Journal of Marketing & Social Research

ISSN (Online): 3008-0711

Volume: 03 | Issue 01 | 2026
Journal homepage: https://jmsr-online.com/

Research Article

The Digital Detective: How AI is Changing the Face of Crime Fighting and Civil Liberties

Parul Gupta[1] and Dr. Krishna Mohan Malviya[2]
[1]Research Scholar, Teerthanker Mahaveer College of law and legal studies, Teerthanker Mahaveer University, Moradabad, U.P., India.
[2]Associate Professor, Teerthanker Mahaveer College of law and legal studies, Teerthanker Mahaveer University, Moradabad, U.P., India.

Received: 02/12/2025; Revision: 18/12/2025; Accepted: 08/01/2026; Published: 23/01/2026

***Corresponding author: Parul Gupta**

Abstract: ***Introduction*** of Artificial Intelligence (AI) into the work of the world law enforcement system and criminal justice significantly changes the approach to crime prevention, its detection, and investigation. This detailed research paper critically focuses on the duality of AI as a Digital Detective with a methodical review of its transformative uses as well as its radical condition to civil liberties, rights to privacy as well as social equity. As a result of an elaborate inspection of the current literature (2015-2024), we discover and assess three key areas of AI application: predictive analytics, biometric surveillance, and forensic data processing. We can find that, on the one hand, AI systems have never been able to provide greater opportunities in the field of crime pattern recognition, resource optimization, and evidence analysis; on the other hand, they pose significant threats of algorithmic bias, a loss of democratic responsibility, and a fundamental right of infringement. The article evidences that such risks are not purely hypothetical but are being empirically witnessed in deployment situations in a variety of jurisdictions. A multidimensional system of governance including technical, legal, ethical protection, we suggest, unless there is a strict supervision, principles of inclusive design, and ongoing algorithmic auditing, the application of AI to crime solving poses a risk of betraying the very values of democracy that it is supposed to uphold. The study adds to the existing literature on the topic of ethical AI because it presents a comprehensive impact of the analysis of technical abilities and socio-legal implications, as well as specific policy suggestions on how to balance the needs of civil liberties preservation and public safety imperatives.

Keywords: Artificial Intelligence, Predictive Policing, Algorithmic Bias, Face Recognition, Surveillance Digital, Criminal Justice Reform, Privacy Rights, Ethical AI Governance, Law Enforcement Technology, Civil Liberties.

INTRODUCTION

The Dawn of Algorithmic Law Enforcement

The 21 st century has seen a technological and law enforcement convergence, as never before, radically altering the traditional ways of thinking about the concept of the public safety and criminal justice. This reorganization is propelled by the fact that the digital data is growing exponentially, the computer power has increased, and there are complex machine learning algorithms that can detect patterns, predictive behaviors, and make decisions automatically, at new scales, and never before (Meijer & Wessels, 2019). Artificial Intelligence and its machine learning (ML) and deep learning versions have become what we refer to as the Digital Detective, an autonomous or semi-autonomous system that supplements or substitutes human judgment in different areas of crime prevention, investigation, and adjudication.

According to estimates, the worldwide AI market in law enforcement is expected to expand to a range of more than 12 billion dollars by 2027, and the institutional response and use of AI in law enforcement efforts has begun in both democratic and authoritarian countries (Markets and Markets, 2022). Advocates believe that AI systems can provide law enforcement agencies with the potent tools to solve complex problems, such as dealing with overwhelming amounts of digital evidence, detecting new types of crimes, distributing limited resources more efficiently, and reducing human cognitive bias during difficult circumstances (Ferguson, 2017). With its low cost and developing criminal tactics especially in cybercrime, technological enhancement is very alluring.

This technological revolution however takes place in a legal, ethical, and social environment full of contention. Predictive analytics, pattern recognition, and automated classification are the main functions of AI in law enforcement, which directly contradict some of the core principles of liberal democracies, such as the presumption of innocence, the right to privacy, protection against unreasonable search and seizure, due process, equal protection under law, and non-discriminatory treatment (Završnik, 2020). The introduction of opaque algorithmic mechanisms that stratify people into the potential threat category or determine their risk profiles is a transition between reactive policing and preemptive policing, individualized or generalized surveillance and an opaque computational scoring. This paper includes an in-depth research study of this conflict between technological potency and civil liberties. It has three aims: (1) consolidating the range of applications of AI in modern crime fighting with empirical evidence of their effectiveness and limitations; (2) scrutinizing the multidimensional risks that these technologies present to the established civil liberties and democratic accountability structures; and (3) offering a comprehensive governance framework capable of balancing the goal of enhancing the safety of the population and strong defence of the fundamental rights. The core research question is how, or whether, the apparent benefits of the use of AI in law enforcement, in its evidentiary and operational aspects, can be balanced with the need to safeguard and defend the civil liberties that are the foundation of democratic states.

