
ALGORITHM BIAS, AUTOMATED DECISION-MAKING, AND THE RIGHT TO EXPLANATION: COMPARATIVE ANALYSIS OF INDIA'S DPDP ACT 2023 AND THE EU AI ACT 2024

Deshna Sanghavi, B.A. LL.B. (Hons.) Candidate, Kirit P. Mehta School of Law,
SVKM's NMIMS, Indore

ABSTRACT

Automated decision-making (ADM) systems powered by algorithmic processes now determine outcomes that are fundamental to individual liberty and dignity — credit eligibility, employment, healthcare triage, criminal bail, and social welfare entitlements. When these systems embed, amplify, or perpetuate bias, the consequences fall disproportionately upon already marginalised communities. Two landmark regulatory instruments have emerged in 2023 and 2024 to address this challenge: India's Digital Personal Data Protection Act, 2023 (DPDP Act) and the European Union's Artificial Intelligence Act, Regulation (EU) 2024/1689 (EU AI Act). This paper conducts a critical comparative analysis of the two frameworks across four dimensions: the scope and definition of algorithmic bias; the recognition and enforceability of a right to explanation for ADM outputs; accountability mechanisms for high-risk AI deployments; and the adequacy of remedial architectures for individuals adversely affected by biased automated decisions. The paper finds that while the EU AI Act provides a more structurally coherent and rights-protective framework, it is not without significant implementation gaps. India's DPDP Act, by contrast, addresses the question of automated decision-making only implicitly and incompletely, leaving a critical regulatory vacuum at precisely the moment when Indian public and private sector deployment of ADM systems is accelerating. The paper concludes with a set of concrete legislative and regulatory recommendations for India, drawing on the EU model while accounting for India's constitutional framework, its judicial doctrine on the right to privacy, and the socio-economic context in which Indian ADM systems operate.

Keywords: Algorithmic bias, Automated decision-making, Right to explanation, DPDP Act 2023, EU AI Act 2024, Artificial intelligence regulation, Data protection, Explainability, High-risk AI, India-EU comparative law.

I. INTRODUCTION

In 2022, the Delhi High Court was confronted with a writ petition challenging the automated rejection of a job application by an algorithmic screening tool deployed by a public sector undertaking. The petitioner — a Scheduled Caste applicant who met every stated eligibility criterion — had been eliminated at the first screening stage by a machine-learning model whose weighting parameters were neither disclosed to applicants nor subject to any independent audit. The Court, lacking a statutory framework to adjudicate the claim, dismissed the petition on procedural grounds. The case was never reported. It is, however, emblematic of a systemic failure: India's legal architecture provides no clear right to know why an algorithm made a consequential decision about you, no right to contest that decision on the merits of the algorithmic process, and no mandatory obligation on deployers to ensure that the algorithm was free from discriminatory bias.¹

This failure is not unique to India. The governance of algorithmic decision-making is one of the most contested frontiers in contemporary public law globally. What distinguishes the current moment is that two of the world's most consequential legal systems — India, with 1.4 billion people and one of the fastest-growing AI deployment ecosystems in the world, and the European Union, with 450 million people and the world's most developed data protection architecture — have simultaneously enacted major regulatory instruments that bear, directly or indirectly, on algorithmic accountability. The juxtaposition of India's Digital Personal Data Protection Act, 2023 and the EU's Artificial Intelligence Act, 2024 offers an unprecedented opportunity for comparative legal analysis.

