PREDICTIVE POLICING AND ITS INTEGRATION WITH ARTIFICIAL INTELLIGENCE: LEGAL AND ETHICAL CONSTRAINTS IN A DATA-DRIVEN AGE

Shreyas Ranjit & Ziya Rakhanji, BBA LLB (Hons), University of Mumbai Law Academy

ABSTRACT

Predictive policing in modern times involves using algorithms to analyse large amounts of datasets in order to predict and help prevent potential future crimes. The rise of artificial intelligence (AI) has immensely transformed law enforcement with Predictive policing being one of the most commonly used methods that utilize artificial intelligence. Predictive policing uses AI to scan large datasets and produce predictions regarding possible crime locations, timing, and potential criminals, thereby increasing preventive efforts and resource allocation. The method is, however, marred by ethics and social issues. Concerns like privacy invasion, algorithmic bias, and the absence of responsibility in automated systems mandate cautious examination. This paper explores the emergence and scope of predictive policing, the ethical and social consequences of its application, and the differing approaches adopted by various countries with a special emphasis on India. Recommendations emphasize ethical frameworks, transparency, and regulatory mechanisms to mitigate the risks of predictive policing and ensure it is aligned with civil rights and societal interests.

Introduction

With today's data heavy world, police departments around the world are shifting towards artificial intelligence (AI) to revolutionize conventional policing practices into proactive, data-heavy strategies. Predictive policing, or the use of data analytics and machine learning algorithms to anticipate where and when crime is most likely to occur, becomes a significant technology in this change. This transformation from reactive to preventive policing is not only technological but also a fundamental change in policing philosophy. As emphasized at the 2009 Predictive Policing Symposium held by the U.S. National Institute of Justice (NIJ), this paradigm draws upon successful methods like problem oriented policing, intelligence-led policing, community policing, and evidence-based enforcement and integrates them under a common structure fueled by data and algorithms. The main appeal of predictive policing comes from its potential to maximize resource allocation, minimize response times, and detect new crime patterns that could escape conventional approaches. Substantial outcomes have been achieved recently, the Virginia Richmond police, for instance, applied historical crime data to forecast celebratory gu1nfire on New Year's Eve in 2003. The analytical approach resulted in a 47% reduction in random gunfire and a 246% rise in gun seizures, and $15,000 in personnel expenses avoided a success described as a hallmark of predictive models.[1]

The basic strategy of predictive policing employs historical and statistical data to calculate the likelihood of future crime in specific geographic locations. It is based on the premise of applying software that categorizes regions or groups based on patterns of crime in a manner that police can focus observation and patrols on high-risk locations. Predictive policing does not substitute the traditional models of policing but complements them with the addition of algorithmic precision to traditional practices such as hot spot policing and intelligence led policing. [2]

But, while promising in terms of strategy, predictive policing has become a point of contention between academia and civil liberties organizations. This amalgamation of big data also raises fundamental questions of constitutional viability in India. These methods implicate the right to privacy and personal liberty under Article 21, right to equality under Article 14, and freedoms

[1] Beth Pearsall, Predictive Policing: The Future of Law Enforcement?, NAT'L INST. JUST. J., No. 266, at 16 (2010)
[2] Jerry H. Ratcliffe et al., The Philadelphia Predictive Policing Experiment, 17 J. EXP. CRIMINOLOGY 15 (2021).

under Article 19 (speech and association, etc.). In ***Justice K.S. Puttaswamy v. Union of India***[3], the Supreme Court established privacy as an aspect of Article 21 and held that any invasion of privacy must be supported by law and be necessary and proportionate. Likewise, discriminatory predictive models disproportionately targeting minorities may infringe Article 14's equality before the law. Describing predictive policing in legal terms, we then need to ask: When and how can the state use algorithmic surveillance without vitiating fundamental rights? As predictive policing increasingly divorces itself from criminological theory and instead relies on computational correlations, critics contend that it threatens to oversimplify criminality. Researchers like Kitchin (2014) and Vlahos (2012) warn that predictive models pay little attention to the underlying socio political and economic context, and thus end up giving a reductionist and potentially skewed representation of society. When context is removed from policing models, the risk of reinforcing stereotypes and structural inequalities increases, especially in racially or economically marginalized communities.[4]

Innes, Fielding, and Cope (2005) also mention that while the technical advanced nature of AI technology can be seen to create an illusion of objectivity, the technology itself tends to conceal embedded biases within the data on which it is operating.[5] These are particularly pertinent in countries like India and the United States, where traditionally there have been deep seated variations in policing styles that are replicated in the datasets upon which predictive models operate. The feedback loop of ongoing policing of the same areas can result in distorted representations of criminality and erosion of public trust in law enforcement agencies.

