
ALGORITHMIC BIAS AND ACCOUNTABILITY IN PREDICTIVE POLICING: A LEGAL AND ETHICAL APPRAISAL

Himadri Mishra, Amity University, Amity Law School, Lucknow

ABSTRACT

As a data-oriented law enforcement method, predictive policing combines statistical methods, machine learning models, and massive datasets to forecast crime trends and determine the actions of law enforcement. Although it is marketed as a strategy to boost efficiency and objectivity, predictive policing systems have received a lot of legal and ethical controversy because they may replicate and magnify the structural biases that are inherent in previous crime data. In this research paper, the antecedents and symptoms of algorithmic bias in predictive policing systems like COMPAS, PredPol, and LASER are critically analyzed and the impacts that the systems have on decision-making and operational policing practices are discussed.

The paper provides an assessment of the regulatory responses that have been adopted in different jurisdictions such as the United States, the United Kingdom, the European Union, Japan, and India through a doctrinal and comparative approach methodology backed by empirical evidence that is in the form of audit reports and experimental studies. The major court cases such as *State v. Loomis* and *Bridges v. Chief Constable of South Wales Police*, show that there is an urgent necessity to apply transparency, accountability, and rights-based supervision over automated decision-making within the criminal justice system. The paper finds that predictive policing algorithmic bias is not only a technical flaw, but a structural issue that requires a sound legal amendment, improved governance structures, and technologically responsible design.

Keywords: Predictive policing, algorithm bias, accountability, artificial intelligence, machine learning, criminal justice, due process, discrimination, data protection, legal regulation.

1. INTRODUCTION

Predictive policing is the combination of statistical analyses, machine learning models, and algorithmic tools to predict patterns in crime, offenders who might commit a crime, and the better use of police resources. This idea began in the days of computational criminology, which would identify nodes of pressures for crime using previous crime data. But due to machines' advances in artificial intelligence (AI) and big data analytics, predictive policing has taken root to serve as a powerful and topic, tool used by police agencies on a global scale. Algorithms and associated tools like PredPol, COMPAS, and LASER have been developed in part to improve workflow and customer safety and reduce human mistakes and inefficient police work¹.

The topic also brings profound concerns around fairness, civil liberties, and discrimination. These models utilize skewed data, resulting from decisions that historically over-policed minority communities, that creates these algorithms which, by virtue of their superiority, would sometimes reconstruct, magnify, and perpetuate racial and socio-economic inequities. These concerns were exacerbated when ProPublica's 2016 investigation titled "Machine Bias" of COMPAS revealed there was racial bias in risk assessments that were used in sentencing².

The use of AI in police work fits in with the trend of governments and the private sector toward data-based governance and decision-making. Predictive models now help police make decisions such as parole eligibility, the ability to be released during pre-trial, patrol, and allocation of police resources. AI's ability to find and analyze enormous sets of data, including demographic data, historical crime data, geospatial data, social network data, and social media data, has, in part, pushed police departments toward the use of automated analytical tools to supplement or even replace human decision-making.

Considering the increase in the use of automated algorithms and models, new considerations regarding accountability and public oversight arise. While previous competences and practices in policing could be objectively assessed through representation by humans or documented processes, AI systems implement methods of decision making that may not be fully understood, even by the developers themselves. As a result, systems of automated decision

¹ O'Neil C, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publishing Group 2016)

² S Barocas and A D Selbst, 'Big Data's Disparate Impact' (2016) 104(3) *California Law Review* 671–732

making can be troublesome under the abstraction of "black boxes." This presents challenges to accountability and human oversight. As O'Neil argues, algorithms will be "weapons of math destruction" if they are able to run "with zero transparency, feedback, or fairness³."

2. RESEARCH METHODOLOGY

This research employs a doctrinal legal methodology which concentrates on an analysis of statutes, case law, policy documents, and academic commentaries that address algorithmic policing.

A comparative methodology is also employed that looks at the different approaches each country takes to regulate predictive policing tools. This includes an analysis of regulatory frameworks, such as international instruments, national AI strategies, and data protection laws such as the GDPR and the EU AI Act.

Overall, these methods provide a thorough, multidisciplinary analysis of predictive policing reflective of both legal analysis and the realities of technology.