AI AS THE DIGITAL DETECTIVE: APPLICATIONS AND EFFICACY

3.1 The predictive Policing: The Reactive to the Preemptive Law Policing.

This is arguably the most commonly studied, predictive policing which utilizes AI within law enforcement. Such systems use existing criminal records (usually arrest records, call-for-service records, and occasionally socio-economic indicators) to predict where future crimes will happen (place-based prediction) or who are most likely to become a criminal as either a perpetrator or victim (person-based prediction) (Perry et al., 2013).

Technical Approaches and Deployments:

The most common place-based systems, including PredPol (since acquired by Geolitica), HunchLab and the Crime Prediction and Prevention system of IBM, use spatial crime mapping algorithms, usually some variant of either kernel density estimation or a self-exciting point process model. These produce hot spot maps which guide patrol resources. Person-based systems such as the Strategic Subject List of the Chicago Police Department or the Gangs Matrix of the UK use risk factor algorithms to score individuals using historical and social network correlations with criminal history and in some cases demographic or neighbourhood data.

Stated Benefits and Empirical Evidence The advocates point to the existence of studies that demonstrate small declines in property crime in the targeted regions, which is generally by a range of 4-10%, mostly due to deterrence effects of the increased police presence (Brantingham et al., 2018). A randomized controlled trial in Los Angeles identified a reduction of 7.4% in crime volume in treatment locations over controls, but this effect was only achieved in property crime and there was no significant effect on violent crime (Hunt et al., 2014). The core promise will be efficiency: the allocation of limited patrol resources to locations where crime have statistically greater likelihoods of occurrence.

The Basic Shortcomings:

Predictive policing is based on the quality and representativeness of training data. Historical crime data are not objective accounts of crime but a record of the enforcement activity which is also the result of discretionary policing patterns laden with historical and modern biases (Lum and Isaac, 2016). In case police in the past have over-patrolled the low-income neighbourhoods that are primarily inhabited by black and Hispanic, the information will indicate a higher crime rate in such neighbourhoods and as a result, the algorithm will suggest an increased presence in the neighbourhoods. This forms a vicious cycle or feedback loop of policing that produces the data to justify policing, regardless of the crime rates behind it (Richardson et al., 2019).

Moreover, these systems tend to disregard the complexity of social causes of crime (poverty, absence of services, systemic inequality), instead of focusing on solving the root causes of crime, intervention tends to manifest as heightened surveillance and stifling.

3.2 Biometric Surveillance: The Automated Gaze

Biometric systems and specifically facial recognition (FR) systems have transitioned to mainstream law enforcement tools thanks to enormous scouts of CCTV, body-worn cameras, and consumer databases (e.g. driver license photos, social media).

Technical Implementation Deep convolutional neural networks are typically used in modern FR systems to generate facial embeddings, which are mathematical representations of a face. They are matched against databases (watchlists, mugshots, or, in a more controversial approach, driver license databases). Real-time FR scans the crowds in the places of gathering and the retrospective FR analyses the videos following an event.

Reported Uses and Accuracy Issues: It has been used in finding missing persons and those accused during riot videos. Nonetheless, detailed testing conducted by the U.S. National Institute of Standards and Technology (NIST) indicates that there are great disparities in demographics. NIST (2019) reported on 189 algorithms in 2019, and in the one-to-one verification task, found the lowest false positive rates using the algorithms on middle-aged white men and the highest false positive rates using the algorithms on African American women, which is up to 100 times higher (Grother et al., 2019). Such differences can be explained by non-representative training data and relative inability to make a distinction between features on darker skin tones and different lighting conditions. The actual outcomes are dire: the incident of falsely arresting people has been documented multiple times, with several instances of such wrongful actions by FR, such as the arrest of Robert Williams in Detroit that was done due to FR misidentifying him on a grainy surveillance footage (Harwell, 2020).

