Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

AI in Law Enforcement: Navigating the Crossroads Between Efficiency and Ethical Governance

Harsimar Kaur[a]

[a]Law Centre-1, Faculty of Law, University of Delhi, Delhi, India

Received 17 April 2026; *Accepted* 21 May 2026; *Published* 25 May 2026

In the labyrinth of the Criminal Justice System and Modern Governance, artificial intelligence is being hailed as a panacea for the pendency, investigative inefficacy and inadequate infrastructure that have been plaguing our governance and law enforcement structures. The assimilation of artificial intelligence into India's law enforcement and judicial system reflects a significant shift in the governing apparatus of this country; law enforcement in this digital era is undergoing major structural reforms and is entering the age of Algocracy- rule by algorithms. However, these reforms emerge at crossroads as, on one hand, systemic efficiency is being promised, but on the other hand, the fundamental safeguards guaranteed by the constitution are being threatened. As India is integrating artificial intelligence in its law enforcement framework from predictive policing, automated video surveillance and biometric identification to AI-powered forensic analysis, case management and algorithmic-assisted adjudication, it faces an intricate negotiation between efficiency, speedy crime resolution, constitutional values, algorithmic bias and ethical concerns like transparency and accountability. This paper aims to explore this complex conflux and critically analyse the efficacy of Artificial Intelligence in enhancing the productivity of our law enforcement systems, whilst scrutinising the ethical dilemmas, legal vacuum and policy gaps therein by navigating through the contours of algorithmic governance while drawing upon constitutional mandates and the Supreme Court's jurisprudential landscape.

Keywords: *artificial intelligence, predictive policing, algorithmic governance, algocracy, right to privacy.*

INTRODUCTION

In India, law enforcement systems are looking to artificial intelligence to gain an advantage in countering crimes that are evolving faster than the systems created to stop them. The criminal justice system is faced with structural challenges, with 55.8 million pending cases in the Indian Courts, overburdened police departments, and persistent investigative inefficiencies. Hence, to combat such systemic shortcomings, the governing structure is pivoting towards the aid of Artificial Intelligence as a corrective remedy. These AI systems are now assisting in predicting criminal activity, biometric identification, forensic analysis and courtroom transcription and judgment translation. The adoption of these systems is accelerating, their scope is expanding at an even greater pace, yet the constitutional ramifications remain insufficiently scrutinised.

The Hon'ble Supreme Court's jurisprudential landscape established that any executive action must satisfy the test of legality, legitimate aim, necessity and proportionality. In Maneka Gandhi v Union of India,[1] the Court held that 'procedure established by law' must be fair, just and reasonable. Any restriction on rights under Article 21 must also meet the tests of fairness and reasonableness under Articles 14 and 19.[2] The court, further, in Justice K.S. Puttaswamy v Union of India, through a nine-judge bench, unanimously held that 'Privacy has been held to be an intrinsic element of the right to life and personal liberty under Article 21 and as a constitutional value which is embodied in the fundamental freedoms embedded in Part III of the Constitution. Like the right to life and liberty, privacy is not absolute. The limitations which operate on the right to life and personal liberty would operate on the right to privacy. Any curtailment or deprivation of that right would have to take place under a regime of law. The procedure established by law must be fair, just and reasonable. The law which provides for the curtailment of the right must also be subject to constitutional safeguards.'

Hence, the threefold requirement (existence of law, legitimate aim and proportionality) for a valid law arises out of the mutual interdependence between the fundamental guarantees against state action's arbitrariness on the one hand and the protection of life and personal

[1] *Maneka Gandhi v Union of India* (1978) 1 SCC 248
[2] 'The right to life and personal liberty under Article 21: A timeline' (*Supreme Court Observer*, 26 June 2025) <https://www.scobserver.in/journal/the-right-to-life-and-personal-liberty-under-article-21-a-timeline/> accessed 13 April 2026

liberty, on the other.[3] These rulings do not establish mere abstract norms, but rather direct constitutional mandates that any apparatus through which the state exerts coercive power over individuals, whether human or algorithmic, must comply with.

The use of Artificial Intelligence in India's law enforcement landscape, though, promises advancements and a strategic edge; the legal and ethical foundations of these very systems are subjected to serious scrutiny. As these technological interventions pose critical questions, such as whether these tools preserve the right to privacy or normalise mass surveillance? Can algorithmic analysis uphold equality and transparency in law enforcement? Wouldn't these tools, which are trained on historical data, lead to systemic biases? Hence, this paper establishes that such interventions must be measured not only by their efficacy in predicting crimes but also by their adherence to constitutional values of equality, morality and procedural fairness.

ALGORITHMIC GOVERNANCE: RESHAPING TRADITIONAL DECISION MAKING FROM HUMAN DISCRETION TO ALGOCRATIC SYSTEMS

The Science behind Algorithmic Governance: Artificial Intelligence is defined by Russel & Norvig as the study of agents that acquire their perceptual abilities from their environment and act in accordance with their structural design tailored to meet specific goals.[4] Automated decision-making mechanisms are built upon machine learning workflows edified by deep learning techniques, which enable these AI tools to operate independently, learn from their own observations, and thereby evolve and advance their functioning.

Algorithmic Governance in Law Enforcement consists of 3 Interdependent Processes –

Building of Data Sets: Large amounts of structured and unstructured data spanning from historical criminal records, geographic coordinates, socioeconomic status, biometrics, to CCTV recordings, social media activity, emergency call logs and other such details are consolidated into centralised databases, which are then utilised and form the ingredients for the training of respective algorithms.[5]

---

[3] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

[4] Stuart J Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson Education Ltd 2022) ch 1

[5] 'Tracing the Rise of Predictive Policing in India' (*SFLC*, 26 February 2026) <https://sflc.in/tracing-the-rise-of-predictive-policing-in-india/> accessed 13 April 2026

Machine Learning: It is the process of training certain computational systems by exposing them to large datasets, whereby they independently detect patterns, correlations, regularities and anomalies and further apply these learned patterns to extrapolate and predict about the newly received data. [6]

Deep Learning: Within the ambit of machine learning falls one of its complex and advanced facets, i.e. deep learning. Deep Learning uses artificial neural networks with multiple interlinked layers that are somewhat designed and modelled on the architecture of the human brain. Empowering these ML models to identify and discern highly intricate patterns across vast datasets like image recognition, speech processing, behavioural pattern prediction, etc. It is through the synergy of these technological advances of machine learning and deep learning that steers the rhythm of algorithmic governance structure from predictive policing systems to facial recognition systems that are deployed across Indian states to assistive tools which are being used in Indian Courts.

