

POLICING BEFORE THE CRIME - ALGORITHMIC BIAS, PRIVACY, OPACITY, AND CONSTITUTIONAL LIMITS IN INDIA

*Eshan Chauhan*¹

ABSTRACT

The growing integration of artificial intelligence into law enforcement has led to the emergence of predictive policing as a proactive tool for crime control. Predictive policing aims to prevent criminal activities by identifying potential offenders and forecasting crime-prone areas. While such technology promises efficiency, speed, and proactive crime control, significant concerns are raised on algorithmic bias, privacy and lack of transparency. The article analyses the shift from traditional to predictive policing, global trends, the existing framework governing privacy in our country, including the Digital Personal Data Protection Act, 2023 and the constitutional principles laid down in privacy jurisprudence. It examines how predictive policing currently operates in a "grey area", lacking a legal framework incapable of addressing the risks associated with algorithmic decision-making. Applying principles of legality, necessity and proportionality, the article contends that the present use of predictive technology goes against democratic principles. A comprehensive legal framework supported by transparency, non-discrimination, accountability and independent oversight is essential to prevent misuse of predictive policing systems and safeguard constitutional rights.

Keywords: Predictive Policing, Algorithmic Bias, Privacy, Transparency

I. INTRODUCTION

The nature of policing has undergone significant transformations in the 21st century. Traditionally, law enforcement agencies have operated as reactive institutions, responding to crimes after they occur. However, with the rapid advancement of technology, law enforcement agencies have begun to turn to predictive technologies not only to address crimes but also to predict them before they occur. Broadly speaking, "Predictive policing is the collection and analysis of data about previous crimes for identification and statistical prediction of individuals or geospatial areas with an increased chance of criminal activity to help develop policing intervention

¹ Eshan Chauhan, 3rd Year B.A.L.L.B (Hons), Symbiosis Law School Noida

and prevention tactics and strategies."² In India, the adoption of this technology has become increasingly visible through the deployment of facial recognition tools and crime-mapping systems. These developments are often justified on grounds of efficiency, speed, and the need for proactive crime control in our evolving digital society.

At the same time, this has led predictive policing to become one of the most debated developments in criminal jurisprudential discourse, as its benefits come with significant ethical and constitutional risks that may affect the functioning of law enforcement agencies. These systems rely on large-scale data collection and analysis through surveillance technologies, digital databases, and monitoring systems. Such practises risk subjecting individuals to continuous surveillance, without their consent. Consequently, the line between law enforcement and unwanted intrusion into one's private life becomes blurred. Beyond privacy, predictive systems are built upon data that contain social and institutional biases. When converted into algorithmic decision-making, such biases run the risk of reproducing discriminatory patterns that target vulnerable and marginalized communities. These problems are further aggravated by the problem of transparency and accountability within the criminal justice system. Unlike traditional policing, algorithmic systems function through opaque decision-making processes that are difficult to understand or challenge. The 'black box' nature of the systems makes it difficult to understand how conclusions were reached and who should be responsible when errors or discriminatory outcomes occur. Considering these concerns, it becomes necessary to examine whether the increasing integration of predictive technologies into law enforcement can be justified within the constitutional framework governing privacy, equality, and democratic accountability in India.

II. ANALYSIS

A. THE SHIFT FROM TRADITIONAL POLICING TO PREDICTIVE POLICING

Policing has undergone significant changes over time, originally seen as a reactive institution in which police officers acted only when a particular crime had occurred. Law enforcement agencies relied on a long process of criminal investigation encompassing multiple stages, including investigation, evidence collection,

² A. Meijer & M. Wessels, *Predictive Policing: Review of Benefits and Drawbacks*, 42 INT'L J. PUB. ADMIN. 1031, 1033 (2019).

interrogation, forensic analysis, suspect identification, trial, and testimony to determine criminal activity.³ While effective in the past, in contemporary times it has been criticized for incorrectly identifying the wrongdoer, being time-consuming, and being unaccountable to the people.⁴ The India Justice Report also notes that the police-to-population ratio is stalled at 155 per 10,000 people, short of the United Nations standard of 222,⁵ highlighting the shortage of manpower to effectively respond to crime. The rise of digital technologies, the expansion of digital infrastructure, and the availability of large datasets presented themselves as an easily available remedy to traditional policing. This digitalization laid the groundwork for the development of predictive policing, a model able to prevent crimes before their occurrence through the collection and analysis of large amounts of personal information such as crime records, geographic profiles, and temporal patterns.⁶ By following recurring trends, predictive systems can generate forecasts of when and where a crime will occur, enabling strategic planning and resource allocation.

