



THE ALGORITHMIC GAZE: AI, PREDICTIVE POLICING AND CONSTITUTIONAL CHALLENGES IN THE DIGITAL AGE

Nitya Katiyar* Sudipti Mukhopadhyay*

ABSTRACT

“When we think that the police machinery and judges are becoming smart, the criminals are getting smarter.”

Bombay High Court Judge, Justice Bharati Dangre, asserted the above statement in a workshop arranged by the Goa State Legal Service Association and Goa High Court Bar Association in September, 2025. This captures the basic essence of why we need to introduce technology within the police system. In order to be ahead of the criminals, we need predictive policing powered by technology to prevent crime. However, using technology for policing without any human oversight can raise serious concerns, such as the possibility that accuracy may not be achieved and that the wrong person might be apprehended. Therefore, using technology for policing might make the work of police personnel swifter than before, but at the same time, it can also be a threat to the basic rights of citizens. This paper shall attempt to address the basic concepts of predictive policing using technology. Also trying to understand the algorithmic bias that comes along with it. The paper reviews the literature of other countries trying to grasp the condition of predictive policing using technology in those countries, as it is not that prevalent in India yet, except in a few States such as Telangana and Uttar Pradesh. This paper shall also outline the various legal concerns that may arise for the technological deployment in predictive policing. The paper concludes with several suggestions, aspects that could be adopted by authorities to reduce concerns about predictive policing using technology.

*BA LLB, FIRST YEAR, NATIONAL LAW UNIVERSITY, MEGHALAYA.

*LLM, FIRST YEAR, NATIONAL LAW UNIVERSITY, MEGHALAYA.

Keywords: Artificial Intelligence (AI), Algorithm, Bias, Predictive Policing, And Surveillance.

INTRODUCTION

The transition from traditional reactive policing to a model of proactive, intelligence-led enforcement is increasingly defined by the integration of artificial intelligence (AI) and 'big data'. The article analyses a critical scenario involving a metropolitan city's 'Smart Safety Initiative,' a digital policing platform designed to enhance public safety through the automated analysis of vast data streams. This system integrates high-density surveillance tools – including CCTV facial recognition, automated license plate recognition (ALPR), and social media monitoring – with historical crime records and socio-economic indicators to generate predictive 'hotspots' and individual risk scores.

The primary aim of this research is to investigate the profound tension between technological efficiency and the protection of democratic rights within this digital landscape. While government authorities justify the initiative as a means of optimising resource allocation and 'surgically' preventing crime, the reality on the ground has revealed significant social and legal crises. Journalists and civil society groups have identified that the system's reliance on historical data creates self-perpetuating feedback loops, where neighbourhoods that have been historically over-policed are repeatedly flagged as 'high risk,' thereby justifying further surveillance and patrols.

What motivates this analysis is the critical lack of operational transparency and the regulatory vacuum surrounding the initiative. The 'black-box' nature of the underlying algorithms makes it nearly impossible for citizens to challenge risk assessments or for regulators to identify algorithmic bias. Furthermore, the case demonstrates a 'chilling effect' on free speech, as activists and journalists report a fear of being tracked through their 'digital footprints' for criticising government policies.

By examining the 'Smart Safety Initiative,' this article seeks to move beyond the technical promise of AI to understand its socio-technical impacts. The goal is to evaluate whether data-driven policing acts as a rationalising force for safety or as a force multiplier for entrenched structural inequality, ultimately proposing a framework for algorithmic justice that prioritises democratic accountability and community oversight.

KEY CONCEPTS

Digital Surveillance: This Concept refers to the continuous monitoring, collection, and analysis of individuals' digital activities, movements, communications, and behaviours through technological systems.

In this case, the government uses:

- CCTV cameras with facial recognition
- Automated license plate recognition
- Social Media Monitoring
- Mobility and location tracking
- Crime databases

With The Surveillance, the State can track where people go, whom they meet, what they post online and whether they attend protests. It may violate the right to privacy, autonomy of individuals and democratic freedom.

Algorithmic Bias: This occurs when AI systems produce unfair or discriminatory outcomes because the data used to train them reflects existing social inequalities or prejudices. It uses the past crime records, arrest databases and socioeconomic indicators. The AI appears 'neutral,' but it actually reproduces historical prejudice against:

- Poorer communities,
- Minority groups,
- and marginalised populations.

Thus, technology can reinforce structural inequality instead of reducing it.

Inequality in Policing: It means that certain social groups or neighbourhoods are policed more aggressively than others, often because of class, caste, race, religion, or economic conditions. The system uses neighbourhood socio-economic indicators to predict crime hotspots. Poor or marginalised areas become targets for increased patrols, surveillance and monitoring. Whereas, Wealthier areas may receive less scrutiny. Also, it creates unequal and discriminatory law enforcement where technology amplifies existing inequalities instead of ensuring equal protection under the law.