3. LITERATURE REVIEW

The existing body of scholarship on predictive policing reflects deep tensions between technological innovation and its socio-legal consequences. Researchers have explored how algorithmic tools reshape the traditional architecture of law enforcement, not by merely enhancing efficiency, but by reorienting institutional priorities toward data-driven surveillance and risk-based governance. These studies challenge the assumption that algorithms are neutral or objective, emphasizing that predictive models inherit biases from the historical datasets on which they are trained, often amplifying structural inequalities rather than mitigating them.

At the same time, an emerging strand of literature critiques the regulatory and accountability vacuum surrounding these technologies. Scholars highlight how proprietary software, opaque scoring mechanisms, and fragmented state capacities prevent effective oversight. As predictive policing becomes embedded in routine criminal justice practices, academic discourse increasingly interrogates the implications for civil liberties, privacy, and democratic control. Against this backdrop, four key contributions offer critical insights into the relationship

³ C O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publishing Group 2016)

between algorithmic policing, discrimination, and institutional responsibility.

- **Sarah Brayne (2021)**, in her ethnographic study of the Los Angeles Police Department, demonstrates how predictive policing systems institutionalize surveillance by integrating databases, social networks, and automated risk scores. She reveals that algorithmic tools disproportionately target marginalized communities and expand police discretion instead of constraining it. Brayne argues that the adoption of these technologies normalizes datadriven surveillance as everyday policing practice.
- **Ben Green (2019)**, examines the “algorithmic governance” paradigm and contends that predictive policing technologies reinforce harmful feedback loops rather than solving crime. He argues that historical, biased datasets produce distorted forecasts which lead to over-policing of already vulnerable groups. Green emphasizes that technological neutrality is a myth and warns that automation masks political choices within law enforcement.
- **Michael Veale & Lilian Edwards (2018)**, critically analyze accountability challenges in algorithmic decision-making systems used by public authorities, including police. They argue that existing legal doctrines are insufficient to explain algorithmic opacity, especially when proprietary software prevents transparency. Their work proposes institutional accountability tools, such as impact assessments and mandatory auditability, to prevent unchecked technological power.
- **Cathy O’Neil (2016)**, highlights how predictive algorithms in policing operate as “Weapons of Math Destruction,” amplifying structural inequalities. She demonstrates that algorithmic risk models penalize socio-economic vulnerabilities and convert them into indicators of criminality. O’Neil contends that the lack of oversight and transparency makes these systems self-reinforcing, creating cycles of discrimination under the guise of objectivity.

4. EVOLUTION OF PREDICTIVE POLICING AND ALGORITHMIC SYSTEMS

Legal action toward predictive policing has changed with the rapid growth in the use of algorithmic tools in policing. At first, predictive policing was seen as a new technological improvement to efficiency and crime reduction. Then, after a growing amount of scholarship

and investigative journalism and empirical research continued to expose significant amounts of racial and socioeconomic bias in these systems. This section looks at the shift from early, unregulated use toward more formal regulatory procedures to create accountability.

4.1 Early Legal Approaches to Policing Technology

Predictive policing initially had its roots in military-style intelligence models, and it was not legally scrutinized. Algorithms like Predictive Policing and HunchLab were marketed to the police as "neutral" algorithmic solutions, to reduce crime without the constitutional and ethical concerns of using police. During this period, there was no regulatory oversight of predictive policing.

Lum and Isaac demonstrated via empirical simulation, predictive policing systems that were trained on and relied upon historically biased arrest data, simply replicated and amplified racialized policing, allocating police resources disproportionately to minority neighborhoods⁴. In a similar vein, a prominent investigation of ProPublica determined that algorithmic risk assessments, like COMPAS, misclassified Black defendants as high-risk nearly twice the rate of white defendants⁵.

A range of human rights organizations outside of the U.S. voiced similar concerns as reflected in a warning issued by the UN Office of the High Commissioner for Human Rights (OHCHR) on new uses of artificial adjuncts in policing⁶.

The early legal commentary was marked by optimism about the possibilities of technology, lack of scrutiny about data sources, and disregard systemic discrimination ultimately paving the way for judicial and legislative engagement later.

4.2 Recognition of Algorithmic Bias in Law

The second stage in the legal development of predictive policing included an explicit acknowledgement of algorithmic bias by the courts and policy makers. One important case is *State v. Loomis*, in which the Wisconsin Supreme Court examined the use of the COMPAS algorithm in sentencing. This development is also significant worldwide, because it was one

⁴ K Lum and W Isaac, 'Predictive Policing Is Biased' (2016) *arXiv*.