To critically evaluate the validity of such claims, a PRISMA based literature review was conducted to review systematically the dominant empirical literature on the effectiveness of predictive policing.[6] The review, as referenced in the literature, revealed that although some applications of predictive policing hold much promise for the war on crime, the technique is not yet founded on a solid, stable empirical foundation. The majority of research fails to control the effect of predictive technology compared to general policing practice or is plagued by methodological issues. Additionally, the Thomson Reuters review of predictive policing

[3] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[4] Lyria Bennett Moses & Janet Chan, Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability, 28 Policing & Soc'y 806 (2016), https://doi.org/10.1080/10439463.2016.1253695
[5] Friedman, B., and Nissenbaum, H. (1996). Bias in computer systems. ACM Transactions on Information Systems, 14(3), 330-347. https://doi.org/10.1145/230538.230561
[6] Meijer, A., and Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. International Journal of Public Administration, 42(12), 1031-1039. https://doi.org/10.1080/01900692.2019.1575664

distinguishes among three basic paradigms ie place based, person-based, and group-based prediction.[7] Place based models identify hot spots on the basis of geographically localized information. Person based models examine individuals' risk levels on the basis of prior behavior and demographic information. Group based models examine social networks to predict the criminal behavior of gangs or aggregates. Each of the three is impressive in its own right, but also exhibits different types of ethical risk, in this case more notably privacy rights and discriminatory profiling. Predictive policing must not be reduced to a technical fix for the intricate social issues that lead to crime. Preventing crime is not merely computational precision, but it needs legal safeguards, social engagement, and equitable governance.

In India, the application of AI in policing via instruments such as Delhi's CMAPS and Telangana's facial recognition systems has developed in the absence of robust data protection laws.[8] Without explicit legislation, effective oversight mechanisms, and transparency of algorithmic choices, predictive policing can become an unregulated force, trampling over basic rights and deepening social biases.

Thus, this paper argues that the central question is not whether predictive policing can be effective in the limiting, short term sense, but whether it can be effective justly, fairly, and democratically. Are such systems feasible within a policing model that honours civil liberties and human rights? Can technology be used to build and not undermine public trust? Based on an intensive and multidisciplinary examination, this research delves into the operational mechanisms, juridical concerns, and moral dilemmas of predictive policing in international and Indian contexts. In so doing, it aims to add to the debate surrounding AI in policing, highlighting both the potential and the risk of 21st century predictive policing. With increasing use of predictive technology, rigorous examination, open government, and evidence-based practice becomes not just desirable but imperative.

Legal Vacuum and the Need for Statutory Framework in India

Predictive policing is also in its nascent stages in India, with only a few reported pilot projects. Bengaluru (Karnataka) Police have begun to use AI-based mapping technology: their platform processes FIR data and emergency-call locations (e.g. from the 112 helpline) to create crime

[7] Thomson Reuters, Technology Fuels New Advances and Challenges in Predictive Policing (Mar. 2013), https://www.naco.org/sites/default/files/documents/Technology%20Fuels%20new.pdf
[8] Marda, V., and Narayan, S. (2020). Data in new Delhi's predictive policing system. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 317-324. https://doi.org/10.1145/3351095.3372865

heatmaps and alarms. By identifying risk areas through these predictions, Bangalore police can deploy patrols (strategicallydeccanherald.com). Karnataka state also rolled out an AI platform named KSP.AI (built in association with Capulus Technologies). The system is said to utilize sophisticated machine-learning models (even a "GPT" language model) to process diverse data (crime records, incident trends, etc.) for crime prevention and optimal resource (allocationlinkedin.com). Officials claim KSP.AI will enable "data-driven analysis, streamlined investigations, and advanced case analysis" for enhanced public safety.

Other Indian jurisdictions are trying out analytic tools as well. Delhi Police have initiated projects encompassing AI and data analytics for prevention of crime (e.g. crime pattern analysis to inform patrol planning) (newmediacomm.com). Hyderabad and Chennai are also piloting predictive-analytics programs, acknowledging AI tools could help address rapid urbanization challengesnewmediacomm.com. So far, these initiatives are still in their infancy – India's CCTNS (Crime & Criminal Tracking Network) constructs integrated crime databases at the national level, but routine predictive models have not yet been widely adopted. More significantly, Indian projects need to be capable of being scaled to local context considering the gaps in data, privacy norms, and the threat of bias (e.g. geographically or by community) are persistent challenges (newmediacomm.com). Overall, India's first experiments (Bangalore's hot-spot mapping, Karnataka's KSP.AI[9], Delhi's analytical pilots) indicate the growing interest in predictive policing, though there are limited published findings on their effectiveness. India's use of AI to policing, most prominently through predictive policing, indicates a readiness to adopt new approaches to crime prevention. Projects like the Delhi Crime Mapping, Analytics, and Predictive System (CMAPS)[10], and predictive tools being developed in Jharkhand, Telangana, and Maharashtra, indicate this growing development.

