INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ALGORITHMIC BIAS IN PREDICTIVE POLICING: A COMPARATIVE HUMAN RIGHTS CRITIQUE OF INDIA AND THE USA

AUTHORED BY - RAJVENDRA SINGH
Junior Research Fellow
Faculty of Law, University of Lucknow.

Abstract

Predictive policing systems, which deploy machine-learning algorithms to forecast criminal activity and identify high-risk individuals, have been marketed as tools of objective, data-driven law enforcement. This article argues that this promise is illusory: by training on historical crime data generated through decades of discriminatory policing, these systems do not eliminate bias but inherit, formalise, and perpetuate it at scale. Drawing on a comparative human rights methodology, this article critically examines predictive policing in India and the United States, two of the world's largest democracies with documented records of deploying algorithmic tools against minority communities. In India, the Crime Mapping, Analytics and Predictive System (CMAPS), the national Crime and Criminal Tracking Network and Systems (CCTNS), and the Automated Facial Recognition System (AFRS) have been shown to disproportionately target Muslim, Dalit, and Adivasi populations, amplifying institutional biases rooted in colonial-era criminal legislation and contemporary casteism. In the United States, tools such as PredPol, Operation LASER, and ShotSpotter have reinforced systemic racial disparities against Black and Latino communities, as documented in landmark litigation, including *Floyd v. City of New York* (2013) and the wrongful arrest of Robert Williams by Detroit police in 2020.

Both jurisdictions exhibit a shared regulatory failure: the rapid deployment of predictive systems has outpaced the development of adequate legal accountability frameworks. India's Digital Personal Data Protection Act 2023 broadly exempts state surveillance from its core obligations, while the United States lacks any federal legislation mandating algorithmic transparency or impact assessment for law enforcement. Neither country meets the international standards established under Articles 17 and 26 of the International Covenant on Civil and Political Rights or the threshold set by the European Union's Artificial Intelligence

ISSN: 2582-6433

Act 2024, which prohibits individual-risk predictive policing based solely on profiling. The article concludes with recommendations for reform, including the enactment of dedicated AI governance legislation in India, the passage of federal algorithmic accountability legislation in the United States, and the alignment of both jurisdictions' domestic frameworks with the UN High Commissioner's 2021 call for a moratorium on AI surveillance systems that cannot be deployed in compliance with international human rights law.

Keywords: *Predictive Policing, Algorithmic Bias, Human Rights, India, United States.*

1. Introduction

The promise of artificial intelligence in law enforcement is seductive: data-driven, apparently objective, and freed from the biases of individual officers. Predictive policing systems, which use machine-learning models to forecast where crimes are likely to occur and who is likely to commit them, have been adopted by police departments across democracies as instruments of efficiency and impartiality.[1] The reality, documented extensively across multiple jurisdictions, is strikingly different. Far from eliminating bias, these systems inherit and amplify the discriminatory patterns embedded in the historical data on which they are trained, subjecting already-marginalised communities to intensified surveillance and enforcement based on algorithmic outputs that cannot be examined, contested, or appealed.[2]

This article offers a comparative human rights critique of predictive policing in India and the United States, two of the world's largest democracies, each with a documented record of deploying algorithmic tools against minority communities. In India, the Crime Mapping, Analytics and Predictive System (CMAPS), the national Crime and Criminal Tracking Network and Systems (CCTNS), and the Automated Facial Recognition System (AFRS) have been used in ways that disproportionately target Muslim, Dalit, and Adivasi communities, drawing on historical policing data contaminated by decades of institutional casteism. In the United States, tools such as PredPol, Operation LASER, and ShotSpotter have reproduced and entrenched racial disparities rooted in the country's history of discriminatory enforcement against Black and Latino populations.[3]

[1] Tim Lau, *Predictive Policing Explained*, Brennan Ctr. for Just. (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.
[2] U.N. High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/48/31 (2021).
[3] Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights*

ISSN: 2582-6433

Both jurisdictions have responded to these harms with inadequate legal frameworks. India's constitutional right to privacy, recognised in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), remains unaccompanied by any AI-specific accountability legislation, and the Digital Personal Data Protection Act 2023 actively exempts state surveillance from its core obligations.[4] The United States, despite a richer body of constitutional case law, has enacted no federal legislation mandating transparency or impact assessment for algorithmic policing tools. Against the benchmark of international human rights standards, particularly Articles 17 and 26 of the International Covenant on Civil and Political Rights and the UN High Commissioner's 2021 call for a moratorium on high-risk AI surveillance, both countries fall critically short.[5] The article proceeds through a conceptual framework of predictive policing and algorithmic bias, separate analyses of the Indian and American contexts, a comparative examination of common patterns and divergent responses, and a set of reform recommendations grounded in constitutional and international human rights law.