⁵ ProPublica, 'Machine Bias' (2016).

⁶ Office of the United Nations High Commissioner for Human Rights (OHCHR), 'Artificial Intelligence Risks Endangering Human Rights' (2021).

of the first cases where a court recognized that obscure algorithms could create constitutional risks⁷.

In the United Kingdom, one major judgement of the Court of Appeal in *R (Bridges) v. Chief Constable of South Wales Police* ruled that the use of automated facial recognition technology was an infringement of the Human Rights Act and UK GDPR in breach of privacy and data protection obligations. Again, while the case did not deal with predictive policing directly, the propositions adopted by the Court, particularly the call for clearer legal frameworks, safeguards against discrimination, and a higher threshold for data accuracy have been problematic when giving rise to discussions of algorithmic policing⁸.

In the U.S., academic research also encouraged legal institutions to address predictive policing bias. A prominent RAND Corporation report that was based on research on predictive policing programs cautioned that many algorithmic implementations lacked sufficient evaluation processes, ignored civil liberties, and had the potential to continue with racial inequities⁹.
Human Rights

Watch similarly documented many occasions on which predictive tools continued “hot spot policing” practices that involved over-policing marginalized communities¹⁰.

Meanwhile, EU institutions carried further legal recognition by formally requiring that algorithmic systems respect nondiscrimination norms within a legal frame under GDPR. Under Articles 5 and 22, individuals have the right not to be subject to decisions that are made solely automatic processing and especially decisions that are significant to an individual's rights or freedoms¹¹.

Overall, these trends reflect a shift away from uncritical acceptance and are finally beginning to recognize predictive policing as a legally sensitive technology with a need for safeguards.

4.3 Development of Accountability Frameworks

The third stage of legal responses involves developing formal accountability frameworks

⁷ State v Loomis 881 NW2d 749 (Wis 2016).

⁸ R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058.

⁹ RAND Corporation, Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations (2013).

¹⁰ Human Rights Watch, Predictive Algorithms and Policing (2021).

¹¹ European Parliament, GDPR and AI Systems: Legal Analysis (2020).

intended to govern algorithmic policing technologies. Such frameworks may take the form of statutory schemes, judicial doctrine, administrative guidelines, and ethical frameworks.

In the United States, various reforms have been implemented at the municipal and state level. For example, Oakland and New York City adopted "surveillance oversight ordinances," requiring police departments to be transparent about their use of algorithmic tools, assess the impact of their use, and seek ratification from a legislative body. Academic scholarship has also emphasized the need for transparency, community-control, and regular audits in the development of data-based policing, including Ferguson's Framing Committee on Data-Driven Policing and the Boston Police Department's Community Advisory Committee. In these ways, the local accountability and the oversight of law enforcement represent one of the most significant shifts in law towards accountability¹².

On an international level, the European Union proposed the Artificial Intelligence Act classifying predictively policing as a "high-risk" type of AI with strict requirements, including risk assessment, human oversight, and independent auditing¹³.

Though slower at the level of formal legislation, Japan and India have both engaged in some policy discussion with respect to the risks of algorithmic policing. For instance, Japan's National Police Agency has positioned ethical deployment guidelines while Indian academics and activists, including contributors to *Economic & Political Weekly*, have documented the risks of predictive policing within a country that suffers from caste and religious discrimination¹⁴. Those types of commentaries have triggered discussions in parliament about the introduction of the Digital Personal Data Protection Act and the issues of developing regulations specifically for AI policing.

At this point, predictive policing is understood not simply as a technological tool but as a governing issue that will require applicable structural legal reform. The recognition of algorithmic bias, along with the normative claim for transparency, has led legislatures and courts to consider more robust measures for accountability.

¹² A Ferguson, 'Policing Predictive Policing' (2017) *Northwestern University Law Review*.

¹³ European Commission, *Artificial Intelligence Act* (2021).

¹⁴ *Economic and Political Weekly (EPW)*, 'Predictive Policing in India: Critical Perspectives' (2020).

