

A Study on The Use of AI In Predictive Policing in Crime Prevention: Current Trends in International and National Level

Vencelin Gino V

Crescent School of Law, B. S. Abdur Rahman Crescent Institute of Science and Technology

Abstract—The prevention of crimes is a public responsibility and the duty of the government. Every government in the world tries to prevent crimes by making a set of rules and having a regulatory body. Digital age needs digital police. Technology alone is not enough to prevent crimes. Use of technology tools should be to take the input of the surveillance data and predict the likelihood of a crime. The term predictive is a way of forecasting. The paper provides comprehensive analysis for the integration of Artificial Intelligence (AI) in predictive policing strategies for crime prevention and the current challenges in the AI tools. The aim is to critically evaluate the technological paradigm shift from reactive to data-driven proactive law enforcement intervention. We also address ethical and social challenges facing predictive policing, including algorithmic bias, the exacerbation of existing social inequalities, and a loss of community trust. We see different technologies being adopted by Indian government to improve and support predictive policing to prevent crime before it occurs. Finally, we list the different approaches in different countries and the status of those approaches and their challenges.

Index Terms—*Artificial Intelligence, Predictive Policing, Crime Prevention, Algorithmic Bias, Ethical AI, Data Analytics, Law Enforcement Technology, Social Implications, Legislative Frameworks.*

I. INTRODUCTION

In India, policing is a state subject. There have been many tools developed to help the government to detect crime. The detective system is a diagnostic method that deals with cures rather than prevention. Hence, it is important for us to foresee the possibility of any crime occurring so that it can be averted before it occurs. “AI can predict possible criminal activities by

analysing past crime patterns, social behaviour and environmental factors using advanced algorithms, machine learning and big data analytics. Artificial Intelligence is to use human life by reducing the iterative task done by human by using a machine with the help of algorithms and collection of data which become turns into a model. The data is collected from different sources and a predefined datasets are developed and algorithms are applied to the dataset and a model is developed. Such dataset can be also developed for crime prediction but it leaves a question that how effective it can predict for a crime based on the data that is given because the crime differs human to human and community to community. An algorithm is also created by humans based on the input taken by others and hence it is prone to bias.

II. LITERATURE REVIEW

In India, policing is a state subject. There have been Artificial Intelligence has the potential to transform law enforcement, with tools such as predictive policing that aim to help prevent crime. But its use has sparked serious alarm among policy makers and human rights groups about the erosion of basic rights. Criminological literature shows that offenders are often found in familiar environments, which leads to the formation of spatial crime hotspots that can be used for predictive modelling¹.

The author explored the use of artificial intelligence (AI) and machine learning (ML) in crime prediction. The research showed the effectiveness of supervised learning approaches in the analysis of various crime types². The use of AI models in the justice and policing sectors raises ethical implications, and particularly

¹ (Mahmud, 2016)

² (Dakalbab, 2022)

those related to honesty, equality, privacy and rights for individuals³.

Crime pattern theory and artificial intelligence, especially neural networks, have promise for predicting criminal activities, but suffer from scalability and real-time application problems. However, current work is often plagued by problems of data quality, bias, scalability and generalisability, thus suggesting a need for more robust models and thorough evaluation strategies. Historical crime data can perpetuate systemic bias and over-policing, resulting in serious ethical and civil liberties concerns.

III. THE TERM PREDICTIVE

Predictive is a form of forecast based on the probability. It signifies that according to specific scenario something is probable to happen. These situations are predicated on the earlier information or perspective of the individual developing the probability. Let us consider weather forecast for rain or cyclones, we obtain the forecast from the forecast station that it's likely to rain today at 9:00 AM tomorrow with 75% likelihood but we may not get rain at all. Because they have forecasted with many factors and if there is any change in one aspect it would affect the whole prediction. For weather predictions, even if it goes false positive it does not harm anyone as it does not amount to a criminal act. Predictive policing is a type of prediction that accuses an individual or group of people and marks them as criminals. If the police take steps on the belief, they are preventing a future crime and arrest the person projected to commit the crime by the system, then the system will bar the person from gaining the immunity in the constitution. And if the police do not take the forecast seriously and it happens, then the police will be blamed for not taking appropriate steps to prevent the crime that has been reported by the system.