2. Predictive Policing and Algorithmic Bias: Conceptual Framework

2.1 How Predictive Policing Systems Work

Predictive policing refers to the application of quantitative and statistical methods to forecast criminal activity, including the geographic areas where crime is likely to occur and the individuals who may be involved.[6] At its core, it is a data-driven approach that seeks to augment, and in some cases replace, traditional investigative discretion with algorithmic inference. These systems ingest large volumes of historical data, including arrest records, incident reports, call logs, and, in certain jurisdictions, social media activity, and deploy machine learning models to generate predictions about future criminal behaviour.

There are two broad categories of predictive policing tools. The first, *place-based* systems, identify geographic "hotspots" where crime is statistically more likely to occur, directing patrol resources accordingly. The second, *person-based* systems, generate risk scores or "heat lists" for individuals deemed likely to be victims or perpetrators of crime. Both categories have attracted significant scholarly and civil liberties scrutiny.[7] Proponents argue that these tools

Violations Impact Police Data, Predictive Policing Systems, and Justice, 94 N.Y.U. L. Rev. Online 192, 194 (2019).

[4] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

[5] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* 2 (N.Y.U. Press 2017).

[6] Walter L. Perry et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* 1 (Rand Corp. 2013); Brennan Ctr. for Just., *Predictive Policing Explained* (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

[7] Ferguson, supra note 5.

ISSN: 2582-6433

enhance efficiency, reduce response times, and enable resource-constrained police departments to deploy personnel more effectively. Critics contend that the apparent objectivity of algorithmic outputs masks deeply embedded social biases, lending scientific legitimacy to practices that are, in effect, discriminatory.

2.2 Defining Algorithmic Bias and Its Sources

Algorithmic bias, in the context of law enforcement, refers to the systematic and unfair skewing of outputs produced by predictive tools against particular individuals or groups on the basis of their inherent or acquired characteristics.[8] It arises not from overt discriminatory intent within the algorithm itself, but from the data on which it is trained. When historical crime and arrest data fed into these systems reflect pre-existing patterns of discriminatory policing, the algorithm learns and reproduces those patterns at scale, with the added veneer of computational neutrality.

A landmark 2019 study by Rashida Richardson, Jason Schultz, and Kate Crawford at the AI Now Institute examined 13 jurisdictions across the United States that had deployed predictive policing tools while simultaneously under federal investigation or under a consent decree for unlawful policing practices. Their findings were unambiguous: systems built on what they termed "dirty data", data derived from corrupt, racially biased, or otherwise unlawful policing, cannot escape the discriminatory legacies embedded within it.[9] The implications are far-reaching. Once biased data generates predictions, police act on those predictions, producing new arrests in the same communities, which then re-enter the dataset, reinforcing the original bias in what scholars have termed a "confirmation feedback loop."[10]

A further dimension of algorithmic bias lies in the use of proxy variables. Although most predictive policing algorithms do not explicitly incorporate protected characteristics such as caste, religion, or ethnicity as inputs, other variables, zip code, social network connections, employment status, and prior arrest records, function as surrogates for these characteristics when drawn from historically biased data.[11] The result is that facially neutral systems produce outcomes that, in practice, discriminate against already marginalised communities. As Andrew Guthrie Ferguson observes, big data policing can "reify many of the systemic inequalities of

[8] Ninareh Mehrabi et al., *A Survey on Bias and Fairness in Machine Learning*, 54 ACM Comput. Surv. 1, 3 (2021).
[9] Richardson et al., supra note 3.
[10] Sheng-Jun Liao & Pak-Hang Wong, *Predictive Policing and Algorithmic Fairness*, 180 Synthese 1, 4 (2023), https://doi.org/10.1007/s11229-023-04189-0.
[11] Ferguson, supra note 7, at 20–33.

ISSN: 2582-6433

traditional policing" while simultaneously presenting itself as a remedy for human bias.[12]

2.3 The Intersection of AI, Surveillance, and Human Rights

The deployment of AI-driven surveillance in law enforcement raises profound concerns under both domestic constitutional frameworks and international human rights law. Shoshana Zuboff's influential account of *surveillance capitalism* captures the broader political economy within which such technologies operate: a system in which human experience is converted into behavioural data, processed by machine intelligence, and used to predict, and ultimately shape, future conduct.[13] When this logic is applied to state policing functions, it risks transforming the presumption of innocence into an actuarial calculation, and the exercise of fundamental freedoms into risk-generating behaviour subject to pre-emptive suppression.

At the international level, the right to privacy is protected under Article 12 of the Universal Declaration of Human Rights and, in legally binding form, under Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which obliges signatory states to protect individuals from arbitrary or unlawful interference with their private lives.[14] The UN Human Rights Committee, in its General Comment No. 16, has extended the scope of this protection to cover the collection, storage, and use of personal data by state authorities, insisting that any such interference be governed by clear, accessible law and subject to effective oversight.[15] More recently, the UN High Commissioner for Human Rights, in a 2021 report on AI and the right to privacy, called for a moratorium on the sale and use of AI surveillance systems that cannot be deployed in compliance with international human rights standards.[16]

Two further rights are critically engaged by predictive policing: the right to equality and non-discrimination, and the right to due process. Under Articles 14 and 26 of the ICCPR, individuals are entitled to equality before the law and effective protection against discrimination on any ground, including caste, religion, and ethnicity.[17] Predictive policing, by systematically directing heightened law enforcement attention towards historically over-policed communities, whether defined by race in the United States or by caste and religious identity in India, risks

[12] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 8 (PublicAffairs 2019).
[13] Universal Declaration of Human Rights art. 12, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948); International Covenant on Civil and Political Rights arts. 14, 17, 26, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].
[14] Human Rights Comm., General Comment No. 16: Article 17 (Right to Privacy), ¶ 10, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988).
[15] U.N. High Comm'r for Hum. Rts., supra note 2.
[16] ICCPR, supra note 8, arts. 14, 26.
[17] Richardson et al., supra note 3.