Social Exclusion Through Technology: This occurs when technological systems marginalise or stigmatise certain groups in society as high risk, due to which the communities may experience reduced freedom of movement, constant surveillance and suspicion from authorities. It can create a form of digital discrimination, where marginalised groups become excluded from equal participation in public life.

Predictive Policing: Predictive policing refers to the application of data analytics, artificial intelligence, and machine learning techniques to anticipate potential criminal activities before they occur. By leveraging historical crime data, demographic information, and real-time inputs, predictive policing aims to identify crime hotspots, allocate police resources efficiently, and ultimately prevent crime. It raises serious issues like predictions may be inaccurate, innocent people may be treated as suspects and historical biases become embedded in policing decisions.

Chilling Effect on Free Speech: A chilling effect occurs when people avoid expressing opinions or participating in lawful activities because they fear surveillance, punishment, or retaliation. The government monitors social media activity, public protests, and online criticism of government policies. As activists and journalists become aware of this monitoring, they begin to fear: being tracked, profiled or targeted by authorities. As a result, people may avoid criticising the government, stop attending protests, or censor their online speech.

LITERATURE REVIEW

Berk (2021): The Statistical Side of Prediction –

According to Richard Berk, artificial intelligence is simply computer code for specific empirical tasks, not an enigmatic process known as ‘human-like’ thinking. For example, he defines ‘models’ as theories about causality, whereas ‘algorithms’ are just methods for accurately predicting. Therefore, Berk concludes that accuracy, fairness, and transparency exist in a perpetual state of trade-off; you cannot optimise all three simultaneously.

Findings: He notes that there are usually cases of bias due to flawed data gathering practices, for instance, due to animosity toward a certain race during data gathering.

Relevance to Case Study: Algorithms are being used by the city's administration for predicting crimes, but presented as truths. Berk's work shows that the city's emphasis on accurately predicting comes at the expense of both fairness and transparency; hence, the ‘high-risk’ areas are being flagged, as there has been no change in behaviour within them.

Brayne (2017): Big Data Surveillance and the LAPD Shifts in Surveillance as Described by Sarah Brayne in Her Qualitative Study on the LAPD –

It includes a lower threshold for inclusion, whereby those who lack any interaction with the police are included in databases through secondary surveillance networks. One can thus be labelled a subject of surveillance without committing any crime since he/she is either the sibling or colleague of a person of interest.

Findings: According to her, stratified surveillance is enabled by big data, where people are subjected to surveillance differently depending on their risk ratings.

Application of Shift to Our Case Study: This enables one to understand why the city of Detroit has integrated social media and movement patterns of citizens into surveillance operations. Indeed, the function creep makes surveillance possible even at the personal level, as witnessed among activists and journalists who have digital footprints but are not known to have committed any offence.

Haley & Burrell (2025): Ethical Challenges and Organisational Culture –

Haley and Burrell argue that technological solutions cannot rectify cultural pathologies within police institutions. They define a ‘culture of impunity’ where misconduct is tolerated, and note that deploying AI in such an environment merely operationalises and systematises injustice under a veneer of objectivity.¹

Findings: They conclude that meaningful reform requires a normative shift that prioritises democratic accountability and community oversight over technical innovation.

Relation to Case Study: The city’s ‘Smart Safety Initiative’ is being deployed without community oversight or clear regulation. Haley and Burrell’s findings suggest that the city’s system will likely become a ‘force multiplier’ for entrenched bias because it is not embedded in an ethical organisational culture that interrogates its own historical data.

Hung & Yen (2023): Algorithmic Fairness and the Social Safety Net –

This paper analyses Chicago’s Strategic Subject List (SSL) and finds that discrimination is primarily caused by biased police actions (arrest patterns) rather than the code itself. They

¹ Patricia Haley and Darrell Norman Burrell, ‘Integrating Artificial Intelligence into Law Enforcement: Socioeconomic and Ethical Challenges’ (2025) 9(2) SocioEconomic Challenges 60
<<https://armgpublishing.com/journals/sec/volume-9-issue-2/article-4/>> accessed 09 May 2026

explain that fairness is a context-sensitive social construct that must be negotiated through democratic processes rather than discovered in a laboratory.²

Findings: They propose a ‘social safety net’ framework, where AI is used to identify vulnerable individuals for assistance (jobs, health services) rather than just for arrests.

Relation to Case Study: The city’s ‘feedback loop’, where over-policed areas are repeatedly flagged, mirrors the findings in Chicago. Hung and Yen’s work suggests the city should stop using risk scores for ‘increased patrols’ and instead use them to allocate social resources to those at risk, thereby breaking the cycle of criminalisation.