IV. TRADITIONAL POLICING

Traditional policing is a reactive model of crime: it reacts to crime after it occurs. Thus, the victim has a way of compensation, and the criminal gets punishment. The model is evaluated by the number of cases and its investigations and solutions. There are

serious drawbacks to this non-strategic, reactive approach.

It depicts the police as forever playing catch-up to the criminal and frequently falls short of addressing the root causes that allow crime to happen. That is, in the traditional policing, there will be a victim and a criminal, and the police will be the hero. In most domestic crimes the police function as a middleman like a referee who attempts to make both the parties agree rather than delving into the underlying cause of the issue and finding a solution or pointing them to a court for the resolution of the conflict. Thus, there is no prevention of future crimes but rather it encourages and cultivates some form of reactive measures for compromise between parties.

V. DATA-DRIVEN APPROACH IN POLICING

We are on the brink of a huge paradigm change in policing technology from the reactive approach to a new vision of public safety with data-driven, proactive action. The new paradigm relies on advanced digital technologies like Artificial Intelligence (AI), Machine Learning (ML), Big Data analytics, Internet of Things (IoT) sensors and geographic information systems (GIS) to predict and prevent crime before it occurs. Better prediction techniques will enable authorities to use resources more effectively, prevent the formation of criminal networks and boost deterrence through prompt intervention.

That change is already underway in India. Indian law enforcement is quick to adopt innovations such as use of Automated Facial Recognition Systems (AFRS) in Delhi and Telangana, predictive analytics to detect crime hotspots in Mumbai and Bengaluru. The motivation is to change the police from non-strategic and reactive to strategic and proactive who can see what their opponent is going to do. But this technological revolution, however, is not without great problems. The deployment of these systems in the Indian enforcement scene poses essential issues that cut to the heart of our democratic democracy.

VI. TECHNOLOGICAL TOOLS IN POLICING

³ (Raji, 2024)

Traditionally police perform patrols through the areas to monitor and maintain security and surveillance of the community. With the advancement of technology now most of the cities have deployed Closed-Circuit Television (CCTV) cameras which monitor crime incidences and used as evidence. Also, CCTV cameras have helped to reduce crimes in certain areas as it makes people aware that there is an eye watching over them and a recording is available to make it as evidence. In busy areas like airports and railway stations facial recognitions are used over the live CCTV footage to detect offenders around the area. Even though the accuracy of such technological involvement is still under debate, it helps to improve the public safety mainly in busy traffic areas.

Predictive Policing Algorithms can be used along with CCTV surveillance which can leverage the use of historical crime data (type, location, time) to generate predictions about future criminal activity. This can be achieved by using place-based prediction in which the Algorithms like "hotspot mapping" identify geographical areas with a high density of historical crime data based on a dataset fed to the algorithms. Police are then directed to patrol these predicted "hotspots" more intensively. Companies like PredPol popularized this model. Another method is person-based prediction. In this the systems analyse data on individuals (e.g., prior arrests, habitual offenders) to generate "risk scores" indicating their likelihood of being involved in a future crime, either as a perpetrator or a victim.

Facial Recognition Technology (FRT) tools are not used as standard law enforcement tools. It works by mapping an individual's facial features from an image or video feed and comparing them against a database of known faces. We can use a still image from a crime scene to a police database of mugshots and compare with the live data. Live video feeds from CCTV cameras or drones are analysed in real-time to identify individuals on a watchlist in a crowd, at a checkpoint, or in a public space.

Geographic Information Systems (GIS) and Crime Mapping go beyond simple hotspot mapping. It allows for the spatial analysis of crime data layered with other demographic and infrastructural data lighting, poverty levels, liquor store locations, public transport routes to identify complex patterns and environmental factors

that contribute to crime, allowing for more targeted environmental design and resource allocation⁴.