ISSN: 2582-6433

structurally violating these guarantees. The use of proxy variables that encode social disadvantage amplifies this risk, as does the opacity of proprietary algorithms that prevent individuals from understanding or challenging the basis for their flagging.[13]

The right to due process is similarly imperilled. When enforcement decisions are grounded in probabilistic risk assessments rather than individualised suspicion based on specific conduct, the classical safeguards of the criminal law, the requirement of reasonable suspicion, the right to be informed of accusations, and the right to contest evidence, are functionally undermined. The person identified by an algorithm as "high risk" has no opportunity to examine, let alone challenge, the data or methodology underlying that designation. In this sense, predictive policing does not merely threaten privacy in isolation; it restructures the relationship between the individual and the state in ways that challenge foundational commitments to the rule of law. The sections that follow examine how these risks have materialised in the specific legal and socio-political contexts of India and the United States.

3. Predictive Policing in India: Emerging Risks and Minority Vulnerabilities

3.1 Key Systems and Their Deployment (CMAPS, CCTNS, Facial Recognition)

India's engagement with predictive policing is not a recent phenomenon, but its intensity and technological sophistication have grown rapidly over the past decade. The most prominent early initiative was the Crime Mapping, Analytics and Predictive System (CMAPS), developed by the Delhi Police in partnership with the Indian Space Research Organisation's Advanced Data Processing Research Institute under a Memorandum of Understanding signed in December 2015.[18] CMAPS is a web-based decision-support platform that draws on real-time data from the Dial 100 emergency helpline and from First Information Report (FIR) records stored in the national Crime and Criminal Tracking Network and Systems (CCTNS) to generate spatial hotspot maps of crime, updating its predictions every one to three minutes. It was designed to enable the Delhi Police to proactively deploy resources to predicted crime zones rather than responding reactively to reported incidents.

CCTNS, the national infrastructure underpinning CMAPS and analogous systems across India,

[18] Delhi Police & Indian Space Research Organisation–Advanced Data Processing Research Institute, Memorandum of Understanding on Crime Mapping, Analytics and Predictive System (CMAPS) (Dec. 2015), discussed in Comptroller & Auditor Gen. of India, Report No. 15 of 2020: Digital Initiatives of Delhi Police ¶ 9.2.4 (2020), https://cag.gov.in/uploads/download_audit_report/2020/9.%20Digital%20Initiatives%20of%20Delhi%20Police-05f911198e45a25.81448827.pdf.

ISSN: 2582-6433

was launched by the Ministry of Home Affairs in 2009 as a Mission Mode Project under the National e-Governance Plan. It now connects over 16,000 police stations across all States and Union Territories, digitising FIR registration, investigation records, charge sheets, and criminal histories into a centralised national database.[19] While CCTNS was conceived primarily as an administrative efficiency measure, it has progressively become the data backbone for AI-driven policing applications. The same dataset that records historical arrests, detentions, and police contacts, many of which reflect decades of discriminatory policing, now serves as training data for predictive algorithms. Beyond CMAPS and CCTNS, Indian law enforcement has also adopted Automated Facial Recognition Systems (AFRS), with Delhi Police acquiring the technology in 2018, ostensibly for locating missing children, and subsequently deploying it in public spaces, political rallies, and protest sites. States including Telangana, Uttar Pradesh, Punjab, and Rajasthan have implemented their own predictive and surveillance tools, resulting in a fragmented and largely unregulated national landscape.[20]

3.2 Caste, Religious Minorities, and Discriminatory Targeting

The most significant human rights concern arising from predictive policing in India is the systematic amplification of existing discriminatory policing practices against caste minorities, particularly Dalits and Adivasis, and religious minorities, most visibly Muslims. A landmark empirical study by Vidushi Marda and Shivangi Narayan, presented at the 2020 ACM Conference on Fairness, Accountability, and Transparency, subjected CMAPS to ethnographic and documentary scrutiny and identified three interlocking forms of embedded bias.[21] Historical bias arises from the fact that the system's training data is drawn from decades of FIR records and police registers that reflect long-standing patterns of discriminatory enforcement. Representational bias results from the over-concentration of police presence and FIR-filing in low-income, minority-populated localities. Measurement bias is introduced at the point of data entry, where the subjectivity of Dial 100 call-takers, who routinely applied more credulous classifications to calls from affluent areas and more dismissive or punitive categorisations to calls from poor and minority neighbourhoods, is formalised as algorithmic ground truth.[22]