Erosion of Reasoned Human Agency and Rise of Algocracy – An Ethical Challenge: The world is gradually advancing from Anthropocene, the age of humans, to the Algocenic era, the age of algorithms. Hence, the pervasive usage of Artificial Intelligence is no longer an improbable reality as it has subtly crept into every aspect of our lives. Algorithms have evolved into becoming an integral part of our law enforcement structure and public administration, giving rise to a new system of governance, i.e. 'Algocracy'. This rule by algorithms is characterised by the gradual replacement of human deliberation and discernment by automated data-driven algorithms in decision-making mechanisms for public administration. Ranging from predictive policing models that are trained on large data sets, further analysing and forecasting potential crime patterns and zones, to seamless automated legal assistance and case management models. These technological advancements are rapidly overtaking the tasks and functions that have always been performed by the cerebral capacities of human authority.

While this shift is being seen as a pivotal moment and significant step towards an efficient and streamlined law enforcement framework propelled by enhanced productivity, speedy redressal, improved accuracy and objective decision making, which shall remedy the

[6] Aurelia Colombi Ciacchi et al. (eds), *AI and Public Administration: The (legal) limits of algorithmic governance* (JuLIA 2025)

prevalent irregularities in the law enforcement system. A critical issue that is being overlooked is the possibility of potential harm that shall be caused as a consequence of reducing nuanced human examination and oversight to mere computation of data points characterised by historical biases. When this historically tainted data, which mirrors prolonged social injustices patterns of the society, such as those related to specific religion, race, caste, gender, or socioeconomic status, is used to train machine learning models, these models learn, reproduce, and often amplify these inequities, leading to unfair outcomes.

Hence, the significance of this shift does not lie merely in the novel solution it brings but also in the constitutional ramifications it poses. As per the Indian Constitution, the principle of Rule of Law is based on the ideals of liberty, fair treatment, due process, equity, equality and transparency.[7] Therefore, the use of automated data-driven mechanisms in the public administrative framework undermines the rule of law by replacing normative governance structure centred on legal reasoning, proportionality analysis, and contextually sound human decision making with opaque 'black box' systems where outcomes are determined by pattern identification across datasets of questionable provenance. The issue is not that automated systems are making the decisions; these systems indeed are enhancing the efficacy of our conventional governance structure, but this is being achieved at the cost of transparency and accountability, subverting the ethical values that the constitution guarantees.[8]

The Grey Area – Legal & Ethical Concerns: Algorithmic Governance doesn't operate in a value-neutral domain, being trained on historical datasets that reflect biases towards certain marginalised communities, localities populated by people belonging to certain castes or religious groups. These models learn to treat such demographic characteristics as prima facie predictors of criminality without reasoned judgment that is efficiently exercised by human agency. As a result, the choices exercised by the opaque operational framework of these models give rise to ethical concerns relating to bias, fairness, transparency and accountability. One of the most critical ethical concerns is the absence of meaningful consent

[7] Namrata Kandankovi, 'Rule of law and its Exceptions' (*iPleaders*, 11 June 2019) <https://blog.ipleaders.in/rule-law-exceptions/> accessed 13 April 2026

[8] Jaiveer Singh and Yagya Agarwal, 'Invisible Hand of Code: Reimagining Constitutionalism in the Age of Algorithms' (*NLIU Law Review*, 27 January 2025) <https://nliulawreview.nliu.ac.in/blog/invisible-hand-of-code-reimagining-constitutionalism-in-the-age-of-algorithms/> accessed 13 April 2026

as data of individuals is being collected via CCTV recordings, call records, demographic records or bank transactions for predictive profiling. The collection and usage of such data of individuals has not been consented to, nor have they been informed. Further, due to the black box structure of these algorithms, how decisions are being made by the algorithms impedes access to information as to how the state, via the use of these models, reached a particular decision, thereby directly violating the right to access information and know how the government works under Article 19(1)(a)[9].

The legal grey area surrounding these ethical shortcomings requires critical attention. India's current statutory framework was not developed to specifically accommodate this modern, sophisticated system of algorithmic governance. The Sensitive Personal Data & Information Rules 2011[10], under the ambit of the Information Technology Act 2000[11], addressed the collection and disclosure of sensitive personal data and information, which included biometric data such as facial patterns, fingerprints, etc. and financial information, among other things. SDPI Rules are exempt from law enforcement agencies that collect such data, but do not apply to corporations.

The IT Act 2000 addressed issues related only to cybercrime and intermediary liability, but made no explicit provision for automated algorithmic decision-making in state functions. The Digital Personal Data Protection Act 2023 (DPDPA)[12] is India's latest major legislative intervention in the data regulation sphere to come in decades, but it is still inadequate to regulate the use of AI in law enforcement owing to its structural limits. Section 17[13] enables the government to omit any state agencies from the data protection provision of the Act, citing national security, sovereignty or public order concerns. This empowers the state to deploy opaque algorithms, overlooking transparency and individual privacy rights protections mandated by the same Act for private entities. Furthermore, in comparison to global frameworks such as General Data Protection Regulation (GDPR) Article 22,[14] which provides individuals with the right to not be governed by decisions based solely on automated processing, the DPDP Act does not empower individuals to question the

[9] Constitution of India 1950, art 19(1)(a)
[10] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011
[11] Information Technology Act 2000
[12] Digital Personal Data Protection Act 2023
[13] *Ibid* s 17
[14] General Data Protection Regulation, art 22

decisions made exclusively by the automated models, nor does it address the right to explanation of how and the reasoning behind these algorithmic decisions.

In response to the growing concerns about algorithmic bias, transparency, accountability and the rising misuse of surveillance, a Private Member's Bill, namely the Artificial Intelligence (Ethics & Accountability) Bill 2025,[15] was introduced in the Lower House in December 2025 – suggesting the establishment of a statutory Ethics Committee and mandatory ethical reviews for surveillance systems and fines for AI misuse. It proposed a sound solution to the prevalent issue of lack of accountability and transparency in AI systems, but being a Private Member's Bill, its chances of being rigorously deliberated upon for enactment are bleak. Hence, when the above-stated regulatory gaps are put together, it creates an oversight vacuum where these ethical transgressions that require urgent attention go largely undervalued and unmet.

PREDICTIVE POLICING IN INDIA FROM ITS APPLICATION TO CONSTITUTIONAL INFIRMITIES

State-Level Implementation & Application: Predictive Policing is the most conspicuous and constitutionally consequential manifestation of a larger structural shift in conventional governance, i.e., algorithmic governance. Predictive Policing is the most prominent and contentious aspect of Algocracy, where advanced automated systems gradually replace human discernment in the sphere of public administration.