Network Analysis Software is a technology used to analyse communication metadata (call records, financial transactions, social media connections) to map and visualize relationships between individuals and organizations. It is instrumental in investigating organized crime, terrorism networks, and complex financial fraud by identifying key nodes and influencers within a network.

Mobile Apps like Delhi Police's Himmat Plus and Kaaval Uthavi allow citizens to report crime, creating new streams of data and enabling community interaction, but also raising concerns about the verification and bias in citizen-reported data.

VII. ACCESS OF TECHNOLOGY TO PUBLIC

Mobile phones in public hands have given a method to report crime and take electrical evidence of crime in domestic or in public places. Also, it has given a method to raise their voice against any violence and injustice in society. As there are positive points there are also the downside of the technology that there are more rumours and irrelevant information are being circulated without checking the facts and it brings fear to the society and spreads wrong information to the public. Technology in public hands set the stage for discussing the immense potential and the significant ethical and legal challenges.

VIII. THE INDIAN CONSTITUTIONAL FRAMEWORK

A. Article 14 (Right to Equality)

How do algorithms avoid creating a system that disproportionately targets specific communities, thus violating equality before law?

Article 14 states that the State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India. Proactive policing interfaces with the Constitution in several ways. There is a possibility for the proactive policing to violate Article 14 that states about the rights to equality as it may predict innocents as criminal based on the given dataset by using the algorithm.

⁴ (Sachin Chauhan, 2025)

Two people committing similar acts may be treated differently based on their location, their lifestyle and other social factors. For example, A person from an affluent area may escape AI “suspicion,” while one from a poor area may be flagged as “high risk.” As it happens over time with traditional policing, AI will be used to over-surveillance Dalits, minorities, migrants, or economically weaker sections. The burden of false suspicion disproportionately falls on marginalized groups who often lack resources to challenge AI-driven errors. In United States of America, software tools used for criminal justice systems to assess the risk of re-offending tend to label Black defendants as higher risk than white defendants even when their outcomes are similar. Few years later it was evident that the algorithm was wrong in its prediction as whom it predicted as re-offending was exactly opposite⁵.

Suppose predictive policing software flags a location as a high-crime prone zone based on past police report then the police start to stop and questioning the residents of that area, mostly belonging to a particular caste or religion. Residents from other areas, even if equally or more prone to crime, are not harassed.

B. Article 19(1)(d) (Freedom of Movement)

Does being flagged by a predictive system or being in a "high-risk" category implicitly restrict a citizen's free movement without due process?

Article 19(1)(d) states that all citizens shall have the right to move freely throughout the territory of India. We cannot assume that once an offender is an offender forever. So, it is important for the algorithm not to tag or flag to pinpoint the previous offenders as a suspect based on the predictive algorithm which will violate Article 19(1)(d) which states the freedom of movement for the individual citizens.

AI tools can predict where crimes may occur and who is more likely to commit them. Based on these predictions, police often increase surveillance, checkpoints and restrictions in certain areas. This impacts the free movement of individuals, especially those labelled as “high risk.”

If AI marks certain neighbourhoods as crime-prone zone, residents face constant checks and questioning. This restricts their right to move freely without harassment. AI may identify specific persons as “likely offenders.” Such individuals may be stopped,

followed, or restricted in their mobility without actual crime committed.

If AI predicts that youths in an area are likely to engage in gang violence, Police respond by setting up checkpoints only in that area, frequently stopping and questioning residents (especially young men), restricting late-night movements. People from that area lose their freedom of movement, even if they are law-abiding citizens.

C. Article 20(3) (Right Against Self-Incrimination)

Could being targeted based on predictive data be seen as a form of testifying against oneself?

Article 20(3) states that no person accused of any offence shall be compelled to be a witness against himself. AI algorithms can use personal data as evidence by analysing our mobile, bank, or social media data and conclude that this person is a criminal. In such a scenario it is essentially using our own actions or data as evidence against us. This amounts to a form of Self-Incrimination. If predictive policing software identifies us as a suspect, during interrogation police may use the AI-generated data to force us to admit guilt which amounts in Compelled Confession.