These technological biases do not arise in a social vacuum. A 2019 survey of nearly 12,000

[19] Vidushi Marda & Shivangi Narayan, Data in New Delhi's Predictive Policing System, in FAT* '20: Proc. of the 2020 ACM Conf. on Fairness, Accountability, and Transparency 317 (2020).
[20] Nat'l Crime Records Bureau, Ministry of Home Affairs, Gov't of India, Crime and Criminal Tracking Network and Systems (CCTNS), https://cctns.org.in (last visited Apr. 2, 2026).
[21] Marda & Narayan, supra note 19.
[22] Common Cause & Lokniti, Ctr. for the Study of Developing Soc'ys, Status of Policing in India Report 2019: Police Adequacy and Working Conditions 57–58 (2019).

ISSN: 2582-6433

police personnel conducted by Common Cause and the Centre for the Study of Developing Societies found that over half of the officers interviewed believed that Muslims were inherently more prone to criminality, with comparable prejudicial attitudes documented against Dalits and Adivasis.[23] When such institutional attitudes inform the data-collection practices that feed predictive algorithms, the resulting systems do not merely reflect bias, they operationalise and entrench it. The problem is further deepened by the historical legacy of colonial-era criminal legislation. The Criminal Tribes Act of 1871, which branded entire communities as hereditarily criminal, and its post-independence successor, the Habitual Offenders Act of 1952, generated registers and records of collective stigmatisation that form a not-insignificant component of the historical policing data now ingested by CCTNS and CMAPS.[24]

The deployment of facial recognition technology in the aftermath of the February 2020 Northeast Delhi riots illustrates how predictive and identification technologies can function as tools of religiously targeted surveillance. Following the riots, in which 40 of the 53 fatalities were Muslim, and in which police conduct was widely criticised for its partiality, Delhi Police used facial recognition technology to identify alleged instigators from CCTV footage, making 137 arrests.[25] Critically, the technology had been repurposed without any legislative authorisation from its original sanctioned use, identifying missing children under a Delhi High Court order, to a function of mass political surveillance targeting protest participants who were disproportionately Muslim. The Internet Freedom Foundation documented the deployment as an "act of mass surveillance" carried out in the absence of any governing legal framework, and called for an immediate halt.[26] This episode is emblematic of a broader pattern in which surveillance tools initially deployed for neutral or benevolent purposes are incrementally expanded to serve politically charged enforcement functions against already-marginalised communities.

3.3 Legal Framework: Right to Privacy Post-Puttaswamy and Accountability Gaps

The constitutional foundation for challenging AI-driven surveillance in India rests primarily on the landmark nine-judge bench ruling of the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), in which the Court unanimously held that the right to privacy

[23] Neha Singhal, The Dangers of Facial Recognition Technolo; gy in Indian Policing, The Caravan (May 26, 2023), https://caravanmagazine.in/technology/dangers-of-facial-recognition-technology-in-indian-policing.
[24] Internet Freedom Found., We Demand the Delhi Police Stop Its Facial Recognition System (Dec. 29, 2019), https://internetfreedom.in/we-demand-the-delhi-police-stop-its-facial-recognition-system/.
[25] Puttaswamy, supra note 4.
[26] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023) [hereinafter DPDP Act].

ISSN: 2582-6433

is a fundamental right protected under Articles 14, 19, and 21 of the Constitution.[27] The Court expressly recognised informational privacy, the individual's right to control the collection, storage, and use of personal data, as a core dimension of this right. The judgment is of direct relevance to predictive policing: the covert collection of biometric data through facial recognition, the aggregation of personal histories in CCTNS, and the use of algorithmic risk scores to justify heightened police attention all constitute interferences with informational privacy that, under the *Puttaswamy* framework, must satisfy the tests of legality, legitimate aim, proportionality, and procedural safeguards.

However, the gap between constitutional principle and regulatory reality remains wide. The Digital Personal Data Protection Act, 2023 (DPDP Act), India's first comprehensive data protection legislation, contains a sweeping exemption in Section 17 that grants the Central Government broad discretion to exempt State instrumentalities from the Act's obligations on grounds including national security, public order, and the prevention and investigation of offences.[28] In practice, this means that the police forces deploying CMAPS, AFRS, and CCTNS-based predictive tools are not meaningfully bound by the data minimisation, purpose limitation, or accountability provisions that the Act imposes on private entities. The DPDP Rules, 2025, notified in November 2025, make no provision for algorithmic impact assessments, transparency requirements for automated policing decisions, or independent oversight of AI systems in the criminal justice system.