Its core concept is deceptively simple, whereby sophisticated algorithms predict where and by whom crimes are likely to be committed by examining historical data and real-time inputs, allowing for a proactive rather than a reactive policing. The underlying premise is that computational modelling yields more accurate and faster insights into criminal activities than traditional speculation exercises done by the officers. Optimising resource efficiency and preventing destructive criminal activity before it begins or further escalates at an aggravated level are the main outcomes desired by the predictive policing systems. It is due to this that the implementation and deployment of these systems has progressed across the Indian states at a rate that completely surpasses any regulatory structure.

[15] Artificial Intelligence (Ethics and Accountability) Bill 2025

Delhi Police's Crime Mapping, Analytics and Predictive System (CMAPS), developed in partnership with the Indian Space Research Organisation, collects data every three minutes from satellite feeds, the Dial-100 emergency helpline, and the Crime and Criminal Tracking Network Systems (CCTNS), generate real-time crime hotspot maps for patrol deployment. Further, the Delhi Police has E-Beat Book Integration with Automatic number plate recognition (ANPR). This system allows officers to scan license plates and quickly identify stolen vehicles, track fleeing suspects and solve crimes.[16]

Maharashtra deploys the Maharashtra Advanced Research and Vigilance for Enhanced Law Enforcement (MARVEL) system, which offers crime prediction models, CCTV analytics, OCR tools, object detection and metadata processing. MahaCrime-OS is one of a part of the MARVEL project that helps officers in drafting letters, scanning bank transactions, and identifying suspicious activity.[17] Uttar Pradesh on similar lines has deployed Trinetra 2.0 - an AI-powered facial recognition and criminal tracking system that works with U.P. Police interlinking data from data from prisons, district police, Government Railway Police (GRP), and the Under Trial Management System (UTMS), consolidating data of more than 9,00,000 criminals allowing field officers to access criminal histories, FIR details, and photos, and to identify unknown bodies it has further integrated CrimeGPT a conversational AI for quick retrieval of criminal dossiers. JARVIS, on the other hand, developed by Starqu, has enabled the UP police in detecting potential threats like violence, intrusion, pickpocketing, etc. by analysing CCTV footage.[18]

Hyderabad's Integrated People Information Hub (IPIH) aggregates biometric details, family information, bank transaction records, and passport data to build comprehensive predictive profiles.[19] Other States like Karnataka, Punjab, Rajasthan, Himachal Pradesh, Madhya

---

[16] Raj Shekhar Jha, 'Delhi Police's Template to Nab Criminals' *The Times of India* (15 July 2025) <https://timesofindia.indiatimes.com/city/delhi/delhi-polices-template-to-nab-criminals/articleshow/122524309.cms> accessed 12 April 2026

[17] 'MahaCrimeOS AI: How Maharashtra Police Is Using AI to Fight Cybercrime' (*Vajiram & Ravi*, 15 December 2025) <https://vajiramandravi.com/current-affairs/mahacrimeos-ai-how-maharashtra-police-is-using-ai-to-fight-cybercrime/> accessed 12 April 2026

[18] 'UP Police Launches Trinetra 2.0, Running on Staqu Technologies' Crime GPT' *The Times of India* (15 March 2024) <https://timesofindia.indiatimes.com/technology/tech-news/up-police-launches-trinetra-2-0-running-on-staqu-technologies-crime-gpt/articleshow/108523458.cms> accessed 12 April 2026

[19] Ramchandran Murugesan, 'Predictive policing in India: Deterring crime or discriminating minorities?' (*The London School of Economics and Political Science*, 16 April 2021) <https://blogs.lse.ac.uk/humanrights/2021/04/16/predictive-policing-in-india-deterring-crime-or-discriminating-minorities/> accessed 12 April 2026

Pradesh, etc. have also used such tools in enhancing their policing systems. The rapid deployment of Predictive Policing systems is not void of risk, as the opaque operational framework of these systems has been characterised as detrimental to individual liberties. Critics caution that these advancements will result in a discrimination feedback loop and hinder free assembly by allowing arbitrary incarceration.

Operational Realities & Challenges: According to a July 2025 investigative report by The Wire &Pulitzer Centre, use of AI by Delhi Police, especially in face recognition systems from companies Innefu Labs and Pelorus Technologies, led to arrests which were based on the algorithmic analysis. This dependence on 'black-box' oversight usually lacks corroborating evidence, causing pressing privacy concerns and further leading to potential persistence of prejudices against marginalised communities.[20]

Marda and Naryan's ethnographic study of Delhi's CMAPS shows that the architecture of predictive policing systems incorporates and codifies institutional presumptions on poverty and the demographic trend of crimes. Instead of correcting these biases, the algorithm exacerbates them, leading to what academics have called the self-fulfilling prophecy of predictive policing, i.e., a discriminatory feedback loop. The areas with higher call rates to police, which are mostly from slums and resettlement colonies, are highlighted as hotspots drawing more police presence, generating more similar data points, reinforcing surveillance in these particular areas, causing and repeating the same loop.

The principle of presumption of innocence is endangered by predictive policing, which uses sophisticated algorithms to analyse huge databases in order to identify prospective crime hotspots or suspects. These techniques run the risk of translating a statistical probability, a numeric, into de facto guilt without reasoned judgment as exercised before the advent of these advanced models.[21] This proactive method of policing through algorithm-driven targeting of certain marginalised communities and minority groups is undermining the fundamental tenet that a person is innocent until proven guilty. These predictive tools are used to identify potential future perpetrators, which further intensifies surveillance and even leads to preventive detention based on the probability analysed by opaque algorithmic logic.

[20] Astha Savyasachi, 'Looking Back at the Camera: How Controversial AI Firms Shaped Delhi's Predictive Policing' *The Wire* (03 July 2025) <https://thewire.in/tech/delhi-police-ai-companies> accessed 12 April 2026
[21] Kelly Blount, 'Applying the Presumption of Innocence to Policing with AI' (2021) 92(1) International Review of Penal Law <https://hdl.handle.net/10993/48564> accessed 12 April 2026

This violates the principle that culpability must be based on proved acts and cogent evidence, not a mere probability, as followed across criminal jurisprudence. These consequences are not hypothetical, as in 2022 itself, it was accepted by Delhi Police that it used Facial Recognition Technology to investigate over 750 cases related to the North-East Delhi Riots in 2020. RTI reports analysed by certain digital rights groups indicate that some individuals were arrested based solely on Facial Recognition Technology (FRT) matches without corroborating eyewitness testimony or, in some cases, without formal Test Identification Parades (TIP) to confirm identity.[22]

In Ankush Maruti Shinde v State of Maharashtra,[23] the Hon'ble Supreme Court acquitted six men from the marginalised Paradhi community who had been on death row for sixteen years for a crime that was not committed by them due to faulty, unfair and dishonest, further undermining the fundamental right to fair trial. This case, though it predates the emergence of predictive algorithms, clearly sheds light on how these algorithms codify such institutional biases and attach guilt to certain groups, communities and geographic locations as these systems are trained on data that has significant traces of such implicit predispositions.