Modern policing now relies on digital databases, surveillance systems, geographic information systems (GIS) and analytical software, which allows large amounts of data to be processed in real time.⁷ These technologies allow the police to move beyond conventional crime analysis and adopt a more proactive approach to crime prevention. It also attempts to solve the challenges faced by traditional policing, transforming the policing system to a preventive one rather than a reactive one. This transition also reflects a broader change in policing philosophy. Traditional policing focused more on response after the crime had taken place, but predictive policing focuses more on generating patterns to prevent crime from taking place. As a result, the latter relies more on data, with analytical tools playing a strategic role in guiding operational decisions.

Law enforcement in India has gradually begun incorporating predictive technologies as a response to the growing complexity of criminal activity. While not uniformly

³AMERICAN MILITARY UNIVERSITY, The Criminal Investigation Process: An In-Depth Overview, <https://www.amu.apus.edu/area-of-study/criminal-justice/resources/the-criminal-investigation-process/> (last visited March 19, 2026).

⁴ Arvind Verma, *The Indian Police: A Critical Evaluation* (Regency Publications, New Delhi, 1st edn., 2005).

⁵ Tata Trusts, India Justice Report: Ranking States on the Capacity of Police, Judiciary, Prisons and Legal Aid (2025).

⁶ Kang HW, Kang HB, *Prediction of Crime Occurrence from Multi-Modal Data Using Deep Learning*, 12 PLoS One 1, 19 (2017).

⁷ INTERNATIONAL INSTITUTE FOR COUNTER-TERRORISM (ICT), Era of Technological Transformation, <https://ict.org.il/era-of-technological-transformation/> (last visited March 25, 2026).

implemented across the country, most states have adopted predictive policing technologies to prevent crime. Delhi has implemented Crime Mapping, Analytics and Predictive System (CMAPS), a data-driven platform that examines crime on various factors such as frequency, region and crime type to get a better understanding of criminal tendencies. By generating insights into crime patterns and the behaviour of offenders, CMAPS supports predictive policing and informed decision-making, thereby enhancing crime control and public safety.⁸ Bangalore adopted an AI and predictive analysis model under its Safe City Project to reduce street crime. It functions by placing CCTV cameras at bus stops, railway stations and different junctions which are linked to a Facial Recognition System (FRS). This system cross-references live feeds against a centralised database of known offenders.⁹ Telangana Police also launched TSCOP, a mobile app that assists investigating officers in detecting faces of potential suspects and missing persons by cross-referencing them with the CCTNS database, maintained by the Ministry of Home Affairs, as well as other databases maintained by the State of Telangana. The app also allows officers to capture photos of offenders and screen them through the databases for identification during patrols.¹⁰

B. CONSTITUTIONAL AND REGULATORY FRAMEWORK GOVERNING PRIVACY IN INDIA

The fundamental right to privacy was firmly established in the case of *Justice K. S. Puttaswamy v. Union of India (2017)*¹¹, where a nine-judge bench held privacy as an integral part of our right to life and liberty under Article 21 of the Constitution. The Supreme Court considered privacy as essential for protecting our autonomy and emphasised that the state take a proactive role in ensuring safeguards for any such infringement. However, an important aspect of this judgment was that while privacy was considered a fundamental right, it was not held to be absolute and could be restricted by the state in certain situations. For this purpose, a three-pronged test

⁸ Comptroller and Auditor General of India, Report No 15 of 2020: Performance Audit of Manpower and Logistics Management in Delhi Police (Chapter 9: Digital Initiatives of Delhi Police) (2020).

⁹ NEWS18, AI Helps Bengaluru Police Reduce Robberies and Chain Snatching Drastically, <https://www.news18.com/cities/bengaluru-news/ai-helps-bengaluru-police-reduce-robberies-and-chain-snatching-drastically-skn-ws-l-9926980.html> (last visited March 27, 2026).

¹⁰ THE HINDU, Telangana Police Get a New App, TSCOP, <https://www.thehindu.com/news/cities/Hyderabad/telangana-police-get-a-new-app-tscop/article22347693.ece> (last visited April 4, 2026).