But these transformations are taking place in a de facto legal void. As the analysis states, "there is no specific law governing predictive policing in India" (lawfullegal.in). The sole check at present are the general guarantees of the Constitution. As Article 21 states, in the wake of the Puttaswamy judgment, any encroachment on privacy has to be based upon a valid statute, which hitherto does not exist for algorithmic profiling (dlapiperdataprotection.com). India did

[9] AI to Aid Karnataka Cops Analyse Cases, Deccan Herald (July 15, 2024) https://www.deccanherald.com/india/karnataka/ai-to-aid-karnataka-cops-analyse-cases-2860302.
[10] Comptroller & Auditor Gen. of India, Digital Initiatives of Delhi Police (2020), https://cag.gov.in/uploads/download_audit_report/2020/9.%20Digital%20Initiatives%20of%20Delhi%20Police-05f911198e45a25.81448827.pdf.

not even have a specific personal data law up until 2023. That is now altered by the Digital Personal Data Protection Act, 2023[11], just passed by Parliament. The new Act, once brought into force, will regulate digital personal data collection and processing. It enshrines necessity, data minimisation, and security principles, similar to privacy rights. But the implementation is yet to be seen: significant sections and provisions of the Act are yet to be notified. Furthermore, the Act covers only personal digital data hence the vast majority of police databases (e.g. watchlists, CCTV footage) may be outside its scope. Thus, despite this legislative action, India still does not possess a general regime of law on predictive policing.

Simultaneously, other legislations have piecemeal regulations and control. Code of Criminal Procedure Chapter VIII (Sections 151-160) permits preventive detentions, but the courts insist on such detentions being backed with concrete evidence and strict procedural requirements. Predictive predictions short of the "reasonable satisfaction" test laid down in judgments such as ***Joginder Kumar v. State of U.P. (1994)*** [12]would be insufficient. The Telegraph Act (as in ***PUCL v. Union of India***[13]) and other surveillance acts have judicial controls (telephone tapping is warrant-based, etc.). These judgments seem to infer that just as in any bulk automated surveillance, any such similar large-scale automated surveillance must have regulatory controls.

India's existing legal framework is not algorithmic policing-friendly. Practice is reduced to piecemeal executive diktat, with no statutory framework for supervision, transparency, and remedies. This was habitually disapproved by the courts, until the new Data Protection regime is firmly in place (rules and enforcement), predictive policing is mostly unregulated. Courts have warned that "unchecked" systems could infringe constitutional privacy and liberty, experts thus call for immediate legislation: data protection rules, procedural safeguards (warrants, audits), and independent review mechanisms so that predictive tools are brought in line with constitutional values

India's attempts at predictive policing are, nevertheless, thwarted by its own inherent limitations founded on socio-economic diversity, infrastructural variations, and poor regulatory systems. India's technology infrastructure and network vary significantly, with cities such as

[11] Government of India, The Digital Personal Data Protection Act, 2023 (June 2024), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf.
[12] Joginder Kumar v. State of U.P. (1994) AIR 1994 SUPREME COURT 1349
[13] PUCL v. Union of India AIR1997 SC 568

Delhi, Mumbai, and Bengaluru sporting sophisticated AI systems, while rural areas lack the ability to apply digital policing. This variation affects data quality and consistency required for some predictions. Delhi's CMAPS [14]system, for instance, based on past patterns of crime to predict high-crime hotspots, has effectively optimized metropolitan police deployment. Data collection in areas with poor infrastructure may be partial, and this may compromise the system. This is the prime example of the fact that India's cultural and socio-economic diversity presents special challenges to AI policing. Such data is biased by social factors, and AI models trained on such data can only enhance surveillance of marginal communities. Jharkhand's partnership with the National Informatics Centre (NIC) is a case in point, Jharkhand's predictive policing system integrates information from police records, social welfare services, and public infrastructure, and while it enhances detection of crime, it is contended by critics that it disproportionately targets economically marginalized and tribal communities.[15] The threat of discriminatory profiling, wherein communities are subjected to greater surveillance on the grounds of social bias in the data, erodes trust in the police and can further reinforce social inequalities.