Suppose an AI model, based on the phone location, social circle, social media posts and conversations, predicts that this person is likely to commit theft. Now, when police interrogate person, they may present the AI data as evidence. Thus, his own personal data is used against him as testimony.

D. Article 21 (Right to Life and Personal Liberty)

Does pervasive surveillance and pre-emptive intervention infringe on the right to privacy?

Article 21 states that no person shall be deprived of his life or personal liberty except according to procedure established by law. Predictive policing tools analyse past crimes, behavioural data, surveillance feeds, social media, and movement patterns to predict who might commit a crime or where and when a crime might occur. While it aims to prevent crime, it has serious risks for individual rights. AI-driven predictive policing uses mass surveillance (CCTV, mobile tracking, social media scans). Continuous monitoring

⁵ (Julia Angwin, May 23, 2016)

intrudes upon privacy, which is a part of the Right to Life and Liberty⁶.

AI may label a person as a “potential criminal” even if they have never committed a crime. This deprives them of dignity and liberty. Based on AI predictions, police may stop, interrogate, or even detain someone without solid evidence. This amounts to deprivation of personal liberty without due legal process. If people know they are under constant AI surveillance, they may avoid free movement, expression, or association.

IX. BIAS IN THE ALGORITHM

The biggest problem of these methods is that they cloak human prejudice in a veil of mathematical objectivity. You can challenge an officer acting on a hunch but an officer acting on an automated recommendation can say they are just doing the impartial, scientific thing? This automated bias produces a patina of legitimacy that makes discriminating outcomes harder to contest. This is an example of how an instrument of proactive police may swiftly become an instrument of social control and suppression of opposition. The computer doesn't know if it's a protester or a terrorist, it just provides a match.” The human decision to use it in that setting, with that crowd, injects a political and prejudiced judgement into a system that is sold as impartial. The algorithm leverages the pre-existing bias of the authorities who use it and provides them with strong technological reasons for their behaviour.

However, this sense of impartiality presents a black box dilemma, because we do not know how the AI tool has arrived at the solution. The precise working of proprietary forecasting algorithms is often a trade secret. When an algorithm flags a citizen and they are detained or interrogated, they don't know why. They can't cross-examine the algorithm or dispute the weight it allocated to particular data pieces. Such lack of openness is in outright contravention of norms of due process and fair trial.

In computing, the quality of the input to a process or system directly impacts the quality of the output from that process or system. If the input data or information is inadequate, biased, incomplete or of low quality ("garbage"), the output generated will also be bad,

inaccurate or of comparably low quality. This is called the “Garbage In, Garbage Out” (GIGO) problem⁷. Crime data reflects bias in policing. If certain neighborhoods or communities were over-policed in the past, data shows more crime there, and the algorithm recommends more policing there, creating a vicious feedback loop. Models trained on low-quality Indian data such as low-resolution images for FRT, will perform worse on Indian faces leading to higher false positives for certain demographics.

X. LAWS STRUGGLING WITH MODERN TECH

The Indian Evidence Act, 1872 deals with the relevancy of evidence in the court of law. It has no mechanisms for dealing with evidence generated by an AI system. How does one establish the truth of a predictive algorithm? Who is the expert? Can I see the source code and ask about it? The Act is mute.

Bharatiya Nagarik Suraksha Sanhita (BNSS), 2024; Previously known as Code of Criminal Procedure (CrPC), the BNSS prescribes protocol of arrest, search and investigation. Belief or suspicion towards a person is found on the concept of concrete individualised belief. Proactive policing is based on statistical probability not individual suspicion. There is no legal architecture around what a police officer can do with a high-risk score. Can they halt a person? Question them? Search for them? There are no answers in the BNSS, and it leaves a grey area of law.

The Indian Police Act, 1861- this law from the colonial era deals with the organization and functions of the police force and does not deal with the regulation of sophisticated technology. There is no guideline on how AI should be used ethically.