5. COMPARATIVE LEGAL FRAMEWORKS AND GLOBAL APPROACHES TOWARDS REGULATING PREDICTIVE POLICING

Comparative legal frameworks show marked disparity between legal systems concerning regulation, oversight, and ethical regulation of predictive policing. While some countries have engaged more explicit and positive regulation, some remain less engaged and still in their infancy. In the following section, we consider five major legal regimes to disclose how legal systems across the globe respond to algorithmic policing.

5.1 The United States

The U.S. constitutes the largest testing ground of predictive policing measures, which includes programs such as PredPol, HunchLab, and improvements to CompStat.

Constitutional norms, particularly the Fourth Amendment, continue to remain within the most steadfast limits to algorithmic abuse. One of the challenges with predictive-based policing is concerns regarding discriminatory policing, compounded by the existence of evidence. For example, PredPol removed a significant percentage of its hotspots it predicted in areas primarily inhabited by black and Latino individuals, posing questions related to equity and privacy¹⁵

Los Angeles paused its predictive policing initiatives after independent audits revealed significant racial disparities in compliance with its oversight initiatives¹⁶. Similarly, Chicago discontinued its predictive tool entitled the "Strategic Subject List" in part due to too many biases against designated marginalized communities as well as the lack of predicting crime outcomes¹⁷.

At this moment, the U.S. context has constitutional oversight, local lawmaking changes, judicial restraint, and an ever-growing anti-racial bias algorithmic-policing activism.

5.2 The United Kingdom

The United Kingdom has advanced regulatory scheme for algorithmic policing. It is based on

¹⁵ Prison Policy Initiative, PredPol White Paper (2016).

¹⁶ Office of the Inspector General Los Angeles, Audit of Data-Driven Policing (2019).

¹⁷ Chicago Tribune, 'CPD Ends Predictive Policing Program' (2020)

data protection legislation, human rights legislation and judicial review. Under the Data Protection Act 2018 and the UK GDPR, the police complies with transparency, data accuracy and proportionality principles in the use of algorithmic tools.

The UK approach sits within a rights-based governance framework, legal accountability and strong privacy standards, meaning that it is one of the more comprehensive regulatory environments.

5.3 Japan

Japanese police forces began trials of AI-enabled predictive policing systems in preparation for the Tokyo Olympic Games ,2020.A app named **Crime Nabi** uses a deep learning algorithm to analyze historical crime statistics ,geographical conditions to predict crimes.

5.4 Germany

In February 2023, the Federal Constitutional Court invalidated some state laws in Hesse and Hamburg authorizing the police to use automated data processing to predict crimes, in part due to violating the informational self-determination, and because it lacked sufficient legal limits on the use of such data¹⁸.

Also, as reported by a recent Algorithm Watch, predictive crime-prediction systems (e.g., geographic crime forecasting, person profiling) are being implemented without apparent legal underpinning in several Lander, of concern due to fragmentation and regulation of policing and criminal justice respectively¹⁹.

5.5 The European Union

Because of the General Data Protection Regulation (GDPR) and the forthcoming Artificial Intelligence Act (AI Act), the European Union is a global leader in a comprehensive approach to the regulation of AI.

¹⁸ AI-Regulation.com, ‘German Federal Constitutional Court’s Decision on Automated Predictive Policing Algorithms’ (22 February 2023)

¹⁹ AlgorithmWatch, Automating Injustice: “Predictive” Policing and Profiling Systems Used by Law Enforcement in Germany AlgorithmWatch Report (March 2025)

The GDPR, Articles 5, 13-15 and 22 provide meaningful restrictions on predictive policing:

- personal data must be accurate, relevant and limited in relation to the purpose.
- individuals have a right not to be subject to a decision based solely on automated processing.
- data subjects are entitled to an explanation regarding the automated processing of their data.

The European Parliamentary Research Service has reported that predictive policing systems do not, in many instances, comply with the GDPR's standards for transparency and data quality, especially when they impose biases from the data on which they are based²⁰.

The AI Act takes a further step, identifying predictive policing as a "high-risk AI system" and need to require mechanisms of human oversight²¹.

5.6 China

China is a very contrasted scenario in terms of legal regulations. Predictive policing has been implemented on a large scale, through systems such as the Integrated Joint Operations Platform (IJOP), which is used to predict risk and take police action²².