India's predictive policing networks are vulnerable to excessive surveillance, The smart surveillance initiative of Telangana is one such example. Telangana state police use live video analytics together with a massive facial recognition network to identify and follow individuals across Hyderabad.[16] Whereas its easy for real-time identification, the lack of transparency in how the system processes data makes it a privacy concern, with citizens feeling they are being watched without notice or sanction. Not only does the unregulated surveillance invade privacy, but it can have the effect of fostering a culture in which citizens feel they are constantly being watched, impacting individual freedoms.

Platformization and Data Collection World Wide

The **platformization** of various police work marks a significant and drastic shift in how law enforcement approaches data collection and analysis. Traditionally, police departments operated with data which was only confined to their internal databases and it relied primarily

[14] Supra Note no 8
[15] Prabhu Chawla, Making a Case for Futuristic Predictive Policing in India, New Indian Express (Sept. 9, 2012), https://www.newindianexpress.com/magazine/voices/2012/Sep/09/making-a-case-for-futuristic-predictive-policing-in-india-404220.html.
[16] Anushka Jain, Facial Recognition in Telangana: A Surveillance State in the Making?, Internet Freedom Foundation (Dec. 8, 2020), https://internetfreedom.in/facial-recognition-in-telangana-a-surveillance-state-in-the-making/.

on local information to solve various crimes. However, as seen with the adoption of systems like PRECOBS (Pre Crime Observation System) in German-speaking countries which is used to forecast the commitment of "near repeat crimes" using algorithms and knowledge about crimes committed in the past, it evident that predictive policing is transitioning toward integrated, multi-platform systems that merge data from various sources. [17]This shift enables police forces to calculate and analyze large, multifaceted datasets simultaneously, extending far beyond traditional crime reports to include external databases, social media, geospatial data, and other public and private data sources.

Integrated Data Platforms and Predictive Policing

Predictive policing systems which are platform based enable law enforcement agencies to carry out more advanced analytical functions. By combining datasets from various sources, the platforms enable the merger of information in different domains, providing a single, unified view of criminal networks, social affiliations, and behavior patterns. Police departments, for instance, are able to monitor social network affiliations in order to detect future gang members or analyze social media interactions to detect dangerous behavior patterns. This multi-dimensional approach empowers law enforcement to go beyond mere crime prediction and delve into predictive social analyses that anticipate how, when, and why certain individuals or groups may be involved in criminal activities.

The **PRECOBS (Pre Crime Observation System)** platform in Germany exemplifies this evolution. Originally developed to forecast property offenses, PRECOBS has grown to encompass wider crime information and social context, enabling police to forecast hotspots of crime with increased accuracy. Further, as police departments collect and cross-check information from varied sources, their forecasting is now extended to other domains of public safety, for example, following known offenders across jurisdictions, assessing the mobility habits of high-risk offenders, or identifying indicators of growing violence among social groups.[18]

The trend of platformization is also echoed in global models, such as Palantir's Gotham platform in the USA, which aggregates several sources of data to assist police in mapping and

[17] Anna Biselli, Predictive Policing: PRECOBS and the Spread of Preemptive Surveillance, **Netzpolitik.org** (Feb. 1, 2019), https://netzpolitik.org/2019/predictive-policing-precobs-and-the-spread-of-preemptive-surveillance/
[18] ibid

analyzing crime[19]. Palantir's platform has allowed various different agencies like the Los Angeles Police Department (LAPD) to transition to an all-encompassing, data-based strategy where data from criminal histories, social services, and even utility billing records can be cross-checked to generate usable intelligence. Through the application of AI to integrate disparate streams of data, law enforcement agencies can conduct analytics across organizational silos and identify patterns of crime that would otherwise have been hard or impossible to identify using conventional methods. Modern predictive policing is based on the fusion of multiple data sets. Police departments increasingly construct centralized platforms and fusion centers to bring together records, sensor feeds, and analysis tools. A U.S. National Institute of Justice study observed that "the success of predictive policing will all come down to…how different information sources are integrated and how all the data are analyzed". Police therefore connect traditional crime reports with nontraditional data (e.g. health records, social services, land-use) to get a "holistic" view of community risk. For example, one police chief noted that integrating health, school, and land-use data can improve crime-fighting strategies[20].