PREDICTIVE POLICING AT A CONFLICTING DIALOGUE WITH CONSTITUTIONAL MANDATES

Rule of Law: The four universal principles forming the base of the concept of Rule of Law are just law, transparent government, impartial and accessible justice and accountability. In Re Arundhati Roy (2002), the Hon'ble Supreme Court of India stated the rule of law as 'the basic rule of governance of any civilised polity'. This forms the cornerstone of India's Constitutional framework.[24] Based on A.V. Dicey's theory, the Rule of Law in the Indian Constitution is built around three key pillars that are the Supremacy of Law, Equality before Law and Predominance of Legal Spirit. Rule of Law, in its essence, guarantees that state action is non-arbitrary, there is judicial oversight with an independent judiciary, and no one

[22] Astha Savyasachi, 'As AI Took Over Policing in Delhi, Who Bore the Brunt?' (*Pulitzer Center*, 02 July 2025) <https://pulitzercenter.org/stories/ai-took-over-policing-delhi-who-bore-brunt> accessed 12 April 2026
[23] *Ankush Maruti Shinde and Ors v State of Maharashtra* (2009) 6 SCC 667
[24] 'Rule of Law: Dicey's Theory and Its Application in India' (*Defacto Law*, 23 April 2026) <https://www.defactolaw.in/post/rule-of-law-dicey-s-theory-and-its-application-in-india> accessed 24 April 2026

is above the law.[25] However, the rampant deployment of Predictive Policing systems across Indian states undermines each of the pillars of the Rule of Law with subtlety. The current form of algorithmic governance is subtly corroding the structure of the Rule of Law promised by the Constitution.

The first incursion is upon the Supremacy of Law itself, with these automation systems being deployed across India without being backed by any formal statute, without any guidelines on procurement transparency and operational framework. The implementation of these systems is steered by the interaction of private contracts with the discretion of executives, which is being exercised in the twilight zone of legislative irregularities.

The second rupture is on Equality before Law guaranteed by Article 14,[26] with the rise in automated decision making and increased surveillance via advanced AI tools, which further lead to severe concerns regarding biases and opaque operational processes severely compromising the tenet of the rule of law. Under the ideological pretence of algorithmic neutrality, these systems, through mathematical precision, will continue producing decisions with undercurrents of inequality as they are trained on historically biased data.

The third severe blow is to accountability; the replacement of human judgment with algorithmic decision-making has birthed a significant challenge of regulating police actions. When these algorithms recommend the arrest of a suspect and this decision proves to be wrong, then no human agent can be held liable, nor can the algorithm be held liable, posing a serious question of accountability.

The Supreme Court of India, in Chief Settlement Commissioner, Punjab v Om Prakash[27], established the rule of law as the most central and characteristic feature of the Indian constitutional system. Further, in The Court in the State of Punjab v Gurdial Singh[28] held – 'arbitrariness is the very antithesis of the rule of law' and 'every state action must meet the test of reasonableness.' The novel architecture of Algocracy, which relies on tools like predictive algorithms, conflicts with the obiter dicta established in these landmark decisions.

---

[25] Nitin Kumar, 'UNIT - I: Rule of Law' (*University of Lucknow*) <https://udrc.lkouniv.ac.in/Content/DepartmentContent/SM_43412e5b-698a-4851-b0c5-9974067f6302_30.pdf> accessed 13 April 2026

[26] Constitution of India 1950, art 14

[27] *Chief Settlement Commissioner, Punjab v Om Prakash and Ors* AIR 1969 SC 33

[28] *State of Punjab v Gurdial Singh and Ors* AIR 1980 SC 319

These algorithmic systems are deployed by executive procurement without statutory authorisation. Additionally, accountability for algorithmic decisions is dispersed across developers, vendors, procuring agencies, and deploying officers, resulting in a situation where no individual entity can be held liable for the final decision. Further, the algorithmic reasoning is opaque by design, producing decisions that cannot be questioned by the officer or the affected individual. Hence, the arbitrariness is not cured by automation but aggravated by it. As a result, the consequence is not merely a procedural gap but a structural and subtle severance of the rule of law.

Article 14 & Article 15 – Constitutional Guarantee of Equality & Non-Discrimination: Article 14 guarantees 'equality before the law' and 'equal protection of laws' within India, which has been interpreted by the Hon'ble Supreme Court of India for the state action to be non-arbitrary, fair and reasonable.[29]

On the other hand, Article 15 bars the State from treating any person discriminately based on their race, religion, caste, sex, place of birth, or any of them.[30] Therefore, it is constitutionally mandated not to target communities on the aforementioned grounds. However, the systemic mathematics of the statistical inference of these prediction models trained on institutional data that are biased against specific areas, communities, or religions endangers the guarantee of Article 15 and results in outputs muddled with discriminative biases disguised as factual data. As these systems speak the language of statistics, which cannot be aptly comprehended and are further tainted by discriminatory data, these systems are trained on. Consequently, they produce biased decisions that go uncontested, resulting in indirect discrimination in its most constitutionally detrimental form.

Furthermore, when the state implements these algorithms, which are trained on decades of policing data that is biased towards certain communities, individuals and areas due to a historical pattern of over-criminalisation, the state not only repeats the past mistakes but instead legitimises them, dressing them in the language of computational neutrality, creating what experts call a 'disparate impact'.[31] As these algorithms replace human reasoning, they

[29] Constitution of India 1950, art 14
[30] *Ibid* art 15
[31] Gautam Bhatia, 'Article 15 and Typologies of Discrimination II: Disparate Impact' (*Indian Constitutional Law and Philosophy*, 29 October 2013) <https://indconlawphil.wordpress.com/2013/10/29/article-15-and-typologies-of-discrimination-ii-disparate-impact/> accessed 13 April 2026

confront the theory of 'intelligible differentia'.[32] Under constitutional law, government actions and classification must rest on an 'intelligible differentia', a clear, logical and reasonable explanation that must have a rational nexus to the intent of the act. Most of the time, these ML models generate outputs without any disclosure of the reasoning process behind such logics. Therefore, when a system's decision of categorizing a person as a suspect fails to meet the requisite explanation it violates the 'intelligible' test as required by Article 14 and upheld in the landmark judgment of State of West Bengal v Anwar Ali Sarkar[33] where the Hon'ble Supreme Court established that though Article 14 prohibits class legislation it allows for 'reasonable classification', which serves as a check on arbitrary state action that may lead to discrimination against certain individuals or groups.