5.7 Brazil

In Brazil predictive policing is being developed alongside issues of racial profiling and the assumption that the underprivileged areas (favelas) are over targeted. Predictive policing is not governed under a single law in the country. Rather, the regulation of data protection is conducted under the General Personal Data Protection Law (LGPD), which demands transparency, purpose limitation, and data minimization²³. Nevertheless, according to scholars, LGPD is not well applied to policing purposes, and police databases are not often controlled

²⁰ European Parliament, AI and GDPR Briefing (2020)

²¹ European Union, EU Artificial Intelligence Act (2021 Draft).

²² Wikipedia, 'Predictive Policing: China and the Integrated Joint Operations Platform (IJOP)' (2024) https://en.wikipedia.org/wiki/Predictive_policing.

²³ R da Silva, 'Data Protection and Police Use of Algorithms under Brazil's LGPD' (2021) 18(2) Brazilian Journal of Public Law 88–109.

by the independent authority²⁴.

To make predictive algorithms work, Brazilian civil society demands that predictive algorithms be strictly regulated to prevent their ability to reinforce systemic biases in the field of law enforcement²⁵.

6. CASE STUDIES

This section reviews notable real-world predictive policing programs that have influenced legal and ethical discussions around policing technology in a global context.

6.1 The PredPol Controversy in the United States

One of the earliest algorithmic systems to be put into action by U.S. law enforcement agencies in predicting crime hotspots was the Predictive Policing software known as PredPol later renamed Geolitica. Several studies have found that, despite the lack of a significant crime rate increase, PredPol targeted Black and Latino neighbourhoods more, which established a pattern of historical biasing being amplified by the algorithmic process of predicting crime, which has increased to enforce the bias further²⁶.

In 2021, a study of Plainfield, New Jersey established that PredPol was able to generate crime predictions in nearly all majority-Black neighborhoods, but had virtually no predictions in largely white areas, despite comparable crime-reporting rates, which led to the conclusion that PredPol was functioning as a feedback loop of structural bias, with predictions justifying further police deployment, and the resulting arrests recreating the system itself²⁷.

6.2 The COMPAS Algorithm Bias Case

The algorithm was created by Northpointe (since changed to Equitant) as the COMPAS (Correctional Offender Management Profiling Alternative Sanctions) algorithm to help the U.S. judges in their decision-making concerning bail, sentencing, and parole. Controversy arose around 2016 when a journalistic investigation by ProPublica found the risk-scoring

²⁴ M Carvalho and J Ribeiro, 'Enforcement Challenges of Brazil's LGPD in Security and Policing Sectors' (2022) 12(3) Latin American Law Review 95–120.

²⁵ InternetLab Brazil, Algorithmic Discrimination and Predictive Policing in Brazil: Policy Recommendations for Rights-Based AI Governance (2023).

²⁶ A G Ferguson, *The Rise of Big Data Policing* (NYU Press 2017).

²⁷ K Hill, 'PredPol Analysis Report' (2021) The Markup.

methodology of the algorithm to falsely label Black defendants as high-risk nearly twice as often as white defendants, despite being primarily marketed as being race-neutral internally, the algorithm relied on proxies including socioeconomic status, neighborhood background, and stability in employment, which disproportionately classified minority groups²⁸.

6.3 UK's Gang Matrix Discrimination Findings

The Gang Matrix of London Metropolitan Police Service, which was created following the 2011 London riots, was a tool that sought those individuals that were considered at risk of perpetrating gang related violence. Nevertheless, by 2018 the UK Information Commissioner's Office (ICO) discovered that the Matrix discriminated against Black men unlawfully, who comprised over 78 per cent of the ones listed, despite evidence demonstrating that gang involvement in London was not connected to racial disproportionality of this kind²⁹.

The investigation into the ICO concluded that the Matrix breached the UK Data Protection Act 1998 and then the Data Protection Act 2018 by failing to provide lawful reasons as to why data was being processed, stored out of date and targeting the minority groups with disproportionate effect, lacking evidence-based explanation³⁰.

6.4 The Netherlands SyRI Fraud Detection Algorithm Case

A massive predictive system, the SyRI (System Risk Indication) of the Netherlands was a welfare fraud detector that triggered a series of government data sources. In *NJCM et al. v. State of the Netherlands* (2020), the Hague District Court imposed a fine on the petitioners after stating that SyRI allowed surveillance of low-income and immigrant groups indiscriminately, which was incompatible with the rights to privacy covered by Article 8 of the European Convention on Human Rights³¹.