Fusion Centers & Real-Time Crime Centers: Many countries now operate 24/7 crime centers that onbaord live data streams into unified dashboards. In the U.S., dozens of "Real-Time Crime Centers" consolidate traffic cameras, gunshot detectors, license-plate readers, emergency calls, and other feeds on one platform. Commercial systems like Fusus provide this integration: they merge videos with automatic license-plate readers, gunfire sensors, and CAD alerts so operators can monitor public safety in real time.[21]

Big-Data Analytics Platforms: Vendors offer turnkey data-integration suites. Notably, Palantir's Gotham (used by many U.S. and foreign agencies) claims to "integrate and transform" [22]disparate data into a single coherent asset. An analysis by defense researchers notes Palantir promotes itself as a "data integration and analysis platform" (not explicitly as "predictive policing") underlying how agencies reuse its tools for joint analytics. Europol and Interpol, for example, encourage member countries to feed intelligence databases (crime stats,

[19] See Palantir Technologies, Gotham: Intelligence-Led Investigations, https://www.palantir.com/platforms/gotham/
[20] Beth Pearsall, Predictive Policing: The Future of Law Enforcement?, NIJ J. No. 266, June 2010, at 16–19, https://www.ojp.gov/pdffiles1/nij/230414.pdf.
[21] Colin Wood, Police Real-Time Crime Centers Are Becoming Data Powerhouses, StateScoop (Aug. 24, 2023), https://statescoop.com/real-time-crime-centers-police-privacy
[22] Supra note no 18

travel data, communication intercepts) into multi-country platforms for advanced analysis.[23]

Smart City / Safe City Programs: In many nations, policing is tied to broader "smart city" surveillance initiatives. By 2019, at least 56 countries had deployed AI in Safe City platforms, linking cameras and IoT devices for public safety.[24] Singapore's *PolCam* is a prime example: over 90,000 street cameras feed into the police's Operations Command Centre, enhancing situational awareness. [25] Shanghai, London, Johannesburg and others have similar networks. These integrated systems allow data-driven dispatch (alerting officers to emerging problems) and pattern detection that inform predictive models.

Case Study – Rio de Janeiro CrimeRadar: In Rio, the NGO Igarapé Institute developed *CrimeRadar*, a public-facing predictive app. It fuses Rio's crime report database into an interactive map, producing forecasts of crime likelihood by time and location igarape.org.br. Police and citizens can see "safety levels" on the map and plan accordingly. Reportedly, CrimeRadar helped the Rio police deploy patrols more effectively – for example, by enabling them "to avoid crime by predicting it before it happens". [26]This kind of city-wide data platform (even if open to the public) exemplifies how integrated data use can make policing more proactive.

Ethical and Social Challenges

a. Algorithmic Bias

One of the most challenging task that predictive policing faces is algorithmic bias. Predictive models are trained with historical crime data, and such data can be skewed by the past policing practice that tended to concentrate disproportionately on specific communities. Consequently, AI systems become adept at sustaining and entrenching biases, particularly against minority groups. A study of predictive policing in Chicago determined that Black and Latino

[23] Europol, AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement (Publications Office of the European Union, Luxembourg, 2024), https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf.
[24] Deloitte, Surveillance and Predictive Policing Through AI, Urban Future with a Purpose, (Global Government & Public Services) (2024), https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html
[25] Police Life: The Watchful Protectors, SPF (Dec. 12, 2023), https://www.police.gov.sg/Media-Room/Police-Life/2023/12/The-Watchful-Protectors.
[26] Katherine Aguirre, Emile Badran & Robert Muggah, Crime Prediction for More Agile Policing in Cities – Rio de Janeiro, Brazil, U4SSC Case Study (Oct. 2019), https://igarape.org.br/wp-content/uploads/2019/10/460154_Case-study-Crime-prediction-for-more-agile-policing-in-cities.pdf.

communities were disproportionately characterized as high-crime communities based on predictive policing, leading to increased surveillance and police presence among these communities. This not only undermines the legitimacy of predictive policing but also expands on current social inequalities. Predictive policing technology can reinforce discriminatory behavior by hiding it behind a smokescreen of mathematical objectivity.. The historical crime records employed by these algorithms represent not who is more likely to be criminal, but rather who gets more frequently targeted by the police. Members from minority religions and lower castes tend to get more scrutinized by the police even when there is obvious evidence of innocence.[27] A case in point is ***Ankush Maruti Shinde v. State of Maharashtra***[28], where six men from the marginalized Paradhi community endured sixteen years on death row in solitary confinement before the Supreme Court of India finally acquitted them. The police initially deemed them guilty based on their community, ignoring an eyewitness identification of four other individuals as the actual perpetrators.