Article 21 - Right to Life & Personal Liberty from Procedural Fairness to Due Process: Article 21 is the constitutional assurance that the life or liberty of an individual cannot be interfered with unless it is done through a procedure that is fair, just and reasonable.[34] Building upon the Maneka Gandhi case[35], which established that procedure established by law must be met with due process, the Supreme Court in the landmark Puttaswamy[36] judgment further expanded Article 21 to be included in the ambit of the Golden Triangle, i.e. Article 14, Article 19 & Article 21.

The Court further declared the right to privacy as a fundamental right and drew a line for state action, ruling that the state may not collect personal data such as biometrics, financial records, personal geographical histories, etc. and use it for profiling purposes without citing a genuine legitimate reason that meets the test of legality, necessity and proportionality. Furthermore, another seminal ruling by the Supreme Court in A K Kraipak v Union of India (1969),[37] it was held that the principles of natural justice apply to administrative actions as well and are not limited to judicial ones. This judgment established that for fairness to prevail in its true sense, the administrative actions which are based on bias or a reasonable likelihood

[32] Paras Sharma, 'The Ghost in the Administrative Machine: Toward a Constitutional Doctrine of Algorithmic Review in India' (*Law School Policy Review*, 18 March 2026) <https://lawschoolpolicyreview.com/2026/03/18/the-ghost-in-the-administrative-machine-toward-a-constitutional-doctrine-of-algorithmic-review-in-india/> accessed 13 April 2026
[33] *State of West Bengal v Anwar Ali Sarkar* AIR 1952 SC 75
[34] Constitution of India 1950, art 21
[35] *Maneka Gandhi v Union of India* AIR 1978 SC 597
[36] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1
[37] *A K Kraipak and Ors v Union of India and Ors* AIR 1970 SC 150

of bias must be treated as void. However, these aforementioned judicial mandates are being challenged by the pervasive application of advanced predictive algorithms at every stage of their operation. These systems collect data without consent, analyse it without transparency and generate potential suspects without explaining how and why these individuals were flagged and without them being aware of their profiling.

Article 20(3) - The Foundation of the right against self-incrimination: The pivotal ruling of Selvi v State of Karnataka (2010)[38] promulgated that the involuntary administration of narcoanalysis, polygraph examinations and brain mapping procedures is violative of both the constitutional guarantee against self-incrimination under Article 20(3) and the fundamental right to privacy and bodily integrity safeguarded by Article 21.[39] The Supreme Court called these investigation tactics testimonial compulsion, coercing individuals to disclose any personal knowledge without their voluntary conscious choice. In Nandini Satpathy v P.L Dani (1978),[40] the Supreme Court further expanded the protection against self-incrimination and included mental and psychological coercion in addition to physical coercion during police interrogations. The court ruled that the right to remain silent as provided under Article 20(3)[41] of the Constitution and Section 161(2), CrPC (now S.180(2), BNSS)[42] shall extend to the investigative stage, including the pre-arrest phase and not limited to the trial stage only.

In a structurally novel way, the predictive policing systems transgress the spirit of these rulings as they are not coercing a verbal confession but extracting a data profile. Systems like CMAPS, without suspects' consent, analyse biometrics, call records, financial records and geographical information tracked and replicate the data to create a behaviour pattern of the individuals, providing a probable insight into their personalities, thereby creating an algorithmic assessment of criminal propensity. As a result, the individuals are deceptively made to testify against their prospective conduct through the involuntary disclosure of personal information to a system that operates in the shadows and cannot be questioned.

[38] *Selvi and Ors v State of Karnataka & Anr* (2010) 7 SCC 263
[39] Constitution of India, art 21
[40] *Nandini Satpathy v Dani (P L) and Anr* (1978) 2 SCC 424
[41] Constitution of India 1950, art 20(3)
[42] Code of Criminal Procedure 1973, s 161(2); Bharatiya Nagarik Suraksha Sanhita 2023, s 180(2)

Article 22 - Protection Against Arbitrary Arrest and Detention: Article 22, which is a safeguard against arbitrary arrest and detention[43], is at loggerheads with the Predictive Policing systems, which use algorithmic proficiency to predict potential crime hotspots and suspects thereof. The immunity provided by Article 22 against coercive state power is being threatened due to the advancement of Algocracy, which is progressively resulting in increased profiling, over-policing and detention based on statistical surmise rather than concrete proof. An arrested person must be apprised of the grounds of the arrest, as stipulated in Article 22.

In D.K Basu v State of West Bengal,[44] the Supreme Court provided detailed guidelines about what constitutes a lawful procedure of arrest and ruled that any failure to comply with the guidelines shall render the arrest unlawful. The court further in Arnesh Kumar v State of Bihar[45] held that an arrest must be based upon a reasoned and recorded satisfaction of necessity by the police officers. Building upon these, the Supreme Court, in a recent ruling of Mihir Rajesh Shah v State of Maharashtra,[46] held that the right to be informed about the grounds of arrest is a constitutional imperative under Article 22(1)[47], and the grounds must be communicated clearly and effectively in a language comprehensible to them. The essence of these rulings is disrupted by the application of algorithmic policing as these systems are fuelled by opaque mechanism which generates risk scores without providing any rational reasoning. Hence, the whole structure of Article 22(1) is jolted as a person who is detained by an algorithmic decision, which is devoid of the fundamental ethics of maintaining transparency, shall not have access to the precise reasons of their arrest as mandated by various jurisprudential deliberations in line with Article 22(1).

The Court in State of Karnantaka v Sri Darshan Thoogudeepa (2025)[48] held that mere absence of written grounds does not make an arrest illegal unless there is a clear prejudice or denial of fair opportunity to contest. In arrest made by algorithmic policing, demonstrable prejudice is inherent; hence, individuals cannot possibly contest the grounds that are an output of opaque algorithmic reasoning, the logic of which is not known even to the arresting officer.

[43] Constitution of India 1950, art 22
[44] *Shri Dilip K Basu, Ashok K Johri v State of West Bengal, State of UP* (1997) 1 SCC 416
[45] *Arnesh Kumar v State of Bihar and Anr* (2014) 8 SCC 273
[46] *Mihir Rajesh Shah v State of Maharashtra and Anr* (2025) INSC 1288
[47] Constitution of India 1950, art 22(1)
[48] *State of Karnataka v Sri Darshan etc* (2025) INSC 979

This indicates that predictive policing arrests fail the demonstrable prejudice test, making such arrests constitutionally infirm.

The analysis made in this section, backed by various case laws, demonstrates that the algorithmic policing system is fundamentally inconsistent with constitutional values of equality, transparency, accountability and the requirement of protection of fundamental rights. Hence, if allowed to operate at such an accelerating pace without a formal legislation imposing requisite statutory limitations, these systems, which are hailed as harbingers of efficiency, would transform into architects of a constitutional crisis.