¹¹ *Justice K.S. Puttaswamy And Anr. vs Union Of India And Ors* 2017 (10) SCC 1.

was also introduced by Chandrachud J. to determine when state action could restrict our right to privacy. The three requirements were-

(i) Legality: The action by the state must be backed by a particular law.

(ii) Necessity: The action should seek to achieve a legitimate state aim such as national security, protection of revenue and deployment of natural resources.

(iii) Proportionality- There should be a rational nexus between the objective and the means adopted to achieve it.

Thus, any type of surveillance activity must be measured within these three requirements. The significance of this judgment is particularly relevant in the context of predictive policing. As this model relies on the collection, processing and analysis of data to prevent crime, important constitutional concerns are raised on whether these technologies comply with the requirements of legality, proportionality and necessity.

Although the court, through the Puttaswamy judgement, emphasised that the state takes measures to protect our privacy, only a limited framework exists for surveillance and data protection. The Information Technology Act 2000¹² provides limited protection through provisions like Section 43A, which states that compensation will be paid by bodies corporate if sensitive information is mishandled by them. Additionally, Section 72A provides punishment when personal information of an individual is leaked without their consent. However, data protection is not the primary aim of this law; it focuses on the regulation of transactions carried out by electronic means. Consequently, it only provides limited protection for personal data privacy associated with contemporary surveillance and predictive systems.

A more comprehensive framework was introduced with the Digital Personal Data Protection Act, 2023 (DPDP)¹³. It focuses on how personal data is collected, processed and stored while imposing obligations upon data fiduciaries to responsibly handle personal information. It attempts to strengthen informational privacy by mandating that data only be collected for specific and lawful purposes (Section 6), accompanied by a clear notice to data principals regarding the purpose of such a collection (Section 5). The act further recognises the rights of data principals to

¹² Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

¹³ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

process their personal data (Section 11), seek correction or erase inaccurate information (Section 12). To ensure compliance, this act also prescribes financial penalties for entities that do not comply (Section 33).

As part of its compliance framework, Section 10 of this act mandates Significant Data Fiduciaries (SDFs) to undertake periodic Data Protection Impact Assessments (DPIAs) as part of their compliance duties, which aim to minimise data risks. However, the requirement applies only to entities designated as SDFs by the Central Government. This centralises the determination of "high-risk" processing within the executive rather than through predefined statutory criteria.¹⁴ Its application to addressing the concerns of predictive policing also remains limited. The act is silent on the specific risks posed by automated decision-making, including profiling and predictive analytics, with there being no explanation for algorithmic bias, opacity and excessive surveillance.¹⁵ The limitations are further reinforced under Section 17, which grants overriding powers to the state in matters relating to the interests of sovereignty and integrity of India, friendly relations with foreign States and maintenance of public order. These exemptions assume greater significance in the context of predictive policing, where law enforcement agencies may rely on extensive datasets to identify crime patterns and conduct surveillance activities.¹⁶ Independent audits, transparency mechanisms, and oversight mechanisms remain absent, which results in predictive technologies relying on executive policies and administrative decisions rather than clearly defined statutes. Consequently, India's current regulatory framework remains insufficient in addressing constitutional concerns of privacy and accountability posed by predictive policing.

III. ALGORITHMIC BIAS, PRIVACY CONCERNS, AND OPACITY

A. ALGORITHMIC BIAS AND DISCRIMINATION

Predictive Policing models are not perfect and face multiple criticisms. One of the major criticisms it faces is susceptibility to algorithmic bias. While these systems are presented as objective and data-driven, they suffer from high algorithmic bias, which

¹⁴ MONDAQ, Data Protection Impact Assessments (DPIAs) Under the DPDP Act 2023: Scope, Methodology and Role in High-Risk Processing, <https://www.mondaq.com/india/data-protection/1698554/data-protection-impact-assessments-dpias-under-the-dpdp-act-2023-scope-methodology-and-role-in-high-risk-processing> (last visited April 8, 2026)

¹⁵ Sahil & Dr. Shobhna Jeet, *Predictive Policing, AI Surveillance, and Privacy in India: A Legal Analysis under the DPDP Act 2023*, 3 INT'L J. TRENDS EMERGING RES. & DEV. 84, 85 (2025).