The biggest omission is the lack of an all-encompassing data protection regulation. The Digital Personal Data Protection Act (DPDPA), 2023 has been enacted, but has not yet come into action and has come under criticism for allowing large exemptions to government entities, notably for law-and-order purposes. This means there are no strong legal safeguards on how police can gather, manage and share the huge amounts of personal data essential for proactive policing. These regulatory vacuum permits law enforcement to deploy sophisticated technology

⁶ (Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors, 2017)

⁷ (Citrome, 2024)

with minimal legal justification, oversight or accountability

XI. ACCOUNTABILITY OF BIAS PREDICTION

When the Algorithm gets it wrong, it's important to ask who is responsible? If a predictive system labels an innocent person as a potential criminal, resulting in police harassment or arrest, who is liable? There is a fundamental legal principle that for every right there must be a remedy. Proactive policing creates a vacuum of accountability. Who should be blamed when an algorithm makes a mistake? The existing law does not provide clear-cut answers.

The cop? "Reliance in good faith by an officer on algorithmic recommendations could be argued as simply relying on a reliable technological tool." Are they responsible for the algorithm's mistake?

The Senior Officer who authorized for Deploying the System? Is it the role of the Police Commissioner who approved for the implementation takes accountability for biased response?

Software Engineer? The private company that developed the algorithm can say it's just a toolmaker, and that it's the police who get to decide how to use it. They also tend to keep their source code as a trade secret, so it is not open to scrutiny.

The Government? Ultimately, the state is accountable for the actions of its agencies, but in a practical sense it is difficult to hold the abstract state accountable.

There is no clear liability, leaving a citizen targeted, harassed or arrested erroneously based on a faulty algorithmic prediction with no clear way to seek redress. They can't sue an algorithm. Perhaps the gravest danger to justice in this new paradigm is this accountability vacuum, which insulates the powerful decision-making system from any consequences for its errors.

XII. INTERNATIONAL MODELS OF AI-DRIVEN PREDICTIVE POLICING

Countries around the world have taken different approaches to the use of predictive policing technologies, based on their legislative frameworks,

technological capacities, and law enforcement goals. These approaches differ considerably in design, scope and implementation, and provide valuable lessons on both good practice and possible pitfalls.

PredPol (formerly Geolitica), HunchLab and Palantir are all US-made current predictive police software and are used widely. It is mostly utilised for place-based predictions in large cities such as Los Angeles, Chicago and New York. Hotspot maps are generated daily to inform patrols of the systems. Research shows that these systems tend to perpetuate racial and socioeconomic biases. An audit of Los Angeles found that predictive policing disproportionately targets Black and Latino areas⁸. The outcry has been so strong that communities like Santa Cruz and New Orleans have outlawed the use of predictive police software, claiming the results are discriminatory, and it doesn't work any better than chance⁹.

The UK's approach, and that of West Midlands Police in particular, has been less about predicting locations and more about assessing the risk of individuals and analysing networks. The National Data Analytics Solution (NDAS) was a project that used artificial intelligence to forecast who could be at danger of being involved in significant violence, either as a perpetrator or victim, by assessing people's connections and their past encounters with police and social agencies¹⁰. The project was clandestine and highly guarded by civil rights groups. Eventually, it lost its funding in 2022 amid concerns over ethics, legality and transparency. The failure highlights the difficulty of building ethical and lawful person-based forecasting algorithms.

China has used predictive AI in the most extreme and invasive way, to embed enforcement into the wider Social Credit System¹¹. The state is always observing its inhabitants through a massive network of cameras, facial recognition and data collecting from apps, purchases and social media. AI is utilised not only to forecast crime but to predict societal instability and non-desirable behaviour. Proactive use of punishment (e.g., travel bans, decreased credit ratings). This is the complete antithesis of democracy in which the state employs technology to exercise unlimited control over society and to punish pre-crime. It warns of the

⁸ (Bhuiyan, 2021)

⁹ (Jany, 2022)

¹⁰ (National Data Analytics Solution (NDAS) Privacy Notice, n.d.)