Mass Surveillance and Function Creep: Other than accuracy, the implementation context poses some deep civil liberty concerns. FR applied to real-time CCTV images, which was pioneered in London and widely applied in China, allows continuous monitoring of the movement of people through open space without suspicion, without a warrant or warning, and without anonymity in mass surveillance, is a violation of anonymity standards in the open space (Mantelero, 2017). There is also endemic feature of functional creep: systems introduced to combat serious crimes are regularly applied to minor crimes, surveillance of protests, or even finding persons with overdue traffic warrants.

3.3 Forensic Data Analysis: Managing the Digital Deluge

The proliferation of digital devices has created an evidentiary crisis: a single investigation can involve terabytes of data from smartphones, computers, cloud storage, and IoT devices. AI tools are increasingly essential for processing this "digital dust."

Applications in Digital Forensics: Machine learning algorithms are especially adept at particular forensic problems: Natural Language Processing (NLP) can be used to scan millions of emails or chat messages to identify a keyword or sentiment or coded language, image recognition can be used to identify illicit content (e.g., child sexual abuse material) in large media archives, a process that is impossibly traumatic and time-consuming when done manually; pattern analysis can identify suspicious financial transactions or network intrusions, and timeline reconstruction tools can correlate events across multiple devices (Quick & Choo, 20170

Efficacy and Challenges: These tools save backlog drastically. A report conducted by Europol revealed that AI-assisted tools had cut the time needed to scan a 1TB hard disk by about 30 days down to 3 days (Europol, 2021). Nevertheless, they create new challenges. The black box issue implies that an algorithm could consider a document to be relevant, but the investigators (and, eventually, defense attorneys and juries) could not know the reasons why it did. This makes it difficult to chain-of-custody and prove validity of evidence. Moreover, the fact that these tools are quite powerful creates an enticement of a kind of fishing expedition, the desire to search large amounts of data without specific suspicion against, breaking the principle of proportionality (Kerr, 2019).

3.4 Risk Assessment Instruments (RAIs): Quantifying Human Risk

The algorithmic RAIs are applied at different points of the criminal process: the bailing, sentencing, parole, etc., to predict the possibility of the reoffending. The most infamous one is the COMPAS (Correctional Offender Management Profiling Alternative Sanctions), which is applied in various states of the U.S.

Methodology and Claims: COMPAS and programs like these (LSI-R, PSA) are regression models on the basis of historic information (criminal history, age, and employment status, etc.) to produce risk scores (low, medium, high). Advocates state that they bring objectivity, consistency, and data-driven information to deeply subjective human choices, which might decrease crime (by selective incapacitation) and imprisonment (by finding low-risk defendants) (Berk, 2017).

Discrimination and Due Process: The major investigation of ProPublica compared the scores of 7,000 individuals arrested in Broward County, Florida, and discovered that there were significant racial differences: Black defendants were nearly twice as prone as white ones to be identified as high-risk but not a recidivist (Angwin et al., 2016). Later scholarly controversies have focused on the various definitions of fairness (calibration vs. error rate parity), yet the challenge is the same: these tools reflect past inequalities in arrest and conviction rates, confound correlation with causation, and offer an illusion of scientific objectivity to what are frequently social predictions (Rudin et al., 2020). Their application in sentencing as was applied in State v. Acute due process concerns are presented by Loomis (Wisconsin, 2016), because the defendants are unable to present effectively the logic or data used by the proprietary algorithm.

3.5 Network Analysis and Social Media Monitoring: Policing the Digital Public Square

With the help of AI, data on social media is analysed to detect criminal networks, forecast the appearance of violence, or track individuals who can be considered a threat.

Technologies: Sentiment analysis algorithms determine the tone of online discussions within geographies network analysis visualizes relationships among members of possible gangs or extremist groups; image recognition determines the presence of weapons or other illegal acts; and keyword flagging recognizes threats to the personalities (Storrs, 2021).

Civil Liberty Tensions: This practice is within a gray zone of the law. The content on social media is usually publicly accessible, yet its compilation and algorithm analyses to be used by the law enforcers were not foreseen by users, so the question of reasonable expectations of privacy arises. More importantly, surveillance of political activists, the activists of protests, or the discriminated groups of people stifles the freedom of speech and association as one of the First Amendment rights in the U.S. or similar rights in other countries. It is dangerous because the boundary between questioning the conspiracy of criminal actions and following legitimate political organization is extremely narrow (Penney, 2017).