The ruling was also the first case in the world to invalidate a government algorithm on the ground of its discriminatory results due to the absence of transparency and the inability to comprehend how the risk scores were produced, which has become a landmark in algorithmic

²⁸ S Barocas and A D Selbst, 'Big Data's Disparate Impact' (2016) 104(3) *California Law Review* 671–732.

²⁹ Information Commissioner's Office (ICO), *Investigation into the Gangs Matrix* (2018).

³⁰ *Ibid*

³¹ *NJCM and Others v State of the Netherlands* ECLI:NL:RBDHA:2020:865 (District Court of The Hague 2020).

accountability³².

6.5 Chicago's Heat List Program

The Strategic Subject List of Chicago Police Department (also called the Heat List) implemented a regression-based modelling algorithm to rank people who are allegedly at a high risk of gun violence activity. The program had over 400,000 residents by its peak, most of whom were included without any criminal background, and research revealed that the Heat List continued racial profiling in the pretext of data-driven policing³³.

The Office of the Inspector General (OIG) audit established that the SSL was not scientifically reliable, generated inconsistent risk ratings, and lacked the ability to demonstrate any quantifiable effect on reducing gun violence, which provoked due-process concerns³⁴. People on the Heat List received extra police attention without the benefit of a procedure, which made them face the issue of due process concerns³⁵. The program was formally discontinued in 2019 because of questionable methodology, was not scientifically reliable, did not yield any measurable impact on gun violence, and generated more worries about due process.

7. LEGAL AND ETHICAL CHALLENGES

Predictive policing systems have serious underlying problems that will not go away with technological fixes. Although global reforms and new artificial intelligence regulations are developing, numerous legal, institutional, and ethical problems remain. This section highlights the key obstacles to fair and accountable predictive policing.

7.1 Algorithmic Bias and Discrimination

An ultimate regulatory issue consists of structural biases in predictive policing data and algorithms. Predictive systems are fed with historical policing records, which are the legacy of decades of discriminatory enforcement policies, and thus replicate racial and socioeconomic

³² F Zuiderveen Borgesius, 'Discrimination, Artificial Intelligence, and Algorithmic Decision-Making' (2020) 37 Computer Law & Security Review.

³³ Chicago Office of Inspector General (Chicago OIG), Review of the Chicago Police Department's Predictive Risk Models (2019).

³⁴ Chicago OIG, *supra* note 44

³⁵ *Ibid*

inequities³⁶.

The evidence confirms that algorithmic bias in predictive policing tools like COMPAS, PredPol, and the Gang Matrix is disproportionately assigning minority populations to the high-risk category, which subsequently generates additional enforcement data in those locations, thus solidifying the assumptions of the algorithm³⁷ and bias is further exacerbated by the feedback loop³⁸.

7.2 Lack of Transparency

There are a significant number of predictive policing systems which are black box in nature, and may be guarded as proprietary intellectual property, with no ability to have an external review of how such decisions are made, which sabotages the right to procedural fairness and due process³⁹.

Law enforcement agencies themselves do not fully understand how the risk scores or hotspot maps are created, and even where these schemes exist, interpretability and are explicitly prioritized by the emerging regulatory framework of the European Union, especially the AI Act, although in practice, they have been largely aspirational in policing terms⁴⁰.

It makes it impossible to challenge algorithmic evidence in court, which hinders the control of the rule of law and obscures the visibility of civil society⁴¹.

7.3 Absence of Clear Accountability Mechanisms

One of the regulatory gaps that persist is the inability to assign responsibility when predictive policing systems have discriminatory consequences⁴². Conventional liability systems expect to be able to determine human actors, but with algorithmic decision-making, human responsibility is diffused among software warehouse vendors, police, data scientists, and

³⁶ K Lum and W Isaac, 'To Predict and Serve?' (2016) 13(5) Significance 14–19.

³⁷ R Richardson, J Schultz and K Crawford, 'Dirty Data, Bad Predictions' (2019) 94 NYU Law Review 1–40.

³⁸ S Barocas, M Hardt and A Narayanan, *Fairness and Machine Learning* (MIT Press 2023).