¹¹ (Awasthi, 2026)

dangers of governments using AI to spy on people without any rules.

Location-based prediction is often found to propagate bias internationally, while individual-based prediction poses major ethical difficulties. Even the most sophisticated democracies have failed to deploy these mechanisms in a fair and transparent manner, and many have scaled back or abandoned efforts. China's approach is a cautionary story of techno-authoritarianism.

XIII. INDIA'S TOP-DOWN DRIVE FOR SMART POLICING

At the national level, the Government of India has introduced a number of projects that constitute the infrastructure for data-driven policing, albeit frequently without a legal framework. Crime and Criminal Tracking Network and Systems (CCTNS) is the backbone of modern policing in India¹². Launched in 2009, CCTNS seeks to network all the police stations in the country to develop a nationwide database of crime and criminals. Any predictive policing system runs on the digitised centralised historical crime data that CCTNS feeds. Its adoption across the country is a pre-condition for systems such as the proposed National Automated Facial Recognition System (NAFRS)¹³.

The Interoperable Criminal Justice System (ICJS) goes a step further by linking CCTNS with the databases of courts (eCourts), prisons (ePrisons) and forensic labs. The purpose of it is to make sure that information flows through the criminal justice system. ICJS greatly multiplies the data accessible for analysis. An algorithm would now conceivably be able to take into account data on court decisions, prison records and forensic evidence, compiling more comprehensive and potentially more invasive risk profiles of individuals.

The National Automated Facial Recognition System (NAFRS) is expected to provide a centralised platform for police in India to deploy facial recognition technology. It has been developed to be compatible with other databases like CCTNS and to enable retrospective and real-time identification of criminals. The NAFRS project is a poster child for the national-

level push for technology without legal architecture to support it.

The Smart Cities Mission focuses on establishing integrated CCTV networks, IoT sensors and command-and-control centers in 100 cities builds the pervasive surveillance infrastructure on which predictive policing applications depend. The central government's approach has been technocratic, focusing on infrastructural development and database integration. Privacy, federalism, data protection, and algorithmic prejudice have mainly been afterthoughts, creating a worrisome mismatch between technological capabilities and legal accountability.

XIV. MORDEN TECHNOLOGY IMPLEMENTATION ACROSS INDIA

Policing is a state topic in the Indian Constitution, with a wide variation in the ways in which it is conducted and experimented with among states. It establishes "laboratories" in which multiple models are being evaluated.

The Telangana Police in Hyderabad has led the way in the use of surveillance technology. They have created one of the biggest Command and Control Centres in the country with thousands of CCTV cameras integrated. They employ FRT for an enormous range of uses, like spotting criminals in a crowd or confirming who owns a vehicle. They've also experimented with utilising FRT to encourage behaviour, such as employing cameras to identify people dumping waste illegally. Technology is used extensively and for multiple purposes in Telangana's model and there is a lack of clarity between crime prevention, general law enforcement and civic management.

The Punjab Police have extensively employed technology, especially in combating terrorism and narcotics trafficking. They use FRT and network analysis technologies to map and take down drug supply lines. They were the first to employ the Punjab Police app with FRT during the COVID-19 lockdown to identify quarantine violators, exhibiting both the agility and the potential for function creep of these tools. The Punjab's approach is primarily about

¹² (Crime and Criminal Tracking Network & Systems, n.d.)

¹³ (Jain, 2026)

focusing on some select, high-priority crimes through network analysis and targeted surveillance.

Mumbai Police embraces technology to complement conventional means, not substitute them¹⁴. They employ crime mapping, based on GIS, to detect hot locations and to improve patrol routes. The focus has been on integration of existing systems such as CCTNS and using data for resource allocation rather than implementing cutting-edge AI for individual risk assessment. A more deliberate, operation-driven strategy that leverages data to inform human decisions, not to replace them.