ARTIFICIAL INTELLIGENCE IN JUDICIAL SYSTEM: INSTITUTIONAL ADOPTION, CHALLENGES & STRUCTURAL RISKS

Institutional Adoption & Scope of AI tools: Indian courts have long been afflicted with huge pendency and have been facing an efficiency quotient deficit to meet the ever-growing demand of the litigation landscape due to structural and administrative irregularities. It is against this backdrop of institutional strain that the judiciary resorted to digital modernisation of the judicial system as a potential solution.

The Supreme Court, taking a significant step towards this modernisation drive, launched two AI-powered tools, namely SUPACE (Supreme Court Portal for Assistance in Court Efficiency), which enables a smooth flow of case management, assisting judges in arranging and retrieving case material. The other tool is SUVAS (Supreme Court Vidhik Anuvaad Software), which translates judgments into regional languages – expanding the reach of judicial rulings to litigants who earlier were deprived of access to judgments due to linguistic barriers.[49]

Adding to this is the implementation of the e-Courts Mission Mode Project,[50] a collaborative effort administered by the Department of Justice, Ministry of Law & Justice and the Hon'ble Supreme Court of India. It is the most comprehensive initiative aiming at an extensive revamp of the judicial infrastructure, establishing a paperless, digitally integrated and

[49] 'INDIA' (*Oxford Institute of Technology and Justice*, 01 September 2025) <https://www.techandjustice.bsg.ox.ac.uk/research/india> accessed 13 April 2026
[50] 'E-Courts Mission Mode Project' (*Press Information Bureau*, 17 December 2024) <https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2085127> accessed 13 April 2026

publicly accessible judiciary, further improving the e-Filing system to reduce procedural delays.

Artificial Intelligence is structurally transforming the field of legal practice. Predictive analytics tools are being employed by legal practitioners to examine gargantuan databases of court rulings, opinions, reports, etc., and further enabling analysis of judgment patterns and case details to predict the outcomes of the legal disputes being contested. AI platforms for speedy contract drafting and for reviewing discrepancies by automated identification of clauses inconsistent or detrimental to the case are being used by lawyers for efficient and streamlined workflow. Further tools like LegRAA (Legal Research Analysis Assistant) and Adaalat AI offer assistance on similar lines, helping in navigating through legal research and management of cases, thereby enabling enhanced productivity in legal practice.

Structural Risks & Challenges with Respect to Use of AI Tools in Adjudication: The potential risks of unchecked usage of AI in judicial proceedings have been repeatedly called out by the judiciary. The Allahabad High Court in Mata Prasad Pandey v State of Uttar Pradesh[51] warned against using AI-generated legal findings in Court proceedings, pointing out that these tools may produce fictitious or hallucinated precedents that may seem authentic prima facie but have no trace in the real world at all. The Delhi High Court went a step further and reprimanded the counsel in the case Greenopolis Welfare Association v Narender Singh and Ors. (2025)[52] for using AI tools and expressly discouraged the counsel from drafting arguments using AI tools without the application of reasoned human intelligence, as these tools are still developing and operate in a grey area.[53]

These concerns, as discussed by the judiciary, are not exaggerated but fairly legitimate, as AI tools being used are trained on historical data reflecting the biases of past judgments. Hence, when such systems are used to search for relevant precedents or turned to for assistance in judicial decision-making, they might subtly imprint these biases in their outputs under the guise of neutrality. Hence, the integrity of legal reasoning made with the assistance of these tools is threatened by the operating framework of these very systems, as they are

[51] *Mata Prasad Pandey v Civil Judge (JD) South Room No 25 Sultanpur & Anr* 2025:AHC-LKO:10838
[52] *Greenopolis Welfare Association (GWA) v Narender Singh and Ors* (2025) CM(M) 1909/2025, CM APPL 61372/2025
[53] 'Delhi High Court Flags 'AI-Generated' Plea Citing Fake Case Law - 2025-09-27' (*Supreme Today*) <https://news.supremetoday.ai/delhi-high-court-flags-ai-generated-plea-citing-fake-case-law-20250927175334f665ef> accessed 13 April 2026

tainted with the biases prevalent in the Indian Legal System and are prone to hallucinations leading to citation of fabricated cases.

In Jaswinder Singh v State of Punjab (2023)[54] the High Court used ChatGPT to understand bail jurisprudence on cruelty cases. The judge clarified his stance that the tool was used not to determine the merits of the case but only to get a broader perspective regarding the bail application. Further, in Md Zakir Hussain v State of Manipur (2024)[55] the court revealed that it used ChatGPT not for assistance in judicial decision-making but only for research purposes to know about the service rules in the Village Defence Service. Adding to this is the Gummadi Usha Rani & Anr v Sure Mallikarjuna Rao & Anr (2026)[56] case, which exposed a significant institutional concern encircling the Indian Judiciary that is the slow, significant and consequential pervasion of AI tools in adjudication. In this case, the Trial Court based its ruling on four judgments that turned out to be non-existent and were mere hallucinations of the AI tool used. This has raised questions on the integrity of judicial decisions, which are supposed to be the result of human intellect and perception and not statistical inference of some automation tool.

Algorithmic working relies on pattern recognition based on the data fed into it. Hence, the application of such tools in the pronouncement of judgment poses a risk of perpetuating societal biases reflected in the data, as it is fed by identifying probable irregularities in the historical data. This kind of functioning of these systems makes them fundamentally unfit to be used in adjudication, as they shall reflect the prevalent bias and will be detrimental in deciding cases that require departing from the historical bias. Such cases can be decided only with judicial courage and independent human reasoning that can construct meaning, balance competing notions and apply moral agency.

Kerala High Court is the first in India to implement a policy regarding the use of Artificial Intelligence Tools in District Judiciary,[57] recognising the increased use of AI in the judicial landscape and the risk posed thereof. The policy mandates strict human supervision, bans AI as a substitute for judicial reasoning, and limits the usage of the tools to those approved

[54] *Jaswinder Singh v State of Punjab* (2023) CRM-M-22496-2022
[55] *Md Zakir Hussain v State of Manipur & Ors* (2024) WP(C) No 70/2023
[56] *Gummadi Usha Rani and Anr v Sure Mallikarjuna Rao and Anr* (2026) SCC OnLine SC 341
[57] 'AI tools not for decision making: Kerala HC guidelines to district judiciary on AI usage' *The Economic Times* (20 July 2025) <https://economictimes.indiatimes.com/articleshow/122794562.cms> accessed 13 April 2026

by the High Court or Supreme Court, aimed at enhancing efficiency while ensuring transparency, fairness, and accountability. Hence, the question is not of enhanced efficiency but preserving the integrity of the judiciary itself, as reliance on AI, if left unchecked, risks undermining due process, reasoned decision-making, and the human discernment that anchors judicial legitimacy.