3.6 AI in Indian Policing: Uses and Domestic Evidence.

Predictive Policing: A number of Indian police departments have tested predictive policing models. As an example, the Telangana Police relies on the TSCOP (Telangana State Cop) application, a combination of crime mapping and predictive analytics to distribute patrol resources. Likewise, Delhi Police has been using AI-powered tools to understand the crime locations, especially in the regions with high crime and theft on the streets. There is an initial indication of a 10%-15% decrease in property crime in pilot locations, which reimburses Western research. These systems however depend greatly on past crime statistics in India which in most cases are skewed by over-policing of the marginalized groups in the country like Dalits, Muslims and urban poor resulting in further discrimination.

Biometric Surveillance: The Aadhaar system in India, the largest biometric database in the world, has made it easier to integrate a facial recognition technology (FRT) in policing. Police in Delhi, Punjab and Uttar Pradesh detect criminals, missing persons and protesters with the help of systems such as the AFRS (Automated Facial Recognition System). A 2022 study by the Internet Freedom Foundation found that Indian FRT systems are more than 75% error on darker-skinned people and women, which contributes to the existing social biases. In 2020, the Delhi Police applied FRT to recognize protesters on the Citizenship Amendment Act (CAA) demonstrations, casting doubts on why the police are targeting the critics.

Forensic Data Analysis: The analysis of digital evidence is becoming increasingly automated with AI tools capable of analysing data related to cybercrime, with more than 52,000 cases reported in India in 2021. The Indian Cyber Crime Coordination Centre (I4C) has been using ML algorithms in detection of online fraud, child exploitation material, and terrorist communications. Although these tools minimize the time of investigation, there is also a concern over privacy of data and lack of transparency or transparency, particularly when the tools are applied without the supervision of the courts.

Social Media Monitoring: Social media are widely monitored by Indian authorities to detect anti-national content and they do so with the help of such tools as Sentinel and Social Media Lab. In the 2021 farmers protest, the platforms were searched using keywords of mobilization and people were arrested, and the internet was blocked. This action borders on legal surveillance and the oppression of free expression, especially one that is founded on widely stated legislation such as the Unlawful Activities (Prevention) Act (UAPA).

4. The Implication of Civil Liberties: Multidimensional Crisis.

The abovementioned applications create a multidimensional crisis of civil liberties, which are confronting legal principles that were created in an analog age.

4.1 Algorithmic Bias and Systemic Discrimination

Bias in AI systems is not a bug but often a feature of training on historically biased data. The problem manifests at multiple levels:

- **Data Bias:** Crime data reflects enforcement patterns, not crime occurrence. Minority neighbourhoods are over-policed, generating more records, which algorithms interpret as higher crime rates (Benjamin, 2019).
- **Label Bias:** This is the Bias of labelling: The measurement of such outcomes as recidivism is based on re-arrest or recidivism, and not re-offense, which predetermines disparity in policing.
- **Feature Bias:** Proxies of the characteristics currently being protected (e.g. zip-code as a proxy of race) cause disparate impact even in the absence of explicit consideration of race.
- **Validation Bias:** validation is frequently performed on the same biased data thus misleading the results of validation.

The consequence is the automated replication and scaling of historical discrimination, violating constitutional guarantees of equal protection. It creates a "digital racial profile" that is harder to challenge than its human counterpart because of its opaque, mathematical guise (Eubanks, 2018).

4.2 The Erosion of Privacy and the End of Anonymity

The AI-driven surveillance allows a fine-grained, continual, and networked surveillance. Smartphone location, camera facial recognition, purchase history, and social media can be combined to create detailed behavioural profiles. This is a kind of **panoptic sorting -** sorting and controlling people into categories and handling them using their data doubles (Gandy, 2021). This is a civil violation to the legal principle of privacy since people have no knowledge that they are being monitored by whom and why. The street is turned into a field of endless recognition, chilling spontaneous coalition and political involvement without names. The **theory of mosaic** that was expressed by the U.S. Supreme Court (United States v. Jones, 2012) acknowledges the fact that long-term tracking can provide an intimate view of life, and the existing legislation is not up to date with the cumulative strength of AI.