Data reflecting bias in the Indian criminal justice system further substantiates this issue, Dalits, and Adivasi communities that are particularly vulnerable comprise over half of the undertrial prison population, despite accounting for only 39% of the total population[29]. Predictive policing tools often mirror these biases. In the United States, mathematicians have called on their peers to reject work on predictive policing systems due to concerns that these algorithms perpetuate racial bias [30]. In particular, structural racism results in African-Americans being disproportionately policed compared to white individuals[31], which then skews crime data used by predictive algorithms. This creates a harmful cycle which creates a situation where more a particular group is policed, the more the algorithm identifies that group as likely offenders, leading to further policing of the same group.

b. Privacy Concerns

The data-intensive character of predictive policing poses serious privacy concerns, since AI

[27] Rashida Richardson, Jason M. Schultz & Kate Crawford, Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, 94 N.Y.U. L. Rev. Online 192 (2019), https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson_etal-FIN.pdf.
[28] Ankush Maruti Shinde v. State of Maharashtra AIRONLINE 2019 SC 492
[29] Thakur, A., & Nagarajan, R., Why Minorities Have a Major Presence in Prisons, Times of India (2020), https://timesofindia.indiatimes.com/india/in-a-minority-but-a-major-presence-in-our-prisons/articleshow/73266299.cms.
[30] Predictive Policing Algorithms Are Racist. They Need to Be Dismantled., MIT Technology Review (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/
[31] Supra note no 26

systems tend to handle lots of personal data with minimal protections. Monitoring technologies such as facial recognition are especially intrusive, as they harvest intimate biometric information that can be misused so readily. Additionally, the cross-linking of databases within platformized policing environments reduces the privacy of the individual even further, as it is hard for citizens to understand what is happening to their data and how it is being shared.

Since predictive policing models are based on vast amounts of personal data, their effect on the right to privacy needs to be addressed. Opaque processing of such data is a violation of privacy as defined under the judgment of ***Justice K.S. Puttaswamy (Retd.) v. Union of India*** [32], which laid down the 'proportionality and legitimacy test.' The test demands four conditions to be satisfied for the state to legally invade privacy rights:

1. The action must be backed by law.

2. The action must be necessary in a democratic society to achieve a legitimate aim, such as reducing crime.

3. The degree of interference must be proportionate to its purpose.

4. There must be procedural safeguards to prevent misuse.

At present, the first requirement is not fulfilled, since there is no direct legislation controlling the application of predictive policing algorithms. Furthermore, the absence of transparency owing to law enforcement exemptions under the Right to Information Act, 2005, keeps the algorithms from being open to public scrutiny, which is believed by many to be no more than state surveillance in the guise of internal security. This issue is with increased seriousness argued by the projected merger of India's National Security Grid (NATGRID) with the private information of citizens, such as bank information (The Hindu, 2020)[33]. Additionally, risks to data security are high, as highlighted by the recent hacking of Maharashtra's Criminal Investigation Department's website.[34]

[32] Justice K.S. Puttaswamy (Retd.) v. Union of India ((2017) 10 SCC 1)
[33] National Intelligence Grid to Be Ready by Early 2020, India Today (Updated Feb. 8, 2022), https://www.indiatoday.in/india/story/national-intelligence-grid-to-be-ready-by-early-2020-1601949-2019-09-22
[34] Maharashtra CID Website Hacked, Defaced, The Hindu (Mar. 8, 2020), https://www.thehindu.com/news/cities/mumbai/maharashtra-cid-website-hacked-defaced/article31005341.ece.

The second of these criteria, however, is equally questionable since predictive policing has been demonstrated to be ineffective and discriminatory, and there are more sustainable ways of decreasing crime. [35]Last but not least, the lack of procedural safeguards implies that criterion four is also not met.

c. Accountability and Transparency

One of the inherent limitations of predictive policing is that AI decision-making is non-transparent. Predictive algorithms are essentially black boxes, and therefore law enforcement agencies and the public cannot see and interpret the processes that lead to specific predictions. Lack of transparency creates an accountability gap because the targeted individuals cannot challenge the output of the AI or law enforcement agencies for biased results. Furthermore, the "black box" nature of the algorithm also keeps officers in the dark and from challenging the results.[36]

Black box nature of such algorithms is objectionable on a number of grounds. One it creates a gap for lack of accountability because the concerned persons or groups of persons are not in a position to question or probe the output of the AI even when the output directly impacts their rights and freedoms. For example, if a predictive policing algorithm flags some persons or locations as high-risk on unclear grounds, the persons or groups are most likely to be subjected to enhanced scrutiny or priority police attention without even being aware of grounds of such attention. Such a lack of transparency denies persons the right to contest potentially wrong or discriminatory decisions made with no appeal.

In addition, the question of transparency is not in the interests of law enforcement officers, who may be relying on the outputs of the AI without understanding or questioning the data and assumptions on which the predictions are based. Relying on AI-generated insights may lead officers to over-rely on the technology at the cost of their ability to make independent and context-dependent judgments. If AI-informed predictions are applied without critical analysis, there is the possibility that law enforcement practice will become increasingly reliant on faulty data, reinforcing biases in existing crime data, and diminishing contextual or situational

[35] Ramachandran Murugesan, *Predictive Policing in India: Deterring Crime or Discriminating Minorities?*, LSE Human Rights Blog (Apr. 16, 2021),
[36] Supra note no 26

considerations that a human officer would otherwise detect.