¹⁶ Id.

reproduces and sometimes amplifies existing social inequalities when influenced by sensitive features like nationality, race and skin colour.¹⁷ Beyond this, proxy variables like residential location, educational attainment and socio-economic status can also contribute to unwanted racial or demographic bias. These variables function as proxies for protected characteristics and may produce substantially similar discriminatory outcomes.¹⁸

The problem originates from the presumption that historical data accurately reflects present criminal activity. However, in reality, crime data mirrors patterns of police deployment rather than offending rates. It is apparent that in areas where police presence is high, there will be larger volumes of recorded offences, arrests and police interactions.¹⁹ When predictive policing systems are fed with this biased information, they identify the same areas as 'crime hotspots', recommending increased surveillance in the area. This creates a reinforcing feedback loop where police presence produces more recorded incidents, justifying surveillance in those areas.²⁰

The dangers associated with algorithmic jurisdiction have been documented across various jurisdictions. A notable example from the USA is where the Los Angeles Police Department (LAPD) ended its predictive policing system (PredPol and Operation Laser) because of its discriminatory nature, disproportionately targeting black and brown communities.²¹ Another example is from the United Kingdom, where a study commissioned by the UK government indicates that police officers deployed in 'crime hotspots' identified by data analytics are more likely to arrest people due to bias and not probable cause.²²

In India, such concerns assume greater significance, exacerbating the deep-rooted inequalities in our country. Weaker sections of the society, such as the economically

¹⁷ J. Joseph, *Predicting Crime or Perpetuating Bias? The AI Dilemma*, 40 AI & SOC'Y 2319.

¹⁸ M. Kaufmann, S. Egbert & M. Leese, *Predictive Policing and the Politics of Patterns*, 59 BRIT. J. CRIMINOL. 674, 681 (2019).

¹⁹ Matt Franchi, J.D. Zamfirescu-Pereira, Wendy Ju & Emma Pierson, *Detecting Disparities in Police Deployments Using Dashcam Data*, FAcT '23, 534 (2023).

²⁰ James Quick, *Algorithmic Security And The Limits Of Predictive Policing: Data Ontology, Structural Bias, And The Reorientation Of Predictive AI Toward Cyber Threat Forecasting*. 2, 13 (2026).

²¹ THE GUARDIAN, LAPD to End Predictive Policing Program After Years of Criticism, <https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform> (last visited April 15, 2026).

²² Paul Cornish & Michael Clarke, *Algorithms and Bias in Policing*, Royal United Services Institute (RUSI) Report, 1(2019), https://assets.publishing.service.gov.uk/media/5d7f6b2540f0b61ccd4a4b80/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf.

weaker sections, the scheduled castes and the scheduled tribes, have historically been subjected to police discrimination. Training AI on historical data presents an inherent limitation of certain kinds of algorithmic biases, which may provide adverse analysis in cases where the accused belongs to a particular caste, religion or race.²³ Consequently, marginalised and vulnerable groups are likely to be targeted by the algorithm.

Such outcomes raise serious concerns about equality and non-discrimination. Predictive models that disproportionately target communities risk undermining these constitutional rights by institutionalising discriminatory practises through technology.²⁴ Thus, the danger of predictive policing lies in the fact that entrenched social inequalities can transform into algorithmic inequalities. When discrimination is justified on the grounds of technological objectivity, it makes it more difficult to detect, challenge and rectify.

B. PRIVACY VIOLATIONS

One of the most pressing challenges affecting the functioning of predictive policing systems is its invasion into one's privacy. Unlike traditional systems, predictive systems operate through large-scale collection, processing and analysis of data to forecast crimes before their occurrence. These systems rely on CCTV cameras, facial recognition software, and social media activity to enhance the efficiency of law enforcement.²⁵ However, due to the state's ability to monitor individuals on a large scale, the right to privacy is often affected.

The dangers associated with predictive policing extend beyond surveillance into the realm of informational privacy. In *Puttaswamy (2017)*, the court, while recognising privacy as our fundamental right, also acknowledged that individuals have an interest in controlling their personal information. Predictive systems challenge this principle by extensively relying on data processing to generate behavioural patterns and risk assessments for predicting crime activity. Consequently, information about

²³ N. Ramachandran & Mahajan Harshal Rajesh, *Artificial Intelligence in Policing*, 72(1) Indian Police J. 1, 8 (2025).