The location of the Delhi Police and the nature of the difficulties it faces (protests, political events) mean that the use of technology by the Delhi Police is under the most rigorous scrutiny¹⁵. Use of AFRS at protests has been quite controversial. They also have a citizen reporting mobile application (Himmat Plus) and a large network of CCTVs. The implementation in Delhi has not yielded the desired results, which has hindered the introduction of such a tool across the rest of the country. This unequal application results in a situation where a citizen's experience of predictive policing is totally dependent on their location and results in disparity in the application of law and privacy rights. The Tamil Nadu police launched Kaaval Uthavi app in 2022, aimed at helping civilians to contact police for help in situations fast by incorporating a prominent red-alert button that communicates the user's live location to a control room and alerts the nearest patrol unit. It is a tool for assistance and emergency reaction. It doesn't employ data analytics or AI to predict crimes or potential criminals.

XV. PRINCIPLES FOR RESPONSIBLE AND RIGHTS-RESPECTING PROACTIVE POLICING

It is neither possible nor desirable to reject technology altogether. The objective should be to take it on responsibly. The future foundation for India's proactive policing should be based on the following principles:

Legislative requirement:

The use of predictive policing and FRT needs to be regulated by a special and strict law, established by Parliament. The law needs to identify the allowable

purposes, the boundaries of usage and the controls. It must pass the Puttaswamy triple test.

Transparency and Auditability:

"Right to Explanation" laws are necessary. Before any technology is deployed agencies must do and publish Mandatory Algorithmic Impact Assessments (AIAs). Citizens should have the right to know when an algorithm has been used to make a decision against them, and to be given an explanation in clear words.

Human-in-the-Loop: Algorithms should stay advising tools only. Ultimately, a qualified police officer must decide to stop, question or arrest an individual, and must be able to justify reasonable suspicion based on the output of the algorithm and other observable criteria.

Data Quality and Bias Mitigation:

Policies should be put in place to evaluate training data for bias, diversify datasets, and test algorithms for biased outcomes on an ongoing basis. The goal should be to reduce bias, not to institutionalise it.

Robust Redressal Mechanisms:

The law must provide a clear and accessible grievance redressal procedure. This includes the right to contest algorithmic decisions, to have one's data updated, and to get compensation for damage caused by system faults.

Sunset Provisions and Periodic Review: The authorisation to employ such strong systems should not be everlasting. It should be regularly renewable by legislature, based on shown effectiveness and a record of proven compliance with rights.

XVI. PROBLEM OF AI

For AI, somewhere, someone should give input for the algorithm with the set of data on which the model will be built. The system itself does not think so it can predict only based on the data given to the system. It cannot make any critical thinking on its own. It has two methods which are called supervised learning and unsupervised learning. In supervised learning, a label with the dataset is given to extract a particular information from the dataset. For example, a mugshot

¹⁴ (Thacker, 2025)

¹⁵ (Kava, 2026)

of an accused can be a label which can be given with the live surveillance camera to identify accused in a crowded area like market or railway station, but we cannot ensure that the person is going to commit a crime at this time but whatever we have is just a pre-history of the person. So, it is important to have an analytical system with AI models, and which can predict the situation but human police to analyse the scenario and act with all legal compliance with constitutional provisions.

XVII. CONCLUSION

The technological move from reactive to proactive police is not just an update of tools; it is a change in the core philosophy of public safety and the relationship between the state and the citizen. The varying state-to-state adoption of policing strategies in India demonstrates that while technology can enhance law enforcement and public safety, the absence of a uniform legal and regulatory framework results in uneven implementation, a spectrum of accountability measures, and inconsistent protection of citizens' privacy and fundamental rights. The potential benefits for crime prevention are too great to dismiss, but at the same time the risks for fundamental rights and democratic ideals are too serious to ignore. India is at a crossroad. The course it selects will determine its character as a nation for decades to come. Will it adopt a regime of widespread surveillance that strips away the basic rights of freedom and equality of its people, or will it forge a new cautious preventative path that takes advantage of technology but protects the fundamental rights of its people?