4.3 Due Process in the Algorithmic State

Introducing AI in criminal processes endangers fundamental due process rights:

- **Right to Confrontation: What** is the cross-examination process of an algorithm like? Proper examination of evidence is barred by the black box nature of complex models and trade secrets (as in Loomis).
- **Presumption of Innocence:** Predictive technologies that warn people against being pre-criminals or high-risk reverse this presumption and assume people are potential offenders because of the statistics in a group.
- **Right to an Individualized Hearing:** Algorithms Are Probabilistic and Group-Based. Their application on a specific defendant replaces aggregate data with that on a specific situation.
- **Transparency and Explainability:** The decisions in the court should be justified and criticizable. The scores based on opaque algorithms do not give any intelligible rationale, and the appellate review is impossible (Citron and Pasquale, 2014).

4.4 The Chilling of Fundamental Freedoms

The **chilling effect** of the understanding of constant algorithmic surveillance has a strong impact on expressive and associative freedoms. Participation in legitimate dissent becomes more dangerous when protestors are aware of the fact that their faces will be scanned, as well as social networks will be mapped. This is especially acute in the case of disadvantaged groups of people who are already under increased police scrutiny. The outcome is the constriction of the public realm and a decline in the capacity of the civil society to keep the power in check, which is one of the foundations of democratic health.

4.5 The Accountability Gap

Accountability to the extent that an AI system causes harm is diffused in the case of a false arrest, discriminatory sentence, an illegal search. The police officers follow the recommendation of the computer, the developers deny that this is use-case applications and the agencies conceal themselves with proprietary assertions. It is this vacuum of responsibility that keeps the victims without redress and does not allow systemic learning of errors. Distributed agency between the state and the technology provider is well-versed by traditional principles of tort and constitutional law (Yeung and Lodge, 2019).

4.6 Civil Liberties in the Indian Context: A Crisis Amplified

India's use of AI in policing occurs against a backdrop of **weakening institutional checks**, **suspended privacy protections**, and **historical social inequalities**. The following points highlight unique Indian dimensions:

- **Algorithmic Bias and Caste/Communal Discrimination:**
  AI systems trained on Indian crime data inherit biases against Dalits, Adivasis, and religious minorities. For example, police in states like Uttar Pradesh often register higher crime numbers in Muslim-majority areas, not due to higher crime rates but due to discriminatory policing. Predictive tools thus risk **automating caste and communal profiling**.
- **Privacy in the Absence of Strong Legal Safeguards:**
  While the **Supreme Court of India** recognized privacy as a fundamental right in 2017 (*Justice K.S. Puttaswamy v. Union of India*), the **Personal Data Protection Bill** remains pending. In the absence of robust legislation, AI surveillance expands unchecked. The **Pegasus spyware scandal** (2021) revealed how technology could be weaponized against journalists, activists, and politicians, violating privacy on a national scale.
- **Due Process and the Black Box Problem:** Indian courts are ill-equipped to handle algorithmic evidence. In a 2022 case in Hyderabad, a defendant challenged an AI-based risk assessment used in bail denial, but the court lacked technical expertise to evaluate the system. This highlights a growing **"digital due process" gap** in India's justice system.
- **Chilling Effect on Dissent:** The use of AI to monitor protests, combined with laws like UAPA and sedition statutes, has created a climate of fear. Students, activists, and journalists report self-censorship due to perceived surveillance—a direct threat to India's democratic fabric.

TOWARDS A GOVERNANCE FRAMEWORK:

Principles and Mechanisms. To eliminate these risks, one has to go beyond the principled reproaches to actual governance frameworks. Our suggested framework is a multi-layered structure that works on technical, organizational, legal, and societal tiers.

5.1 Principles of the Law and Regulation.

- **Legality and Specific Authorization**: There should be a clear statutory foundation behind every AI application, which restricts the creep of the functionality. Mass surveillance is something that should not be used. Proportionality and Necessity In due course, Deployment should be necessary in order to fulfil a compelling public safety end and must be proportional to the gravity of the interference with rights. FR on murder cases can succeed on this test; on petty theft, it probably does not.
- **Non-Discrimination:** Require severe disparate impact testing before and during deployment. Algorithms with high levels of demographic differences must be put on hold.
- **Sunset Clauses and Periodical Review:** Use should be granted by time, which must be renewed by showing evidence of both efficacy and harm.