The result is a constitutional framework that recognises the right to privacy in principle, a data protection statute that carves out state surveillance in practice, and no AI-specific regulation that addresses the particular dangers of predictive policing for caste and religious minorities. India has no independent algorithmic accountability body, no mandatory audit requirements for predictive policing systems, and no meaningful mechanism for individuals flagged by an algorithm to contest the basis of their designation. The constitutional guarantees under Articles 14 and 21, equality before the law and the right to life and personal liberty, are formally intact, but they are structurally undermined by a legislative and institutional framework that offers no practical remedy to those most likely to be harmed. As the Software Freedom Law Centre has observed, the pace of predictive policing's deployment across Indian states has significantly

[27] Software Freedom Law Ctr., Tracing the Rise of Predictive Policing in India (Feb. 26, 2026), https://sflc.in/tracing-the-rise-of-predictive-policing-in-india/.

[28] The Criminal Tribes Act, 1871 (later amended by the Criminal Tribes Act, 1924); Habitual Offenders Act, 1952; Scroll.in, AI Tech Is Increasingly Being Used by Police Worldwide. Here's Why India Needs to Regulate It (Apr. 1, 2021), https://scroll.in/article/989094/ai-tech-is-increasingly-being-used-by-police-worldwide-heres-why-india-needs-to-regulate-it.

ISSN: 2582-6433

outstripped the development of legal safeguards, rendering the expansion of algorithmic surveillance a largely unchecked executive project.[13]

4. Predictive Policing in the USA: Documented Harms and Legal Gaps

4.1 Key Systems and Their Deployment (PredPol, ShotSpotter, Palantir)

The United States has been the principal laboratory for predictive policing technology, and the systems developed there have shaped global debates about algorithmic law enforcement. Three systems have been most consequential: PredPol, ShotSpotter, and Palantir. PredPol, developed from earthquake-aftershock modelling at UCLA, divides urban areas into 500-by-500-foot blocks and generates twelve-hour crime-probability forecasts based on historical incident data. At its peak, it was used by more than fifty police agencies across the country. Operation LASER, deployed by the Los Angeles Police Department from 2011 and federally funded by the Bureau of Justice Assistance, ran alongside PredPol, generating individual "chronic offender" risk scores based on criminal history, social media activity, and license plate reader data. Both were ultimately abandoned, LASER in 2019 and PredPol in 2020, but not before generating years of documented harm.[29]

Palantir Technologies, a data analytics firm with deep roots in US intelligence and defence contracting, built predictive policing infrastructure for departments including the Los Angeles and New Orleans Police Departments. Its deployment in New Orleans is particularly notable for its opacity: a journalistic investigation revealed that the system had been operating in secret for 5 years through a philanthropic arrangement, entirely bypassing City Council oversight. The NYPD paid $2.5 million to Palantir for a policing programme whose parameters were never publicly disclosed despite civil liberties organisations' formal records requests.[30] ShotSpotter, an acoustic gunshot-detection system that also generates predictive deployment recommendations, has been linked to over one hundred law enforcement agencies. Multiple major cities, including Chicago, have since ended their contracts following sustained criticism of its accuracy and discriminatory impact.

4.2 Racial Bias, Over-Policing, and Civil Rights Violations

The racial harms produced by predictive policing in the United States are extensively documented. An analysis of Oakland's PredPol deployment found that, despite the algorithm's

[29] Lau, supra note 1.
[30] See *Minority Report*, Harvard Civil Rights–Civil Liberties Law Review (Mar. 7, 2018), https://journals.law.harvard.edu/crcl/minority-report-why-we-should-question-predictive-policing/.

ISSN: 2582-6433

formal race-neutrality, Black neighbourhoods were targeted for drug-related patrols at twice the rate of white neighbourhoods, notwithstanding independent survey evidence that drug use is roughly equal across racial groups. This is a textbook illustration of the proxy-variable bias identified in Section 2.2: demographic and socioeconomic surrogates embedded in historical arrest data produce racially disparate outputs under a formally race-neutral algorithm.[31]

ShotSpotter's deployment pattern presents a parallel structural harm. The Electronic Privacy Information Centre documented that Sound Thinking disproportionately places acoustic sensors in predominantly Black neighbourhoods on the basis of historical crime data, producing a self-reinforcing surveillance cycle: sensors generate alerts, alerts generate police contacts, contacts generate more crime data, and that data confirms the original placement decision. The company's refusal to disclose its classification methodology, even in judicial proceedings, prevents external audit or legal challenge.[32] The compounding effect of these feedback loops means that communities of colour bear not merely the immediate burden of more frequent police contact, but the longer-term consequences of algorithmic entrenchment: each cycle of biased prediction deepens the data foundation driving the next generation of predictions.

The landmark federal class action *Floyd v. City of New York* (2013) provides the judicial backdrop against which the harms of algorithmic policing in the United States must be assessed. Judge Shira Scheindlin found that the NYPD's stop-and-frisk programme violated both the Fourth Amendment and the Equal Protection Clause of the Fourteenth Amendment through a pattern of systematic racial profiling. Between 2004 and 2012, over 4.4 million stops were conducted: 52% involved Black individuals and 31% Latino individuals; no weapon was found in 98.5% of frisks.[33] Although *Floyd* pre-dates widespread algorithmic policing, the racial targeting patterns it judicially confirmed, premised on crime-demographic data, are structurally identical to those encoded in predictive tools today. The case establishes the constitutional baseline against which those tools must be measured.