The central thesis of this paper is threefold. First, that algorithmic bias in ADM systems constitutes a cognisable harm under both constitutional and statutory frameworks in India, but that the existing legal architecture is inadequate to provide effective remediation. Second, that the right to explanation — the right of an individual to receive a meaningful, human-understandable account of why an automated system reached a decision about them — is a necessary but not sufficient condition for algorithmic accountability, and that neither the DPDP Act nor the EU AI Act fully realises this right in enforceable terms. Third, that India must undertake targeted legislative reform, informed by but not slavishly copying the EU model, to establish a rights-protective and innovation-compatible framework for ADM governance.²

The paper proceeds as follows. Part II provides a conceptual taxonomy of algorithmic

bias and automated decision-making. Part III examines the constitutional foundations for algorithmic accountability in India. Part IV analyses the DPDP Act's treatment of ADM. Part V examines the EU AI Act's framework. Part VI conducts a structured comparative analysis across four dimensions. Part VII proposes reforms for India. Part VIII concludes.

II. ALGORITHMIC BIAS AND AUTOMATED DECISION-MAKING: A CONCEPTUAL TAXONOMY

A. Defining Automated Decision-Making

Automated decision-making refers to any process by which a decision with legal or similarly significant effects on an individual is made solely or primarily on the basis of automated processing of personal data, without meaningful human deliberation at the point of the decision. ADM systems range from rule-based expert systems — which apply pre-programmed criteria deterministically — to machine-learning models — which identify patterns in historical data and apply them probabilistically to new cases — to deep learning neural networks, which operate through layers of mathematical abstraction that may be opaque even to their developers.³

The legal significance of ADM lies in its scale, speed, and opacity. A human adjudicator making an individual credit decision may exhibit bias, but that bias is contestable through cross-examination, appeal, and the transparency of reasoning that inheres in human deliberation. An algorithmic system making ten million credit decisions per hour is not contestable in the same way: its reasoning is encoded in weights and parameters that are neither legible to lay persons nor readily disclosed by deployers protecting trade secrets.

B. A Taxonomy of Algorithmic Bias

Algorithmic bias is not a monolithic concept. Scholars in law, computer science, and social science have identified at least seven distinct categories of bias that may infect ADM systems, each requiring different legal and technical responses.⁴

Historical bias arises when training data reflects past discriminatory practices, which the model then learns and perpetuates. A hiring algorithm trained on historical promotion data from an organisation that discriminated against women will learn to replicate that discrimination, regardless of whether the protected characteristic of gender is explicitly

included in the model's inputs. Representation bias arises when training datasets under-represent certain demographic groups, causing the model to perform less accurately for those groups. Measurement bias arises when the proxy variables used to represent real-world phenomena are themselves discriminatory: using postcode as a proxy for creditworthiness, for example, may function as a proxy for race in jurisdictions with racially segregated residential patterns.

Aggregation bias arises when a single model is applied uniformly to a population that is in fact heterogeneous, producing systematically worse outcomes for sub-groups whose characteristics deviate from the population mean. Evaluation bias arises when the metrics used to assess model performance fail to capture harm to sub-groups. Deployment bias arises when a model is used in a context different from the context in which it was trained and validated. Feedback loop bias arises when a model's outputs influence future training data, causing the model to become progressively more biased over time — a phenomenon observed in predictive policing algorithms that intensify surveillance in communities already over-policed.⁵

Each of these bias categories has distinct legal implications. Historical and representation bias implicate anti-discrimination norms. Measurement and aggregation bias implicate the right to equality and non-discrimination under Article 14 of the Indian Constitution. Deployment and feedback loop bias implicate the duty of care of deployers and the adequacy of ongoing monitoring obligations. A legal framework that addresses only one or two of these categories will fail to provide comprehensive protection.

C. The Right to Explanation: Theoretical Foundations

The right to explanation refers to the entitlement of an individual who has been subject to an automated decision to receive a meaningful account of the logic, criteria, and data inputs that produced that decision, in a form sufficiently comprehensible to enable the individual to assess its lawfulness, accuracy, and fairness, and to contest it if appropriate. The concept has philosophical roots in procedural justice theory — the proposition that legitimate decision-making requires not only substantively just outcomes but also a process that respects the dignity and rational agency of those subject to it.⁶

The right to explanation is distinct from, though related to, the concept of algorithmic transparency. Transparency refers to the general discoverability of information about a system's

design, training, and operation. Explanation refers specifically to the individual-level communication of the reasoning behind a particular decision. An ADM system may be technically transparent — its documentation publicly available, its code open-source — while still failing to provide an individual with a meaningful explanation of why their loan application was rejected or their parole denied. Conversely, an explanation may be provided in terms that are formally compliant but practically meaningless: 'Your application was assessed by an automated system using multiple factors' tells an individual nothing useful.