Talukder & Shompa (2024): Systematic Review of AI in Criminal Justice –

In their review of 37 articles, Talukder and Shompa find that while AI improves efficiency, its ‘black-box’ nature complicates public trust. They identify significant gaps in legal frameworks, concluding that the lack of standardised policies across jurisdictions leads to inconsistent and potentially unjust outcomes.

Findings: They emphasise that interdisciplinary collaboration and transparent practices are essential to balance technological advancement with equity.

Relation to Case Study: The city’s journalists and activists report a lack of transparency and an inability to challenge the algorithm. This confirms Talukder and Shompa’s findings that opacity is a barrier to accountability and that the city’s initiative is suffering from a lack of a comprehensive regulatory framework to protect civil rights.³

COMPARATIVE SYNTHESIS AND CASE APPLICATION

The literature demonstrates a clear consensus: the ‘Algorithmic Gaze’ is not a neutral tool. While it offers operational efficiency, it frequently reifies historical bias. All five sources agree that algorithms inherit the bias of their training data, meaning the city’s reliance on ‘arrest databases’ ensures that past discriminatory policing will dictate future surveillance targets.

There is, however, a divergence in focus and proposed solutions:

² Tzu-Wei Hung and Chun-Ping Yen, ‘Predictive policing and algorithmic fairness’ (2023) 201 *Synthese* 206

³ Khairul Alam Talukder and Touhida Ferdousi Shompa, ‘Artificial Intelligence in Criminal Justice Management: A Systematic Literature Review’ (2024) 1(1) *Journal of Machine Learning, Data Engineering and Data Science* 63

Sources of Bias: Berk, Hung & Yen emphasise that bias is external to the algorithm, located in police actions and data management. Conversely, Haley & Burrell focus on internal organisational culture as the primary driver of technological abuse.

Scope of Surveillance: Brayne and Talukder highlight the breadth and depth of new surveillance. Brayne's 'secondary surveillance' concept directly explains why the city's activists report a fear of being tracked even if they are law-abiding.

Governance: Talukder and Haley & Burrell call for legal and regulatory standards, while Hung & Yen suggest a radical shift toward a social welfare model of AI deployment.

In conclusion, the city's Smart Safety Initiative stands at a crossroads. The literature confirms that without algorithmic transparency, independent audits, and community participation, the system will likely continue to produce the chilling effects and social exclusions identified by the city's civil society groups. This case confirms that in the digital age, policing is no longer just about the street; it is about the data, and the data is a social product that carries the weight of history.

STRUCTURAL INEQUALITY IN AI-BASED PREDICTIVE POLICING

Algorithms used in the criminal justice system, from the initial perception of surveillance-based policing onward, must be carefully trained because they might curtail freedom and liberty if the data is biased. In a USA-based journal – *Annual Review of Criminology*, Richard A. Berk observed that if the data is not collected properly, such as recording an accused's age based on his words rather than verifying it from the driver's licence, it may lead to wrong carry-forwarding of data in the algorithm. Therefore, proper recording of data is the first necessity to prevent the exemplification of inequality in society. Various countries have been using AI in their immigration system, and there has been a concern of excluding or red-flagging the South Africans or Indians without any proper grounds for improper documentation, but just based on their nationality.⁴ Similarly, if any region-specific bias is inculcated within the predictive policing technologies, it would eventually hamper the rights of individuals. Even in the paper of Hung and Yen, as referred to above, it was stated that the algorithm in predictive policing

⁴ Petra Molnar and Lex Gill, "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System" (*International Human Rights Program and Citizen Lab*, 2018) <<https://ihrp.law.utoronto.ca/sites/default/files/media/IHRP-Automated-Systems-Report-Web.pdf>> accessed 16 May 2026

generally uses arrest databases rather than actual conviction records. This leaves room for bias that could be inculcated within the system.

Another problem that arises in predictive policing is that it can provide surveillance in public places and not in private spheres or in mass private property, such as shopping malls. So, the crime data fed into the system is systematically incomplete. Furthermore, the data may be insufficient in areas where people do not trust the police and therefore do not report crimes. Therefore, if such data is relied on, it can lead to confirmation bias and the misallocation of resources, as Sarah Brayne also points out in her paper. It is called a self-perpetuating feedback loop. This can even lead to further restrictions on movement in a particular area due to increased police deployment there. Everyone in that area will be posed with greater suspicion. This ultimately hampers the liberty of certain individuals without any wrongdoing on their part in the first place.

For the above practices, a data-driven technology can unintentionally create a self-perpetuating feedback loop that targets marginalised communities. This is because the rate of recidivism might be aligned with the socio-economic factor or any other factor; therefore, as the base factor is not the same, it is practically not possible to imbibe the virtue of fairness, in its varied definition as seen in Berk's paper, within the system. Even while creating the algorithm, even if it is not self-biased, the AI may detect a pattern of family income, ZIP code and other factors which ultimately may strongly correlate with a particular race or group, thereby ultimately swaying bias towards that community.