4.3 Legal Framework: Fourth Amendment, Due Process, and Regulatory Gaps

The primary constitutional framework governing police encounters in the United States is the Fourth Amendment's protection against unreasonable searches and seizures. *Terry v. Ohio* (1968) established the "reasonable suspicion" standard, requiring that an investigatory stop be

[31] See id.
[32] See Letter from Electronic Privacy Information Center to Att'y Gen. (2022), https://epic.org/documents/epic-letter-to-attorney-general-garland-re-shotspotter-title-vi-compliance/; 42 U.S.C. § 2000d.
[33] Terry v. Ohio, 392 U.S. 1, 21 (1968).

ISSN: 2582-6433

grounded in "specific and articulable facts."[34] Predictive policing creates acute constitutional tension with this requirement. As Ferguson has argued, algorithmic tools undermine *Terry*'s individuated-suspicion requirement by shifting the basis for police action from an officer's observation of a specific individual's conduct to statistical inferences about a geographic zone or a demographic profile. When a person is stopped because an algorithm has flagged their neighbourhood as high-risk, the nexus between the stop and any articulable fact specific to that person is strained by the Constitution.[35]

Civil rights law presents further structural limitations. Under *Washington v. Davis* (1976), the Equal Protection Clause requires proof of discriminatory *intent*, not merely disparate impact, making constitutional challenges to formally race-neutral predictive algorithms structurally difficult to sustain even where outputs are demonstrably racially disproportionate. Title VI of the Civil Rights Act of 1964 provides some leverage, prohibiting racial discrimination in federally funded programmes, but its application to algorithmic bias in policing remains legally unsettled.[36]

The regulatory gap at the federal level is substantial. The Algorithmic Accountability Act was introduced in Congress three times, in 2019, 2022, and 2023, and failed on each occasion to advance beyond committee referral.[37] In the absence of federal legislation, some cities and states have acted independently. Santa Cruz, California, banned predictive policing in 2020; Chicago ended its ShotSpotter contract in 2024. Executive Order 14,074 (2022) directed federal law enforcement to review its use of predictive algorithms but left state and local police, which deploy the overwhelming majority of these tools, entirely unaddressed.[38] The result is a constitutional framework that formally prohibits unreasonable searches and racially discriminatory policing, but an institutional and legislative landscape that has so far failed to translate those commitments into effective constraints on the algorithmic systems now determining who is policed, where, and with what intensity.

[34] Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 Wash. U. L. Rev. 1109, 1141–46 (2017); Lau, supra note 1.
[35] Floyd v. City of New York, 959 F. Supp. 2d 540, 562 (S.D.N.Y. 2013).
[36] 42 U.S.C. § 2000d; U.S. Const. amend. XIV, § 1; see also Washington v. Davis, 426 U.S. 229, 239 (1976).
[37] Algorithmic Accountability Act of 2023, S. 2892, 118th Cong. (2023); H.R. 5628, 118th Cong. (2023).
[38] See *Politicians Move to Limit Predictive Policing*, supra note 1; Exec. Order No. 14,074, 87 Fed. Reg. 32,945 (May 31, 2022); *What Does the New White House Policy on AI Mean for Law Enforcement?*, The Policing Project (Apr. 15, 2024), https://www.policingproject.org/news-main/2024/4/15/what-does-the-new-white-house-policy-on-ai-mean-for-law-enforcement-here-are-our-takeaways/.

ISSN: 2582-6433

5. Comparative Analysis: Patterns, Divergences, and Human Rights Implications

5.1 Common Patterns: Bias, Opacity, and Minority Targeting

Despite their very different constitutional traditions, social structures, and policing histories, India and the United States exhibit a structurally identical mechanism of algorithmic harm. In both jurisdictions, predictive systems are trained on historical crime and arrest data that reflects decades of discriminatory enforcement: in the United States, against Black and Latino communities shaped by the War on Drugs and racially motivated stop-and-frisk practices; in India, against Muslims, Dalits, and Adivasis shaped by colonial-era criminal classification and post-independence institutional casteism. The National Academies of Sciences documented this feedback loop comprehensively in the US context, showing that communities subjected to intensive surveillance accumulate arrest records that, when fed into algorithms, are misinterpreted as evidence of higher criminality rather than of greater policing attention.[39] The Indian Supreme Court's acquittal of six Paradhi men in *Ankush Maruti Shinde v. State of Maharashtra* (2019), who spent sixteen years on death row on no basis other than their community membership, illustrates precisely how caste-based presumptions of criminality generate the tainted data that predictive systems subsequently formalise.[40]