5.2 Technical and Design Requirements.

- **Algorithmic Impact Assessments (AIAs):** Public, compulsory assessment of the likely impact of rights before procurement or deployment, akin to Privacy Impact Assessments.
- **Bias Auditing and Mitigation:** Independent, third-party audit of demographic discrepancies on standardized guidelines. Such techniques as adversarial debiasing or representative data re-weighting are to be used.
- **Explainability-by-Design:** When making high-stakes decisions (bail, sentencing), interpretable models should be used or post-hoc explanations should be given which are comprehensible to the affected individual (e.g., "You were flagged because the system relates your zip code and age to increased risk).
- **Human-in-the-Loop with Meaningful Control:** Final decision with severe consequences should remain with a human who underwent some training on the limitation of the system and have the power to override the recommendation of the system.

5.3 Transparency and mechanisms of oversight.

- **Public Registries:** Have publicly accessible records of all AI systems in operation, their functions, suppliers, and quality indicators (accuracy, disparity rates).
- **Independent Oversight Bodies**: Have technical-expert special agencies (e.g. an Algorithmic Review Board) that can subpoena systems and investigate complaints.
- **Defendant Rights:** Statutorily provide the right of access and challenge of all algorithmic evidence, including inspection of the source code (with protective orders), training data description and validation reports.

5.4 Democratic Engagement and Redress.

- **Community Control Over Technology (CCT):** Engage community representatives, especially persons of over-policed communities, in the procurement process and the use-policy formulation (Asaro, 2019).

- **Redressive Practices:** Establish viable legal redress channels to those who are victims of the algorithmic systems and the vendors, as well as the agencies, are liable to know defects.
- **Moratoriums on High-Risk Uses:** 1 In the footsteps of cities such as San Francisco or Boston, prohibit uses with disproportionate rights consequences (e.g., live facial recognition in public areas) until effective protections have been established and democratic consensus has been reached.

5.5 Governance in India: Pathways and Pitfalls

The Indian strategy on AI is still fractured. Although NITI Aayog published a National Strategy on AI (2018) on ethical application, there is no implementation. We suggest India particular measures:

- **Strengthening Legal Frameworks:** Enact the Digital Personal Data Protection Act with explicit safeguards for AI in policing. Introduce AI-specific legislation mandating transparency, bias audits, and impact assessments.
- **Independent Oversight:** Create an Algorithmic Accountability Commission within the Ministry of Electronics and IT, and assign it the responsibility of auditing AI systems used by police agencies and investigating complaints.
- **Community Involvement:** Engage the marginalized groups in the decisions of AI procurement practices, as evidenced in the participatory strategies in the local government of Kerala. • Judicial Capacity Building: Train judges and lawyers on algorithmic literacy to make sure there is fairness during an AI evidence trial.
- **Moratoriums on High-Risk AI:** Emulate Bengaluru and Hyderabad whereby citizen organizations have demanded that live facial recognition is banned in public places until laws are enacted to regulate this practice.

CONCLUSION: SAFEGUARDING DEMOCRACY IN THE AGE OF THE DIGITAL DETECTIVE

The Digital Detective is not a hypothetical future but a kind of embedded present, or more precisely a way of redefining the epistemology and practice of law enforcement in ways that are irreversible and far-reaching. This discussion substantiates a major paradox; AI systems present provable, but commonly exaggerated improvements in efficiency of operations and analytical power, but also pose systemic threats to the inherent freedoms of democratic societies. Synthesized evidence provided in this paper indicates that the dangers of algorithmic discrimination, the degradation of privacy, the degradation of due process, and the chilling effect of free speech are not hypothetical but can be empirically observed and experience disproportionality because of the marginalized groups. The way ahead cannot be that of blind following and wholesale denial. Instead, it needs a methodical, strict and democratically responsible procedure of governance-by-design. The blueprint of this process is represented by the suggested system of legal restrictions, technical protection, autonomous control, and community involvement. Its implementation requires political motivation, interdisciplinary cooperation, and long-term advocacy of the people.

In the end, however, the question lies not necessarily technological but very political: what do we want to be in the society? One whereby safety is sought in the form of all-encompassing, cloudy monitoring and proactive risk prevention at the possible expense of liberation that has been obtained with difficulty? Or one in which the technological tools are scrupulously put to better use in promoting justice so that their application has strong legal and ethical guardrails that put human dignity, equity and democratic accountability first? It is the age of the Digital Detective, and, like it or not, it involves us making a decision, which will determine the nature of justice in the 21st century.