A COMPARATIVE ANALYSIS OF AI REGULATORY FRAMEWORKS

European Union: The European Union uses an extensive, risk –based regulatory framework to mitigate the perils posed by algorithmic governance. At its foundation lies the General Data Protection Regulation (GDPR), which serves as a fundamental framework that aims at imposing human accountability and transparency on these algorithmic systems, which otherwise would have resulted in privacy breaches, algorithmic bias and lack of accountability. Article 22 of GDPR[58] allows individuals to contest these automated decisions and empowers them with the right not to be subjected to decisions made exclusively by algorithmic processing, including profiling. This Article holds profound importance as it guarantees human intervention, freedom to voice opinions and the right to contest.

The Hague District Court in the System Risk Indication (SyRI) 2020[59] case held that the use of the digital scoring system of the Dutch government to predict welfare fraud was unlawful and violated Article 8 of the European Convention on Human Rights (ECHR)[60] as the system lacked transparency and sufficient safeguards for privacy. The system lacked safeguards to prevent invasive surveillance and risked discriminating against vulnerable groups. This judgment highlights the importance of working of the automated systems in conformity with human rights.

The European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689) is the world's most comprehensive and legally binding framework for AI governance. Under this Act, both the developers and deployers of these systems are subject to high penalties for non-compliance with the mandatory risk-based impositions.[61]

[58] General Data Protection Regulation 2016, art 22
[59] *NCJM et al and FNV v The State of the Netherlands* [2020] ECLI:NL:RBDHA:2020:865
[60] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) (ECHR) 1953, art 8
[61] EU Artificial Intelligence Act 2024

The Act directly confronts issues of transparency deficits and inherent bias through the integration of safeguards into the deployment and design process of AI systems. Article 5[62] of the act establishes prohibitions against AI tools that pose unacceptable risk to safety, livelihood and fundamental rights, further forbidding social scoring mechanisms, cognitive manipulation and indiscriminate facial data scraping, exploitation of vulnerable groups, etc. Article 10[63] establishes a requirement for high-quality, free of error and representative datasets and mandates proactive evaluation of potential biases that could result in discriminatory outcomes. Article 14[64] ensures substantive human oversight, whereas Article 27[65] necessitates pre-evaluation of impacts on fundamental rights before official deployment of AI systems.

The EU AI ACT requires ex ante compliance assessments, compulsory registration in a public EU database, fundamental rights impact assessments (FRIA) before deployment to analyse potential risks to people's fundamental rights, maintainability of logs to trace the system's function and judicial approval for biometric identification. The Act provides for the right to receive explanations and file complaints against algorithmic decisions affecting them. The principle followed by the EU is simple: to regulate before deployment rather than await a violation to occur for a requisite regulation to be enacted.

Canada: Canada is one of the pioneering countries to implement an ethical and accountable AI governance regime. The Treasury Board of Canada Secretariat's Directive on Automated Decision-Making and its Algorithmic Impact Assessment Instrument[66] tool constitute an instrumental step towards ethical AI governance, mandating the assessment of potential risks and implications of automated systems deployed by federal institutions. This assessment requirement evaluates the effect on rights, risk of bias, explainability for algorithmic decisions and the necessity of human oversight. This framework helps mitigate the risk of potential violations of rights, ensuring procedural fairness in public services and is indicative of the Canadian government's commitment towards building ethical and safe AI mechanisms.

[62] EU Artificial Intelligence Act 2024, art 5
[63] EU Artificial Intelligence Act 2024, art 10
[64] EU Artificial Intelligence Act 2024, art 14
[65] EU Artificial Intelligence Act 2024, art 27
[66] 'Directive on Automated Decision-Making' (*Canada.ca,* 24 June 2025) <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592> accessed 13 April 2026

United States of America: The United States has adopted a decentralised sector-specific regulating policy in contrast to the EU's unified and comprehensive enactment. In the U.S.A., predictive policing tools like PredPol and ShotSpotter have been subjected to substantial legislative and legal criticism due to transparency issues and discriminatory biases. Further, there have been municipal bans on the use of facial recognition tools by the government in certain cities. In State v Loomis[67], the Wisconsin Supreme Court ruled that while the COMPAS recidivism algorithm could be used in criminal sentencing, it cannot be completely dependent upon, citing the opacity, exclusive shielding and possibility that algorithmic risk scores may embed racial disparities into decisions relating to sentencing. The USA has been operating under a fragmented regulatory approach with respect to AI governance.

United Kingdom: The U.K. Court of Appeal in R (Bridges) v Chief Constable of South Wales Police[68] ruled that use of live facial recognition technology was unlawful due to a lack of a clear legal framework governing its use, insufficient data protection impact assessments and failure to meet public sector equality requirements. This judgment is significant as it recognised that algorithmic systems can produce discriminatory outcomes and there must be accountability in how these tools are deployed. However, post this judgment, there has been a shift in the U.K.'s policy with respect to this predictive tool, as in R (Thompson and Carlo) v Commissioner of Police of the Metropolis,[69] the Court upheld the Metropolitan Police's revised 2024 Live Facial Recognition (LFR) policy as lawful. While recognising the technology's chilling effect on rights, the court ruled that the policy's safeguards were adequate.

The U.K government is aiming at a pro-innovation decentralised strategy for AI deployment in law enforcement systems. This approach seeks to enhance operational efficiency while controlling risks to ethical mandates. The UK government is actively implementing the Algorithmic Transparency Recording Standard (ATRS),[70] designed to maintain oversight for AI in decision-making, while allowing the use of tools like Live Facial Recognition (LFR). The UK's AI policy aims to strengthen public confidence and ensure accountability by

[67] *State v Loomis* [2016] 881 NW 2d 749 (Wis)
[68] *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058
[69] *R (Thompson and Carlo) v Commissioner of Police of the Metropolis* [2026] EWHC 915 (Admin)
[70] 'Algorithmic Transparency Recording Standard' (*Observatory of Public Sector Innovation*, 2021) <https://oecd-opsi.org/innovations/algorithmic-transparency-standard/> accessed 13 April 2026

requiring public sector organisations to disclose a detailed report of how and why they use AI and information on data collected, associated risks and mitigation strategies.

India's Position: The comparative analysis allows us to understand that the regulatory gap in India is structural, specific and has significant constitutional implications. Currently, the use of AI in the law enforcement structure of the country is not governed by any specific legislation. Regulation in this sphere is characterised by the absence of critical safeguards s, such as there is no mandate for audits for checking algorithmic bias, no enforceable right to explanation to individuals, no independent oversight authority or mechanism, and no provision for ex ante assessments, among other shortcomings.