A second shared pattern is opacity. In neither jurisdiction are individuals subject to predictive flagging informed of that fact, nor are they given any meaningful opportunity to contest the algorithmic basis for their designation. In the United States, the LAPD's Inspector General concluded in 2019 that auditing PredPol was effectively impossible due to the software's proprietary complexity. In India, expansive law enforcement exemptions under the Right to Information Act 2005 mean that details of CMAPS, CCTNS-based tools, and facial recognition deployments are insulated from public scrutiny. Both contexts thus reproduce what scholars describe as the "black box" problem of AI governance: outcomes that are discriminatory in effect cannot be contested because the processes that generate them cannot be examined.[41]

5.2 Divergent Legal and Institutional Responses

Notwithstanding these structural parallels, the two jurisdictions differ significantly in the legal

[39] Nat'l Acads. of Scis., Eng'g & Med., *Proactive Policing: Effects on Crime and Communities* 144–47 (2018); see also Sheng-Jun Liao & Pak-Hang Wong, *Predictive Policing and Algorithmic Fairness*, 180 Synthese 1, 4–6 (2023).
[40] Ankush Maruti Shinde v. State of Maharashtra, (2019) 15 S.C.C. 470 (India).
[41] Margaret L. Boittin et al., *Evidence of Caste-Class Discrimination from a Conjoint Analysis of Law Enforcement Officers*, 117 Am. Pol. Sci. Rev. 1127, 1128–29 (2023).

ISSN: 2582-6433

tools available to challenge algorithmic policing. The United States, despite the absence of federal AI-specific legislation, possesses a mature body of constitutional case law through which courts have imposed judicially enforceable structural remedies. The *Floyd v. City of New York* precedent, which required the appointment of a federal monitor, mandated revised police training and established ongoing judicial oversight, demonstrates that the Fourth and Fourteenth Amendments can, in appropriate cases, generate prospective obligations on police departments that go beyond individual compensation. India, by contrast, has not produced a single judicial decision specifically addressing the discriminatory use of predictive policing technologies. While *Puttaswamy*'s recognition of privacy as a fundamental right provides a constitutional foundation, it has not yet been operationalised in the context of algorithmic policing, and the Digital Personal Data Protection Act 2023 actively retreats from accountability by exempting state surveillance from its core obligations.[42]

The divergence in regulatory ambition is also stark when compared with the global benchmark set by the European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689). Article 5(1)(d) of the AI Act, which became enforceable on 2 February 2025, categorically prohibits AI systems that assess or predict an individual's risk of committing a criminal offence based solely on profiling or personality characteristics, attracting penalties of up to €35 million or 7% of global annual turnover for non-compliance.[43] Neither India nor the United States has enacted legislation of comparable scope or enforceability. The AI Act thus functions in this comparative analysis not as a jurisdiction to be directly compared, but as a human rights benchmark that exposes the depth of the regulatory deficit in both countries. By EU standards, India's complete absence of algorithmic accountability law and the United States' reliance on litigation-only constitutional remedies are equally inadequate responses to documented and ongoing harm.

5.3 Cross-Jurisdictional Lessons and the Limits of Technical Reform

The UN High Commissioner for Human Rights, in a 2021 report that directly addressed AI-driven predictive surveillance, called for a moratorium on AI systems that pose serious risks to human rights pending the establishment of adequate safeguards, and for outright bans on systems that cannot be deployed in compliance with international human rights law.[44] This

[42] Floyd v. City of New York, 959 F. Supp. 2d 540 (S.D.N.Y. 2013); PRS Legislative Research, *The Digital Personal Data Protection Bill, 2023: Legislative Brief* 4–5 (Aug. 2023), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.

[43] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, art. 5(1)(d), 2024 O.J. (L 1689); see also *Partial Ban on "Predictive" Policing*, Fair Trials (Dec. 12, 2023), https://www.fairtrials.org/articles/news/partial-ban-on-predictive-policing-included-in-final-eu-ai-act/.

[44] U.N. High Comm'r for Hum. Rts., *Artificial Intelligence Risks to Privacy Demand Urgent Action*, Press Release

ISSN: 2582-6433

recommendation, applicable to both jurisdictions, provides the normative frame within which each can draw contextually specific lessons from the other.

India can draw most directly from the United States' experience of judicial accountability. The *Floyd* litigation demonstrated that structural remedies, independent monitoring, mandatory training reforms, and transparency requirements can be imposed on discriminatory policing systems through constitutional litigation even in the absence of AI-specific legislation. India's existing jurisprudence on the right to privacy under Article 21, combined with the non-discrimination guarantees in Articles 14 and 15, provides a viable constitutional foundation for comparable litigation challenging algorithmic systems that disproportionately target Muslim, Dalit, or Adivasi populations. The Vidhi Centre for Legal Policy has specifically recommended that India mandate public disclosure of the legal basis, data sources, and auditing mechanisms for any predictive policing deployment, modelled precisely on the kind of oversight that *Floyd* institutionalised.[45]

The United States, conversely, can draw on India's experience to develop a sharper awareness of the colonial genealogy of policing data and the structural nature of algorithmic harm. While American civil rights discourse has increasingly emphasised the link between the War on Drugs, mass incarceration, and racially biased policing datasets, a comparative reading against India's predicament illuminates how deeply the problem of data contamination is rooted in state-sanctioned historical discrimination that cannot be resolved by technical debiasing alone. The colonial Police Act 1861, still the foundational legislation governing Indian policing, and its counterpart, the history of slavery and Jim Crow enforcement in the United States, both demonstrate that predictive algorithms inherit not merely statistical patterns but entire institutional architectures of minority subjugation.[46] This shared genealogy underscores a fundamental lesson that both jurisdictions must internalise: so long as the data on which predictive systems are trained reflects discriminatory enforcement, no algorithmic adjustment or technical audit can substitute for the deeper structural reform of the institutions that generate that data.