³⁹ A Završnik, 'Algorithmic Justice and Due Process' (2021) 29(1) International Journal of Law and Information Technology 1–22.

⁴⁰ R Wexler, 'Life, Liberty, and Trade Secrets' (2018) 70 Stanford Law Review 1343–1429.

⁴¹ J A Kroll, J Hurlburt, S Barocas, E Wachten et al, 'Accountable Algorithms' (2017) 165 University of Pennsylvania Law Review 633–705.

⁴² K Yeung, 'Algorithmic Regulations' (2018) 31 Philosophy & Technology 1–14.

policymakers⁴³.

Courts had difficulty placing legal responsibility as is the case of *Loomis v. In Wisconsin*, when the courts admitted the application of a proprietary algorithm but claimed no direct liability to its shortcomings⁴⁴.

The regulative scholars propose a chain of accountability model that could be used to regulate AI, which includes the duty to show transparency and audit trails, the liability of the vendor in cases where the detrimental effects of systems are proven, and so on⁴⁵.

7.4 Violation of Privacy and Surveillance Concerns

The systems of predictive policing rely on mass data aggregation that incorporates criminal records and social services data, CCTV systems, phone metadata, and in some cases private-sector data⁴⁶.

This expansive surveillance model creates significant privacy risks, especially when the aggregation of data collection is not well authorized by law or publicly accessible⁴⁷.

The mass integration of data under the guise of predictive analysis may harm the very premises of fundamental protection of rights as the cases of the Netherlands SyRI judgment reveal, when applied in an unproportional and unprotective manner⁴⁸. In most countries, the predictive tools are disproportionately used to survey marginalized communities, which effectively become used to constant surveillance⁴⁹.

Moreover, predictive systems promote pre-emptive policing, in which people are the focus of law enforcement not because they have committed a crime, but because an algorithm has labelled them as being at risk⁵⁰. This should be avoided by a more privacy-by-design mindset.

⁴³ S Larsson, 'Principles of Responsible AI' (2020) 4 Journal of Responsible Technology 1–10.

⁴⁴ *State v Loomis* 881 NW2d 749 (Wis 2016).

⁴⁵ A Mantelero, 'AI and Human Rights' (2018) 34 Computer Law & Security Review 218–226.

⁴⁶ S Brayne, *Predict and Surveil* (Oxford University Press 2021).

⁴⁷ J Stanley and B Steinhardt, *Bigger Monster, Weaker Chains* (ACLU 2012).

⁴⁸ Amnesty International, *Trapped in the Matrix* (2018).

⁴⁹ B E Harcourt, *Against Prediction* (University of Chicago Press 2008).

⁵⁰ D Solove, 'Privacy Harms Us' (2021) 101 Boston University Law Review 793–857.

7.5 Inadequacy of Existing Data Protection Frameworks

Most jurisdictions have introduced general data protection regulations, including GDPR in Europe, LGPD in Brazil, and POPIA in South Africa, but these rules are not explicitly oriented around predictive policing. In addition, the existing legislation seldom requires algorithmic impact evaluation or external auditing prior to implementation⁵¹. And even in cases when the assessment does exist, it is frequently an internal report with lower levels of transparency.

The absence of binding sector-specific standards still causes predictive policing systems to develop at a more rapid rate than legal protection, which has left a vacuum in regulation⁵².

7.6 International Cooperation Deficits

The spread of predictive policing technologies is growing swiftly across the globe, frequently sold to the developing states by Western privately-owned corporations with little or no legal protection⁵³. Global collaboration in the field of policing algorithms is low⁵⁴.

No specific global framework regulates algorithmic policing, and even those bodies that have expressed some general AI principles, like the UN Human Rights Council or OECD, do not regulate the cross-border movement of data and technology, enabling companies to seek shelter in jurisdictions with lower legal standards⁵⁵. Cross-border data flows and technology transfers make it more difficult to regulate algorithmic policing.

8. CONCLUSION AND RECOMMENDATIONS

Predictive policing demonstrates both the promises and perils of AI-enabled policing. Predictive policing has the potential to lead to benefits—better use of resources, better efficiencies, and better use of data to drive decisions but it also has importantly large risks algorithmic bias, an opaque decision-making process, and inadequate oversight. A comparison of a variety of global jurisdictions shows that there is a current patchwork of legal frameworks protecting accountability, transparency, and rights, jurisdiction to jurisdiction and, sometimes,

⁵¹ M Veale and L Edwards, 'Algorithms and Accountability' (2018) 34 Computer Law & Security Review 398–409

⁵² F Zuiderveen Borgesius, 'Discrimination and AI' (2020) 37 Computer Law & Security Review.