²⁴ Sneha Singh & Kashika Mittal, *The Constitution and Artificial Intelligence: The Future of Rights and Governance in India*, 5, 12 (2025).

²⁵ DELOITTE, Surveillance and Predictive Policing Through AI, <https://www.deloitte.com/global/en/industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html> (last visited April 18, 2026).

an individual is continuously monitored without them even knowing about it.²⁶ Such a circumstance can also be understood through the concept of 'Panopticon', originally developed by Jeremy Bentham and later popularised by Michel Foucault. A prison surveillance system where inmates live in fear of constant observation. This type of surveillance may shun the personality and reduce the liberty of individuals if they believe that their conduct is subject to continuous surveillance, affecting privacy and broader democratic freedoms.²⁷

A further problem arises from the possibility of a function creep, where data that is collected for a particular purpose is used for a completely different objective without the consent of the individual. AI systems intended for specific crime prevention goals might gradually be repurposed for unwarranted surveillance activities not initially considered.²⁸ In India, this problem emerged when reports on how AI enabled CCTVs under the Safe City Project were being used for reasons other than women's public safety, such as monitoring VIP movements and detecting suspicious activity.²⁹

Another notable example is India's National Intelligence Grid (NATGRID), a platform for the police and investigating agencies to securely access private databases in real time, which was processing 45000 data access requests per month. Various datasets were accessible through NATGRID, such as details of driving licenses, Aadhaar registration, airline data, bank records, and details of social media accounts that share posts on a particular issue.³⁰ Similar concerns arise from the amendment of Aadhaar authentication rules, allowing for private businesses to use Aadhaar for customer identification. However, at the same time, it raises privacy risks as biometric data can be misused.³¹ This large-scale data collection raises

²⁶ Rainer Mühlhoff, *Predictive Privacy: Towards an Applied Ethics of Data Analytics*, 23 Ethics & Info. Tech. 575 (2021).

²⁷ J. E. Campbell & M. Carlson, *Panopticon.com: Online Surveillance and the Commodification of Privacy*, 46(4) J. Broad. & Electronic Media 586, 597 (2002).

²⁸ Fantin, Stefano and Vogiatzoglou, Plixavra, Purpose Limitation By Design As A Counter To Function Creep And System Insecurity In Police Artificial Intelligence (August 21, 2020). United Nations Interregional Crime and Justice Research Institute.

²⁹ THE PATRIOT, Facial Recognition CCTV Network to Expand Across Delhi Under Safe City Project, <https://thepatriot.in/reports/facial-recognition-cctv-network-to-expand-across-delhi-under-safe-city-project-74311> (last visited April 23, 2026).

³⁰ THE HINDU, National Intelligence Grid Slowly Gathers Pace, Receives 45K Requests a Month, <https://www.thehindu.com/news/national/national-intelligence-grid-slowly-gathers-pace-receives-45k-requests-a-month/article70369184.ece> (last visited April 29, 2026).

³¹ BOOM, Aadhaar Authentication Now Open to Private Companies: Is It Safe?, <https://www.boomlive.in/explainers/aadhaar-authentication-now-open-to-private-companies-is-it-safe-27744> (last visited April 29, 2026).

similar fears that predictive technologies may also be used to utilise our data in a way without adequate transparency, giving rise to a surveillance state.

C. THE BLACK BOX PROBLEM

Another pressing concern affecting predictive policing is the “black box problem”, where the algorithm's internal reasoning on how it arrived at a particular conclusion is hidden from the public. This stems from several factors that often conflate. Many of the machine learning (ML) algorithms (algorithms that are relied on by predictive policing models) are designed so that they cannot explain their predictions in a way that humans can understand.³² Additionally, a degree of opacity may be built in by developers as an intentional form of self-protection.³³ Consequently, individuals are never given the reason why they were put under surveillance, shielding this model from public scrutiny.

Predictive Policing programs such as PredPol and Operation LASER used by the LAPD suffered from a lack of transparency. It took four years of work by activists to bring these programs under public scrutiny.³⁴ Even in India, it was found that there was an intentional opacity which was constructed around Delhi's CMAPS, kept out of the reach of the Right to Information Act, invoking broad exemptions for security and strategic information of the State and law enforcement purposes. This raises concerns about whether national security considerations may justify a degree of confidentiality and excessive secrecy surrounding predictive systems.³⁵

An algorithm detects crime hotspots or identifies individuals as high risk based on factors that are not disclosed to the public. Individuals subject to such restrictions are not informed of the basis of such a decision, making it difficult for them to challenge the basis for arriving at such a decision.³⁶ These outcomes are against universal principles of fairness that require state action to be subject to review.