(Sept. 15, 2021), https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet; U.N. High Comm'r for Hum. Rts., *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/48/31 (2021).

[45] Vidhi Centre for Legal Policy, *India's Tryst with Predictive Policing* (Nov. 11, 2021), https://vidhilegalpolicy.in/blog/indias-tryst-with-predictive-policing/.

[46] Ashwin Varghese, *Racialization and Structural Inequality: The Legacy of Colonial Police in India*, PoLAR: Pol. & Legal Anthropology Rev. (Nov. 8, 2023), https://polarjournal.org/2023/11/08/racialization-and-structural-inequality-the-legacy-of-colonial-police-in-india/.

ISSN: 2582-6433

6. Conclusion

6.1 Summary of Key Findings

This article examines predictive policing through a comparative human rights lens, focusing on India and the United States as its primary jurisdictions. The analysis establishes three interconnected findings. First, algorithmic bias in predictive policing is not an incidental technical flaw but a structural consequence of deploying machine-learning systems trained on data generated by discriminatory institutions. In India, the CMAPS and CCTNS-backed systems formalise historical biases against Muslim, Dalit, and Adivasi communities; in the United States, PredPol, Operation LASER, and ShotSpotter reproduced and amplified racial disparities rooted in a long history of discriminatory enforcement. In both cases, the algorithm does not introduce bias: it inherits and launders it, presenting the outputs of discriminatory human judgment as the products of neutral computation.[47]

Second, the deployment of these systems in both jurisdictions has outpaced the development of adequate legal safeguards. India has no AI-specific policing legislation, and its Digital Personal Data Protection Act 2023 actively shields state surveillance from accountability. The United States lacks comprehensive federal AI regulation, relying instead on post hoc constitutional litigation that provides inadequate prospective protection. Neither country has enacted mandatory algorithmic impact assessment requirements, independent audit mechanisms, or transparency obligations that would allow affected communities to understand or contest the basis for their surveillance and targeting.

6.2 Human Rights Imperatives: Privacy, Equality, and Due Process

The human rights implications are severe and cross-cutting. Predictive policing as currently practised in both jurisdictions violates the right to privacy, enshrined in Article 21 of the Indian Constitution and the Fourth Amendment of the United States Constitution, and binding internationally under Article 17 of the ICCPR, by subjecting individuals to covert data collection and risk-scoring without lawful authority, necessity, or proportionality. It violates equality guarantees, under Articles 14 and 15 of the Indian Constitution and the Equal Protection Clause of the Fourteenth Amendment, by systematically directing state coercion at communities defined by religion, caste, or race. And it subverts due process, under Article 22 of the Indian Constitution and the Fifth and Fourteenth Amendments, by substituting probabilistic algorithmic inference for individualised, evidence-based suspicion as the

[47] Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 Ga. L. Rev. 109, 113 (2017).

ISSN: 2582-6433

foundation for police action.[48]

6.3 Recommendations for Reform and the Path Forward

Reform requires action on multiple fronts. India should enact dedicated AI governance legislation that categorically prohibits person-based predictive policing, mandates pre-deployment algorithmic impact assessments, and establishes an independent oversight authority with the power to audit police AI systems and to receive complaints from affected communities.[49] The DPDP Act 2023 must be amended to remove the broad law enforcement exemption in Section 17 and to subject state data processing to the same accountability standards applicable to private entities. The United States must close the gap between constitutional principle and regulatory practice by passing federal legislation, drawing on the Algorithmic Accountability Act model, that imposes mandatory transparency, audit, and impact-assessment obligations on law enforcement agencies that deploy predictive tools.[50]

Both jurisdictions should, at a minimum, align their domestic frameworks with the international standards articulated by the UN Human Rights Committee under the ICCPR and the OHCHR's 2021 call for a moratorium on AI surveillance systems that cannot be deployed in compliance with human rights law. The European Union's AI Act, with its categorical prohibition on individual-risk predictive policing under Article 5(1)(d), offers a regulatory model that neither country has yet been willing to adopt but that the evidence examined in this article strongly supports. Ultimately, the legitimacy of law enforcement in any democracy rests on its fidelity to the rule of law; rule by algorithm that encodes structural discrimination is no rule of law at all.

[48] Software Freedom Law Ctr., supra note 27.
[49] Ferguson, supra note 5.
[50] International Covenant on Civil and Political Rights arts. 14, 17, 26, Dec. 16, 1966, 999 U.N.T.S. 171.