⁵³ S Feldstein, *The Rise of Digital Repression* (Carnegie Endowment 2019).

⁵⁴ N Smuha, 'EU and Global AI Governance' (2021) 45(6) Telecommunications Policy.

⁵⁵ Organisation for Economic Co-operation and Development (OECD), *OECD Principles on AI* (2019).

even state to state.

Case studies in Chicago, Los Angeles, the U.K., and Europe indicate that predictive systems are perpetuating existing inequities, as well as not meeting our most basic fairness normative expectations. India lacks any kind of regulatory architecture to pursue these same issues, despite the interest in AI-enabled policing.

9. RECOMENDATIONS

To provide equity, accountability, and protections for rights in policing, this paper recommends these reforms:

9.1. Strategic Policy Actions

1. Mandatory Algorithmic Transparency

Governments would require:

- the logic of the model and data used to train the model to be shared;
- to subject the model building to independent audit scrutiny; and
- To adopt explainable AI methods to help create human understanding.

2. Stronger Anti - discrimination Standards

- It is critical that laws ban algorithmic-based forms of discrimination and shift the burden to the deployer of the system to demonstrate the reliability of the system to not be discriminatory.

3. Clear Accountability Pathways

Statutes should define:

- who vendors are liable to;
- what duties police departments have; and
- What remedies can be made available to victims and others.

4. Rights-Based Regulatory Structures

The EU has:

- Data Protection Impact Assessments (DPIAs) for drone use;
- Constraints on processing sensitive data; and
- Oversight authorities for AI are used by private actors and the police.

5. Ethical Guidelines and Human Oversight

- Finally, police agencies should implement - Human-in-the-loop decision-making;
- Continual ethics training on AI; and
- Wariness and strict limits on predictive tools involving individuals.

6. Data Governance and Community Ownership

Finally, communities (particularly those most affected by policing) should have representation on:

- Data governance committees;
- Oversight processes; and
- Evaluation of fairness in algorithms and risks of algorithmic biases.

9.2. Future Research Directions

Scholarship in the future should focus on:

- Developing models of AI governance that are India specific.
- Evaluating long term effects of predictive policing on marginalized communities.
- Creating technological feasibility for transparent and explainable AI.

- Investigating global models of policing standards pertaining to AI across borders.

Predictive policing will exist at the nexus of technology, law, and ethics. A future with accountability necessitates statutory safeguards, ethical commitments, and diverse governance.

BIBLIOGRAPHY

Books

- Ferguson A, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press 2017).
- O’Neil C, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown 2016).

Journal Articles

- Ensign D, Friedler S, Neville S, Scheidegger C and Venkatasubramanian S, ‘Runaway Feedback Loops in Predictive Policing’ in FAT Conference Proceedings (2017).
- Joh E, ‘Policing Numbers: Big Data and the Fourth Amendment’ (2016) 89 *Washington Law Review* 35–68.
- Lum K and Isaac W, ‘To Predict and Serve?’ (2016) 13(5) *Significance* 14–19 <https://doi.org/10.1111/j.1740-9713.2016.00960.x>.
- Richardson R, Schultz J and Crawford K, ‘Dirty Data, Bad Predictions’ (2019) 94 *NYU Law Review* 192–233.
- Selbst A, ‘Negligence and AI Predictions’ (2017) 76 *Maryland Law Review* 121–173

Reports

- Bhandari V and Sinha A, *AI and the Criminal Justice System in India* (Centre for Internet & Society 2020).
- European Union Agency for Fundamental Rights, *Getting the Future Right – Artificial Intelligence and Fundamental Rights* (2021).

Statutes & Regulations

- European Union, *AI Act (Regulation on Artificial Intelligence)* (2024).
- European Parliament, *General Data Protection Regulation (EU) 2016/679* (2016)

Case Law

- *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.
- *United States v Curry* 965 F.3d 313 (4th Cir 2020).
- *HiQ Labs v LinkedIn* 938 F.3d 985 (9th Cir 2019)