CONSTITUTIONAL AND LEGAL CHALLENGES IN AI-BASED

Data-driven policing mainly focuses on individuals and their locations rather than looking behind at the social determinants of safety. This surveillance over each individual poses a threat to the Constitutionally guaranteed rights and freedoms. As discussed above, predictive policing usually leads to the deployment of a larger number of police personnel in a specific area, which leads to restriction of movements. This is a curtailment of liberty guaranteed under *Article 21 in the Indian Constitution*. Besides that, it also violates *the right to privacy*, as every movement of such an individual is under supervision. Further, *the right to privacy* is under threat from function creep, where digital data collected for a specific purpose may be used for another, in this case, policing. Brayne, in her work, states that the police routinely purchase such privately collected data, exploiting the third-party doctrine and also bypassing the need for a warrant. Especially with Aadhar, in the Indian context, which is one of the largest repositories of

personal information, including biometrics, by the government, the context of function creep becomes relevant, to speculate whether such data is used for policing. Further deploying technologies such as Automatic License Plate Readers (ALPRs) allows police to track the daily activities of an individual. Also, Facial Recognition Technologies (FRTs) deployed for policing raise privacy concerns because individuals are not even informed in the first place, so they do not even have the option to opt out. Both ALPRs and FRTs raise accuracy concerns as well.

The right to privacy was adopted by the Indian Courts through *K.S. Puttaswamy v. Union of India*⁵. It was observed that the right to privacy is an inalienable natural right imbued within every individual. Not only that, but it is also the essence of dignity and was read within the ambit of *Article 21 of the Indian Constitution*. It was also observed that the right must be recognised to validate other freedoms guaranteed under the Indian Constitution, as it's the core of every other freedom.

In regard to *freedom of expression*, as the literature above supported, there is a chilling effect because a political dissent would label him as a 'high-risk' individual, which can even lead to social stigma. Therefore, people restrict themselves when there is constant supervision by the State. Further, as discussed in the previous section, the data that is fed into the algorithm often results in systematic inequalities and further amplifies them through the feedback loop. This results in a violation of *Article 14 of the Constitution*, which guarantees Equality before the law.

In addition to these issues, the *due process* of the whole system of predictive policing cannot be assessed, as the algorithms are usually shielded against proprietary secrecy, making the AI system a black box model where the reasoning of a conclusion cannot be adjudged. This predictive policing can be problematic if adopted in the Indian system because in India, we do not strictly follow the due process, but the 'procedure established by law' under Article 21. Therefore, an individual's liberty can be curtailed if the law backs it up with proper procedure, but the procedure needs to be fair, just and reasonable, as highlighted in *Maneka Gandhi v. Union of India*⁶.

In India, we have the Digital Personal Data Protection (DPDP) Act, 2023, which stresses that the data collected from an individual must follow an *informed consent* protocol, which is

⁵ K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

⁶ Maneka Gandhi v. Union of India MANU/SC/0133/1978.

lacking in the aspect of predictive policing, especially in the aspect of ALPRs and CCTVs, where AI is imbued.

Therefore, if predictive policing aims to prevent crime rather than increase surveillance of people, it must understand the root causes of crime. It demands that the budgetary allocation is not towards surveillance or deploying policemen, but allocating such finances to preventative social infrastructure, such as mental health services, housing and food security.

POLICY FRAMEWORK FOR FAIR USE OF TECHNOLOGY IN POLICING

To ensure appropriate use of technology for crime prevention, the following steps can be adopted:

Supportive Interventions: Technology must be used to address the root cause. That is, technology should be used to identify communities and individuals in need of support from the Government, as a lack of support can bring them to the brink of committing criminal activities. The support could be in the form of counselling or other mental health services, it could be in the form of capacity building, such as education or vocational training, which will prepare them for the job market, or it could be in the form of subsidies, thereby helping them to cope with a temporary, economically threatening condition.

Mandating Warrants: In case predictive policing is used to take information from third parties, warrants must still be a requirement. Also, such an information centre shall send a message to all its users or customers informing them that this has been done.

Timely Audits: If AI in predictive policing is deployed, there should be mandatory timely audits on a quarterly basis in order to detect whether there has been bias within the system. This should account for the data fed into the system, as well as other data that has been segregated by the algorithm itself to group certain people and create bias.

Data Management: The data to be used for policing is the data in store with the National Crime Records Bureau (NCRB); their role in providing accurate data and maintaining proper records is essential. There must be transparency in regard to the data fed into the algorithm and the functioning of the algorithm, and the same must be checked quarterly through audits.

Therefore, even if technology is a boon and helps policing in certain aspects, on the other hand, it can also raise serious violations of individuals' rights. Hence, a few aspects have been suggested above for the proper deployment of technology.