This isn't a choice between safety and liberty. It's about establishing a system that delivers both. This calls for not only investment in technology, but fundamental foresight legal, political and ethical. It necessitates a new social contract for policing, one that is written not in code but in law and governed not by the cold logic of algorithms but the everlasting principles of justice, liberty, equality and fraternity entrenched in our Constitution. The future of Indian law enforcement must be not simply smart but also just. The challenge we face is to make sure that in our drive for a digital shield, we don't create digital shackles.

Criminology is not apples to apples comparison. It has to be connected with purpose and act with an injury.

Knowledge and purpose play a significant role in criminology which demands inquiry and critical analytical abilities to grasp mens rea and actus reus to drive to the conclusion. Natural justice does not permit $1 + 1 = 2$. AI based on a predefined algorithm may not deliver natural justice as the police may use their authority and the data to pinpoint the innocents. Therefore, the trained police expertise is vital after the AI tool gives prognosis.

REFERENCES

- [1] S. Awasthi, "China's Social Credit System and Information Control Regime," Observer Research Foundation (ORF), Jan. 3, 2026. [Online]. Available: <https://www.orfonline.org/expert-speak/china-s-social-credit-system-and-information-control-regime>
- [2] J. Bhuiyan, "LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws," The Guardian, Nov. 8, 2021. [Online]. Available: <https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform>
- [3] L. Citrome, "Artificial intelligence and the potential for garbage in, garbage out," Current Medical Research and Opinion, vol. 40, no. 1, pp. 1–2, 2024, doi: 10.1080/03007995.2023.2286785.
- [4] Crime and Criminal Tracking Network & Systems (CCTNS), "About Us." [Online]. Available: <https://digitalpolice.gov.in/DigitalPolice/AboutUs>
- [5] M. A. Dakalbab, O. A. Talib, A. B. Waraga, A. B. Nassif, S. Abbas, and Q. Nasir, "Artificial intelligence and crime prediction: A systematic literature review," Social Sciences & Humanities Open, vol. 6, no. 1, Art. no. 100342, 2022.
- [6] A. Jain, "National Automated Facial Recognition System," Panoptic, Jul. 18, 2026. [Online]. Available: <https://panoptic.in/case-study/ncrbs-national-automated-facial-recognition-system>
- [7] L. Jany, "Researchers use AI to predict crime, biased policing in major U.S. cities like L.A.," Los Angeles Times, Jul. 4, 2022. [Online]. Available: <https://www.latimes.com/california/story/2022->

07-04/researchers-use-ai-to-predict-crime-biased-policing

- [8] J. Angwin, J. Larson, S. Mattu, and L. Kirchner, "Machine Bias," ProPublica, May 23, 2016. [Online]. Available: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
- [9] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., (2017) 10 SCC 1, Supreme Court of India, 2017.
- [10] S. Kava, "Explained: Delhi Police's AI surveillance network and why it's under scrutiny," The News Minute, Jul. 23, 2026. [Online]. Available: <https://www.thenewsminute.com/news/explained-delhi-polices-ai-surveillance-network-and-why-its-under-scrutiny>
- [11] N. Z. Mahmud, "CrimeCast: A crime prediction and strategy direction service," in Proc. 19th Int. Conf. Computer and Information Technology (ICCIT), 2016, pp. 414–418.
- [12] West Yorkshire Police, "National Data Analytics Solution (NDAS) Privacy Notice." [Online]. Available: <https://www.westyorkshire.police.uk/advice/modern-slavery/national-data-analytics-solution-ndas-privacy-notice>
- [13] I. Raji et al., "Predictive policing: The role of AI in crime prevention," International Journal of Computer Applications Technology and Research, 2024.
- [14] S. Chauhan and S. P., "The use of Geographic Information System (GIS) in predictive policing," International Journal of Innovative Research in Technology, pp. 999–1005, 2025.
- [15] H. Thacker, "How Mumbai Police are using technology to prevent crime," The CSR Journal, Apr. 17, 2025. [Online]. Available: <https://thecsrjournal.in/mumbai-police-artificial-intelligence-ai-technology-prevent-crime/>