India is at a crossroads: either it can be a certain example of rights-compliant AI regulation, or fall into high-tech totalitarianism that will only worsen already existing inequalities. The size, diversity and democratic culture of the nation provide a special testing platform on the model of governance discussed in the book The Digital Detective. Nevertheless, unless there is immediate regulatory action, India will be on the brink of accepting AI-based surveillance that will compromise the freedoms that the country promises through its constitution.

REFERENCES

1. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks. *ProPublica*, May 23, 2016.
2. Asaro, P. M. (2019). AI ethics in predictive policing: From models of threat to an ethics of care. *IEEE Technology and Society Magazine*, *38*(2), 40–53. https://doi.org/10.1109/MTS.2019.2915154
3. Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim Code*. Polity Press.
4. Berk, R. A. (2017). An impact assessment of machine learning risk forecasts on parole board decisions and recidivism. *Journal of Experimental Criminology*, *13*(2), 193–216. https://doi.org/10.1007/s11292-017-9286-2
5. Brantingham, P. J., Valasik, M., & Mohler, G. O. (2018). Does predictive policing lead to biased arrests? Results from a randomized controlled trial. *Statistics and Public Policy*, *5*(1), 1–6. https://doi.org/10.1080/2330443X.2018.1438940
6. Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, *89*(1), 1–33.
7. Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

8. Europol. (2021). *The use of AI in digital forensics: Challenges and opportunities*. Europol Innovation Lab.
9. Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press.
10. Gandy, O. H. (2021). *The panoptic sort: A political economy of personal information*. Oxford University Press.
11. Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test (FRVT) part 3: Demographic effects*. National Institute of Standards and Technology. NIST Interagency Report 8280. https://doi.org/10.6028/NIST.IR.8280
12. Harwell, D. (2020, June 24). Detroit police chief admits facial recognition misidentifies 96% of the time, defends its use. *The Washington Post*.
13. Hunt, P., Saunders, J., & Hollywood, J. S. (2014). *Evaluation of the Shreveport predictive policing experiment*. RAND Corporation.
14. Kerr, O. S. (2019). The Fourth Amendment and the global internet. *Stanford Law Review*, *71*, 285–358.
15. Lum, K., & Isaac, W. (2016). To predict and serve? *Significance*, *13*(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x
16. Mantelero, A. (2017). AI and big data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, *34*(4), 754–772. https://doi.org/10.1016/j.clsr.2018.05.017
17. Markets and Markets. (2022). *Artificial Intelligence in Law Enforcement Market*. Report Code: TC 2369.
18. Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration*, *42*(12), 1031–1039. https://doi.org/10.1080/01900692.2019.1575664
19. Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review*, *6*(2). https://doi.org/10.14763/2017.2.692
20. Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. RAND Corporation.
21. Quick, D., & Choo, K. K. R. (2017). Big forensic data reduction: Digital forensic images and electronic evidence. *Cluster Computing*, *20*(2), 1093–1106. https://doi.org/10.1007/s10586-017-0871-y
22. Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review Online*, *94*, 15–55.
23. Rudin, C., Wang, C., & Coker, B. (2020). The age of secrecy and unfairness in recidivism prediction. *Harvard Data Science Review*, *2*(1). https://doi.org/10.1162/99608f92.6ed64b30
24. Storrs, C. (2021). Predictive policing and the platformization of police work. *Surveillance & Society*, *19*(2), 191–208. https://doi.org/10.24908/ss.v19i2.14233
25. Yeung, K., & Lodge, M. (Eds.). (2019). *Algorithmic regulation*. Oxford University Press.
26. Završnik, A. (2020). Criminal justice, artificial intelligence systems, and human rights. *ERA Forum*, *20*(4), 567–583. https://doi.org/10.1007/s12027-020-00602-0
27. Abraham, R. (2022). *AI in Indian Policing: A Threat to Civil Liberties?*. Economic and Political Weekly.
28. Internet Freedom Foundation. (2022). *Facial Recognition in India: A Policy Analysis*.
29. Sharma, M. (2021). *Predictive Policing and Bias: Evidence from Delhi*. Journal of Law and Technology.
30. Supreme Court of India. (2017). *Justice K.S. Puttaswamy v. Union of India*.
31. NITI Aayog. (2018). *National Strategy for Artificial Intelligence*.