paper are serious, but not insurmountable. A rights-respecting approach to predictive policing in India would need to address the infrastructures, law, accountability and capacity in an integrated way. The following recommendations are made as a basis for consideration in the development of policy.

First, India is in need of a proper statutory framework in the sphere of AI assisted policing which goes beyond the exemptions in the law enforcement under the DPDPA. Such legislation should specify the permissible purposes for which predictive policing tools may be used, require data minimisation and purpose limitation, require independent algorithmic audits of such tools prior to deployment and at regular intervals thereafter, and provide a right for those

[25] Bureau of Police Research and Development, *'Data Analytics, Artificial Intelligence, Machine Learning, Dashboarding' NCRB National Workshop on Crime Data Analytics* (Press Information Bureau, 2017) https://pib.gov.in/newsite/PrintRelease.aspx?relid=161769 accessed 18 February 2026

[26] ShodhSamajik, 'Algorithmic Policing and Due Process in Cybercrime Investigations: A Constitutional Analysis Under Articles 14, 19 and 21 of the Indian Constitution' (2025) <https://shodhsamajik.com/shodhsamajik/article/view/57\> accessed 20 February 2026

affected to bring reasons for and even challenge algorithmic profiling decisions. The model of the EU AI Act for high-risk AI is a useful precedent for deploying predictive policing from a conformity assessment standpoint.

Second, the infrastructure of the CCTNS data needs to be enhanced through better data quality, not data digitisation. This means standardised data entry protocols, mandatory FIR registration processes that are monitored for compliance and bias audits of historical crime data before it is used as training data for predictive models. Third-party algorithmic audits should be institutionalised as a condition for the deployment of any system of predictive policing.[27]

Third, civilian oversight bodies with some real independence and teeth need to be established to monitor and evaluate predictive policing deployments. The mandates of Police Complaints Authorities should be increased to include AI-assisted decision-making. A standing parliamentary committee in relation to AI in law enforcement would provide accountability for legislation.

Fourth, the Indian government should prepare national AI ethics guidelines for the law enforcement that are co-designed with civil society organisations, affected communities and independent researchers. The Smart Prahari model which is open-source, transparent, auditable and privacy by default is proof of concept that effective predictive policing doesn't need to be opaque or marginalised communities left out of the design process.

Fifth, police training curriculum at both the basic level and in-service Career Cruising Courses must be re-created to include substantive wraps regarding AI ethics, information data literacy, algorithmic limitations and constitutional rights. Officers need to be able to interrogate the output of algorithms, not blindly accept it.

IX. WAY FORWARD

Predictive policing in India is at a critical juncture. The technological infrastructure, national data systems and political will to implement these tools at scale is now more available. However, the legal framework and architecture of accountability, along with the institutional culture needed to guarantee that predictive policing is used to support and not limit justice, is critically underdeveloped. The implementation challenges documented in this paper data quality failures, algorithmic bias, constitutional rights deficits, regulatory inadequacy, and

[27] GK Today, 'Crime and Criminal Tracking Network and Systems (CCTNS)' (6 November 2025) <https://www.gktoday.in/crime-and-criminal-tracking-network-and-systems-cctns/\> accessed 19 February 2026

institutional transparency gaps are not peripherals but structure rather than obstruction on the path that India has taken. The history of technology-driven policing, both in India and globally, gives us ample evidence that the use of powerful tools of surveillance and prediction in the absence of sufficient legal constraints and institutional safeguards tends to produce more rather than neutralised injustices. For a country as diverse and unequal as India, these kinds of discriminatory feedback loops that are possible through predictive policing are particularly perilous for communities that are already disproportionally subject to state coercion. The constitutional guarantee of equality, fundamental right to privacy and the Rule of Law require us to adopt a more cautious, slower and rights-centred approach. This is not an argument against predictive policing per se. When used in a transparent way, and with high data quality and representation, strong mitigation of bias, meaningful oversight, and accountability in practice, data-driven tools can improve the efficiency and effectiveness of police work in ways that benefit the people of all citizens. But, the preconditions for such a deployment do not exist in India as yet. So building them has to be the priority.