In addition, proprietary algorithms employed in predictive policing technology will likely employ complex machine learning techniques that are hard even for technically savvy people to decipher. Sophistication also dissuades effective scrutiny because police departments might lack expert capacity to effectively audit the algorithms. There is little assurance, then, that AI technologies employed by law enforcement are objective and equitable. Scholars have pointed out the need for "explainable AI" in high-stakes applications such as law enforcement, where decisions have important social and ethical implications

Recommendations:

1. Ethical Frameworks and Oversight Mechanisms

To prevent ethical issues in predictive policing, a systematic ethical framework is needed. This must lead to transparency, accountability, equity, and compliance with human rights principles. Ethical guidelines for AI should require explainability of algorithms so people affected by predictions can see and question the reasons behind them. This may include making interpretable machine learning models part of the algorithm, which provide insight into data points and assumptions used to make each prediction.

In addition, creating AI ethics boards within police forces may offer another level of scrutiny. The boards, made up of ethicists, technologists, and members of the community, would be charged with reviewing the ethical effects of AI usage. Ongoing reviews and audits by such boards can ensure predictive policing is consistent with ethical guidelines and any emerging ethical concerns are resolved in advance. Such a system might also include whistleblower protections, to empower officers and technologists in agencies to report ethical issues without being afraid of retribution.

2. Legislative Reforms and Regulatory Measures

Strong legislative control is central to managing the application of AI in policing. In order to safeguard the privacy of citizens and preserve democratic values, legislatures must enact legislation for regulating data collection, usage, and retention in predictive policing. Such legislation must incorporate principles like necessity and proportionality, whereby data that is gathered is restricted to that necessary for certain policing requirements and law enforcement

measures are weighed against individual rights.

Privacy regulations similar to Europe's General Data Protection Regulation (GDPR) may establish strict standards for collecting and processing personal data, compelling law enforcement agencies to reveal their sources of data, their methods of processing, and the purposes for which their predictive policing outputs will be used. Such regulations may also impose penalties for failing to comply, thus making agencies watchful in maintaining data privacy and protecting citizens' rights to privacy. Additionally, there should be law requiring human intervention in automated decisions to avoid AI-based projections being used for punitive purposes without human oversight.

3. Community Involvement and Transparency Initiatives

Establishing public confidence in predictive policing requires active public involvement and openness. Police organizations should have community oversight panels with members drawn from local communities, civil rights organizations, and data privacy organizations. The panels could engage in considering predictive policing practices and providing input on community concerns. Through public involvement in oversight, the police can gain trust and ensure that predictive policing practices are shaped by community values.

Transparency efforts, including releasing regular reports, can further uncloud predictive policing. The reports must specify the kinds of data being gathered, the frequency of predictive policing deployment, and the observed outcomes in targeted areas. Public availability of information regarding how data is processed and utilized will enable communities to speak out against their concerns and hold law enforcement accountable. Moreover, public discussions regarding the social and ethical implications of predictive policing can yield insightful feedback, enabling law enforcement agencies to improve their practices in accordance with societal demands.

4. Bias Mitigation and Fairness in Algorithm Design

Since predictive policing algorithms have the potential to contribute to existing biases unintentionally, AI designers need to consider bias mitigation strategies during algorithmic training and testing cycles. Data re-weighting of inputs to minimize disproportionate weight on historically biased variables and adoption of representative datasets from multiple

populations can assist in generating more unbiased, accurate predictions. In addition, agencies must perform regular audits of predictive policing algorithms to detect and resolve instances of bias, making sure that these systems run without discriminatory results.

Besides, developers can introduce fairness constraints into algorithms to adjust for known differences, preventing predictive outputs from disproportionally targeting or over-policing certain communities. Establishing transparent audit mechanisms, such as internal and third-party examinations, can verify the fairness of these algorithms and build greater public trust. Working with independent research centers and civil rights groups can additionally enhance the ethical value of AI-based policing instruments by enabling outside examination and advice.

5. Strengthening Data Security and Safeguarding Privacy

Data protection forms the backbone of ethical predictive policing, given the sensitive character of the data involved. This makes it prone to violations and abuse. Advanced law enforcers are expected to deploy sophisticated encryption methods to safeguard data throughout the process—collection and storage, processing, and analysis. Security audits conducted on a regular basis will help determine and resolve vulnerabilities, while access controls can restrict data to authorized personnel alone.