³² Rudin C, *Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead*. NAT MACH INTELL 206 (2019).

³³ J. Burrell, *How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms*, 3(1) Big Data & Society 1, 2 (2016).

³⁴ LOS ANGELES TIMES, Editorial: The Problem with LAPD's Predictive Policing, <https://www.latimes.com/opinion/editorials/la-ed-lapd-predictive-policing-20190316-story.html> (last visited April 30, 2026).

³⁵ Vidushi Marda & Shivangi Narayan, *Data in New Delhi's Predictive Policing System*, 2020 FAT 317, 323 (2020).

³⁶ Eirik Bakke, *Predictive Policing: The Argument for Public Transparency*, 74 NYU Annual Survey of American Law 131, 154 (2018).

Furthermore, when it is found that the algorithm produces a flawed or biased outcome, determining who will be liable becomes increasingly difficult. A dilemma arises whether liability should rest with the designer of it, the private company which supplies it or the executive authorities who authorised its deployment.³⁷ This results in an erosion of institutional accountability where no single person is held responsible for the faults in the algorithm.

In a constitutional democracy like India, where transparency and accountability are considered essential safeguards against arbitrary state power, these concerns assume greater significance. When policing and surveillance decisions are taken on reasons that cannot be scrutinised or understood, the risk of arbitrariness increases. Such opacity undermines procedural fairness under Article 21³⁸ and protection against arbitrary state action under Article 14³⁹. Without transparency, predictive policing risks replacing human discretion with algorithmic decision-making that is not accountable.

IV. SECURITY V/S LIBERTY: DOES PREDICTIVE POLICING SURVIVE CONSTITUTIONAL SCRUTINY?

The introduction of predictive policing in the law enforcement of our country has led to tension between the state and citizens. On one hand, the state has a duty to prevent crime, ensure the safety of individuals, and improve the efficiency of law enforcement, even if it means using advanced technologies to predict the threat beforehand. On the other hand, the use of these technologies results in increased surveillance, profiling and data collection, which infringes upon fundamental rights guaranteed in the Constitution. This tension can be evaluated from the three-fold test laid down in *Puttaswamy (2017)* to evaluate any state action that invades our right to privacy. The three essentials are legality, necessity and proportionality. Applying these essentials to predictive policing raises serious questions.

The first requirement of legality states that infringement of our rights must be backed by a clear law. Currently, India's AI governance is guided by baseline frameworks. While these frameworks provide safeguards, they are not specifically designed to address the emerging and unknown complexities arising from the AI's

³⁷ A. Shapiro, *Accountability and Indeterminacy in Predictive Policing*, in *Predictive Policing and Artificial Intelligence* (Routledge 2021) 1, 185 (2021).

³⁸ INDIA CONST. art. 21.

³⁹ INDIA CONST. art.14.

development, adoption and deployment.⁴⁰ This results in predictive policing operating within a “grey area” of the law. Therefore, it fails the requirement of legality.

Undoubtedly, crime prevention is a legitimate aim. However, the requirement of necessity demands more than a legitimate aim, where the state must prove its action is the least restrictive way of achieving its objective. Conventional policing methods such as investigation, targeted surveillance and community policing serve as effective alternatives without requiring extensive state collection and processing of personal data. As a result, while predictive policing may supplement existing policies, its necessity as a law enforcement tool remains questionable.

Proportionality requires that the benefits of a state measure outweigh the harm caused to fundamental rights. Predictive policing relies extensively on data collection, behavioural profiling and continuous surveillance of individuals who may not be suspected of any offence. These arbitrary intrusions affect privacy, autonomy and protection from arbitrary state action.⁴¹ Thus, for predictive policing to function legally, its actions will have to benefit the people.

While still in an embryonic stage, the absence of legality, necessity and proportionality tilts the balance in favour of the state, giving it excessive power at the cost of fundamental rights.