The most concerning aspect of this regulatory deficit is that it stems not from the lack of constitutional guidelines but from the failure to translate well-established constitutional principles into sound regulation. The Supreme Court, through its landmark judgments from Puttaswamy to Sri Darshan's case, has provided necessary principles for governing and regulating such technologies. Hence, there is no dearth of doctrinal tools, but what is missing is the institutional will to apply these principles in combating the challenges posed by algorithmic governance.

WAY FORWARD POLICY RECOMMENDATIONS

The Artificial Intelligence (Ethics and Accountability) Bill, 2025: From Private Member Bill to Legislative Imperative: The Artificial Intelligence (Ethics and Accountability) Bill,[71] a private member bill which was introduced in the Lok Sabha, was one of the most profound legislative proposals with earnest efforts in addressing the increased use of AI in law enforcement and the need for rights-protective AI governance regulation. The Bill proposed the creation of a statutory AI Ethics Committee having the authority to mandate routine ethical evaluations of AI systems deployed, set accountability standards for algorithmic decision making, provide for grievance redressal mechanisms for individuals affected by such decisions and further impose heavy penalties for non-compliance with stipulated regulations. These proposed suggestions can be used to enact legislation or the Bill in its original form can itself be enacted by making some additions, such as, First, the act must outline the acceptable purposes for deployment of tools and use of AI in law enforcement,

[71] Artificial Intelligence (Ethics and Accountability) Bill 2025

further providing for a list of activities that must be prohibited or limited to be exercised in case of absolute necessity backed by rational reasoning. Secondly, condition every new deployment on prior statutory authorisation. Thirdly, establishing the right to access and challenge decisions, any individual who faces an algorithmic policing action must be apprised of the reason and must be empowered to contest it. Fourthly, officers deploying and using these algorithms must go through rigorous training focused on ethical and constitutional implications, providing for quarterly conduct of such sessions to maintain operational competencies and preventing over-reliance on these tools.

Right to Reasoned State Action – Establishing Explainability Standards: The Constitutional guarantee of reasoned administrative action upheld across the jurisprudential landscape and landmark judgments necessitate establishing the same within algorithmic frameworks through explainability standards. Administrative authorities deploying these algorithms must possess the capability to explain the logic behind particular algorithmic decisions to the individuals affected by such decisions in a language comprehensible to them. In order for this to happen, the state should not deploy systems supplied by private vendors that are absolutely not interpretable.

Establishing an Independent Regulatory Authority: A statutory body such as the National Authority of Algorithmic Accountability and Transparency (NAAAT) or equivalent must be established with three important functions: ex ante approval and assessment of AI tools deployment, routine audits post deployment to reduce discriminatory systemic biases and mitigate their impact and independent adjudication of grievances. Further, the authority must be constituted by technical experts, legal experts and civil society experts; it must be insulated from executive interference.

Human-in-the-Loop – A Legislative Mandate: The premise of accountability requires that final decision-making authority affecting the rights of individuals must be exercised by the intellectual capacities of human beings and not by the statistical processing of algorithms. AI must be treated as an assistive tool, but shouldn’t be used to replace human discernment and shouldn't be made to decide without human oversight. This necessary involvement of humans in the algorithmic framework, also known as a human-in-the-loop mechanism, must be mandated by formal legislation instead of relying on informal operational practice.

Mitigating Bias through Regular Audits: In order to mitigate the discriminatory effects of data bias, regular algorithmic audits are required, which shall involve training of these systems on fresh, vast, diverse, representative high-quality datasets that are not tainted with historical biases. Further, there must be a reform and attitudinal change in the policing practices that generate data reflecting discrimination towards certain individuals, areas, groups or communities.

Restructuring Section 17 of the DPDP Act 2023:[72] The broad exemption of the government under Section 17 must be restructured. Instead of exempting all the government agencies, exemption should be purpose-specific, allowing exclusion from the ambit of data protection principles only for objectives that demonstrate genuine necessity, further being subjected to judicial review. The current approach, with the Central Government having expansive unrestricted power to exempt government agencies, does not pass the test of proportionality as established by judicial doctrine and hence requires a recalibration.

CONCLUSION

Artificial Intelligence, when used in conformity with constitutional values, carries an unparalleled power to transform the criminal justice system that has long been burdened with structural inadequacies. Artificial Intelligence deployment in law enforcement, if steered by the essence of equality, fairness, transparency and accountability, can lead to investigative efficiency, prowess in proactive capabilities and effective judicial accessibility that hasn't been possible by conventional reforms. This paper recognises the enhanced productivity of the law enforcement apparatus of this country, propelled by the deployment of an algorithmic model and does not diminish these advancements.

However, what this paper argues is that these gains have been made by circumventing constitutional mandates. The paper discusses that the age of Algocracy arrived not through legislative deliberation but through the will of executive action through private contracts. This has marked the advent of a governing structure where coercive state power is being exercised discretely by these opaque algorithms trained on historically biased data, the decision of which cannot be contested due to its black box nature, further solidified by regulatory gaps in the legislation. From Delhi CMAPS creating discriminatory feedback

[72] Digital Personal Data Protection Act 2023, s 17

loops to the court's pronouncing judgments on the basis of hallucinated case laws given by these AI tools, this paper has analysed the systemic constitutional and ethical infirmity caused by the grey operations of these tools.

These infirmities have threatened the whole ethical and legal landscape of law enforcement. The principle of the Rule of Law is endangered when accountability is subverted by the rule of codes and reasoned human judgment is replaced with statistical inference. Further, when these algorithms operate under the facade of neutrality, flag individuals based on prejudices of historical data, leading to over-surveillance of certain communities, regions and castes, this leads to the breach of Article 14 and Article 15. Article 20(3) is transgressed when a suspect is deceptively compelled to testify against his future conduct by unconsented disclosure of personal information through biometric, facial recognition technology, among other methods. When the grounds of arrest are not informed to the individual suspected or known to the arresting officer, Article 22(1) and Article 22(2) lose their meaning.

Comparative frameworks analysing EU, USA, UK and Canada's policy highlight that protection of rights, efficiency and innovation must be co-designed to ensure public trust. In the global race of AI leadership, the nation which successfully anchors its robust algorithmic models in principles of accountability, transparency and protection of human rights shall emerge as the true winner. The Constitution of India has provided the exact arsenal with all the tools to create such a robust model in the form of comprehensive judicial precedents from Puttaswamy to Sri Darshan. Now, the only requisite action left is to translate them into legally binding legislative frameworks. The absence of such an intervention will birth a system in which efficiency shall eclipse accountability and where suspicion based on discrimination shall be coded, liberty will be computed, and justice will no longer be reasoned but merely inferred.