Adopting data minimization principles which include gathering only what is needed for particular predictions can also protect privacy. Agencies must be compelled to develop and stick to clear guidelines on data retention such that personal data is stored only for so long as it is needed for particular policing purposes. Further, embracing anonymization and data masking methods wherever feasible can minimize the possibility of revealing individuals' identities, shielding their privacy even under predictive policing paradigms.

6. Encouraging Ethical AI Development and Collaboration

A morally and ethically sound method of AI development in policing is through cooperation among law enforcement, tech developers, academic researchers, and civil rights groups. Building cross-disciplinary collaborations can enable knowledge-sharing about best practices, minimizing bias, and privacy safeguards. It can also help in developing predictive tools informed by the community. Open-source development of AI where possible can also lead to accountability since open-source algorithms can be reviewed and scrutinized by the public,

allowing experts and communities to recommend improvements.

In addition, standards of industry for responsible AI development could be adopted, providing criteria for transparency, impartiality, and data protection that must be achieved by AI developers prior to their technology deployment in law enforcement. These standards can be enforced through a separate regulatory commission that monitors AI use in police work to ensure that ethical principles are applied everywhere and that agencies are provided with recommendations for the adoption of responsible AI principles.

Conclusion

Predictive policing provides a revolutionary new method of crime prevention, utilizing the analytical capability of artificial intelligence to predict criminal behavior, recognize patterns, and allocate law enforcement assets for maximum impact. It represents a revolutionary departure from reactive policing models to proactive data-driven policing. But such transformation comes at a cost. The use of predictive technologies in policing has created a nexus of interconnected legal, ethical, and societal issues—most importantly related to privacy, algorithmic bias, discrimination, due process, and democratic accountability.

India's experience with predictive policing reflects both the promise and the peril of technological advancement in law enforcement. While initiatives such as Delhi's CMAPS and Karnataka's KSP.AI underscore a growing institutional interest in algorithm-driven policing, their implementation remains marred by infrastructural disparities, lack of legal backing, and the absence of transparent accountability mechanisms. Additionally, in a society that is characterized by economic and social disparity, the utilization of historically prejudiced data sets in AI systems threatens to amplify prevailing prejudices against underprivileged groups, thus accelerating systemic discrimination in the name of objective technology.

The constitutional impact of predictive policing is significant. The Indian Supreme Court's acknowledgment of the right to privacy in ***Justice K.S. Puttaswamy v. Union of India***[37] places an explicit requirement that any incursion into private life must meet the tests of legality, necessity, proportionality, and procedural safeguards. At present, the predictive policing frameworks in India are deficient on several counts they are not supported by clear statutory

[37] Supra note no 31

provisions, are non-transparent, and do not provide any substantial redressal mechanisms. The Digital Personal Data Protection Act, 2023, although a positive step, is yet in the nascent stage and does not offer a comprehensive regulatory cover to AI-based policing practices, particularly those entailing surveillance, profiling, and biometric data.

Internationally, the experiences of other nations such as the United States, Germany, and Brazil provide valuable lessons. In the United States, predictive policing has under fire for unfairly targeting African-American and Latino communities, whereas in Europe, like PRECOBS, try to counteract these risks through transparency and regulation. Yet even in more advanced legal environments, predictive policing is controversial, highlighting that technology alone cannot be a solution to complex social problems. Rather, it has to be supplemented with a robust legal framework, autonomous monitoring, and democratic accountability. To harness the benefits of predictive policing while preserving the rule of law and civil liberties, it is essential to adopt a **multi-faceted and interdisciplinary approach**. This includes the establishment of robust ethical frameworks rooted in principles of fairness, transparency, and accountability; the enactment and enforcement of stringent data protection and privacy laws; and the integration of community oversight panels that can represent diverse voices and ensure that technological tools do not alienate or target vulnerable populations.

Furthermore, **bias mitigation strategies** must be embedded into the design and deployment of AI systems. Policymakers and technologists must work together to ensure that datasets are representative, outcomes are regularly audited for discrimination, and algorithmic decisions are explainable and contestable. In high-stakes applications like policing, **explainable AI (XAI)** should be a non-negotiable standard to ensure public trust and legal accountability.

Law enforcement must also resist the temptation to treat AI as a panacea. Predictive policing cannot substitute for community engagement, structural reform, or socioeconomic interventions that address the root causes of crime. The legitimacy of any policing practice lies not in its technological sophistication but in its adherence to constitutional values, respect for human rights, and its ability to command the trust of the public.

Ultimately, the question is not just whether predictive policing can predict crime, but whether it can do so **justly**, **equitably**, and **legally**. As India and the global community continue to experiment with AI in law enforcement, the future of predictive policing must be shaped by

legal foresight, ethical design, and a firm commitment to democratic principles. Only then can technology be a tool for justice rather than a vehicle for surveillance and control.