V. RECOMMENDATIONS

To ensure that police functions as a tool for justice rather than a mechanism for surveillance, a comprehensive regulatory framework will have to be adopted governing the use of AI and algorithmic systems in law enforcement. Predictive policing currently operates under fragmented rules and policies without an established legal foundation, enabling the misuse of state power. Therefore, specific legislation must be enacted to regulate predictive policing, defining the circumstances in which predictive technology may be used, the categories of data collected, the duration of such collection, and the remedies available to individuals. A clear law that allows limited exercise of surveillance powers will strengthen the requirement of legality in *Puttuswamy (2017)*.

⁴⁰ NITI Aayog, STRENGTHENING AI GOVERNANCE THROUGH TECHNO-LEGAL FRAMEWORK 1,2 (2021). https://psa.gov.in/CMS/web/sites/default/files/publication/AI-WP_TechnoLegal.pdf

⁴¹ OXJOURNAL, Predictive Policing or Predictive Prejudice?, <https://www.oxjournal.org/predictive-policing-or-predictive-prejudice/> (last visited May 6, 2026).

To strengthen transparency, law enforcement agencies should ensure that their algorithms are explainable and accessible. Citizens should have access to the data, which is collected and processed, and the purpose of data collection and processing. In furtherance of the principles of consent and transparency recognised under the DPDP Act, public authorities must maintain dedicated portals through which citizens can obtain information, raise grievances and seek clarification regarding algorithmic decision-making. Cities like Helsinki and Amsterdam have followed this suggestion by launching open AI registries, which offer an overview of existing AI systems and the algorithms used by the municipal government. The central aim of this registry is to be more transparent and reduce discrimination.⁴² To further facilitate transparency, in-house software developers must be used rather than commercial companies to develop predictive policing software. Hiring specialised personnel with a background in computer science will easily be possible in India, allowing the development of the software to be checked, and thus avoiding the black box problem. To counter algorithmic bias and discrimination, monitoring the data quality and its collection is of paramount importance. Data quality must be assessed on a regular basis, where a special analysis unit must be set up to monitor data collection and to suggest proposals for the improvement of the software and data quality. Police personnel and software developers who enter the data and interpret the results must be adequately trained. The training should devote attention to the limitations of the algorithms, particularly the possibility of false positives and bias, as well as the individual's responsibilities in interpreting results. Human oversight must remain central to decision-making, ensuring that algorithmic outputs function as advisory tools, rather than definitive conclusions.

To ensure accountability, independent oversight bodies that are adequately funded and staffed must be established. The body's responsibility should extend beyond review of the algorithmic system and must also include examination of all aspects of data usage by the police. Independent review would allow predictive policing practises to remain consistent with constitutional principles, thereby preventing misuse of surveillance technology and restoring public confidence in the criminal justice system.

⁴² VENTUREBEAT, Amsterdam and Helsinki Launch Algorithm Registries to Bring Transparency to Public Deployments of AI, <https://venturebeat.com/technology/amsterdam-and-helsinki-launch-algorithm-registries-to-bring-transparency-to-public-deployments-of-ai/> (last visited May 6, 2026).

VI. CONCLUSION

The growing advent of predictive policing in India marks a new dawn in our criminal justice system, reflecting the growing reliance of the police on emerging technologies to control criminal activity. By promising better allocation of resources and greater efficiency, these models present themselves as an attractive solution in a country where law enforcement faces challenges of understaffing, rising cybercrime and delayed investigations.

However, the promise of predictive policing also exposes its inherent nature, making it a double-edged sword. Predictive policing models rely on historical data to predict crime, which reinforces discrimination in culturally sensitive areas. This type of policing also affects our privacy: when our personal information is collected on a large scale, we become susceptible to state surveillance. Without any proper legal protection, our individual autonomy risks getting weakened. The lack of transparency adds to the list of problems where the functioning of algorithmic systems is hidden from public scrutiny. When the rationale behind a particular decision is hidden, accountability weakens, and democratic oversight is undermined.

In conclusion, the increasing integration of predictive technologies into law enforcement cannot, in its present form, be justified within the constitutional framework governing privacy, equality, and democratic accountability in India. While the objective of crime prevention remains legitimate, the absence of a dedicated legal framework, meaningful algorithmic transparency, independent oversight and adequate safeguards against discriminatory outcomes prevents predictive policing from satisfying constitutional standards. Consequently, greater legal, institutional and technological reforms are required before predictive policing can operate in a manner consistent with the values of a constitutional democracy.