III. CONSTITUTIONAL FOUNDATIONS FOR ALGORITHMIC ACCOUNTABILITY IN INDIA

A. The Right to Privacy and Informational Self-Determination

The Supreme Court of India's landmark nine-judge bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India recognised the right to privacy as a fundamental right under Article 21 of the Constitution, encompassing informational privacy, decisional autonomy, and dignity. The Court held that privacy is not merely the right to be left alone but includes the right to control the narrative of one's own life — a formulation with direct implications for algorithmic decision-making.⁷

If privacy encompasses informational self-determination, then an individual has a constitutionally grounded interest in understanding how their personal data is being processed to make decisions about them. An ADM system that processes an individual's personal data to determine their creditworthiness, employability, or bail eligibility and then refuses to explain its reasoning arguably infringes the right to informational self-determination recognised in Puttaswamy. This constitutional hook is more powerful than any statutory provision because it cannot be legislatively extinguished and can be directly enforced through Article 32 petitions to the Supreme Court.

B. The Right to Equality and Non-Discrimination

Article 14 of the Constitution guarantees equality before the law and equal protection of the laws. Article 15 prohibits discrimination on grounds of religion, race, caste, sex, or place of birth. Article 16 guarantees equality of opportunity in public employment. Together, these provisions constitute a comprehensive anti-discrimination framework. The Supreme Court in

Navtej Singh Johar v. Union of India affirmed that indirect discrimination — facially neutral practices that have a disproportionate adverse impact on a protected class — can violate Articles 14 and 15.⁸

Applied to algorithmic bias, this doctrine has significant implications. An ADM system deployed in public employment that systematically produces lower scores for Scheduled Caste applicants — even without explicitly processing caste as an input variable — may constitute indirect discrimination under Article 15. However, proving indirect discrimination in the ADM context requires access to the model's training data, parameters, and output distributions across demographic categories. Without statutory disclosure obligations, such proof is practically impossible to obtain.

C. The Right to Fair Procedure

Article 21 also encompasses the right to fair procedure in any state action that affects life or liberty. The Supreme Court in *Maneka Gandhi v. Union of India* held that procedure under Article 21 must be fair, just, and reasonable. Where ADM systems are deployed by state actors — or by private actors in state-regulated contexts such as banking, insurance, and public utilities — the constitutional requirement of fair procedure may mandate some form of explanation and opportunity to contest.⁹

The doctrinal question is whether the constitutional guarantee of fair procedure requires substantive explainability — a meaningful account of the algorithmic reasoning — or merely procedural notification that an automated system was used. Indian courts have not yet authoritatively resolved this question, but the trajectory of Article 21 jurisprudence, consistently expansive since *Maneka Gandhi*, suggests that substantive explainability would be constitutionally required in high-stakes ADM contexts involving state action.

IV. INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023: AN ANALYSIS

A. Overview and Structural Architecture

The Digital Personal Data Protection Act, 2023 (DPDP Act) received Presidential assent on 11 August 2023 and is expected to come into force in phased tranches through 2024 and 2025. The Act establishes a framework for the processing of digital personal data, creates the Data Protection Board of India as the primary regulatory authority, and codifies the rights

of data principals and the obligations of data fiduciaries. It is broadly modelled on the General Data Protection Regulation (EU) 2016/679 (GDPR), though with significant departures that reflect India's political economy and administrative capacity.¹⁰

The Act identifies seven grounds for lawful processing of personal data: consent; certain legitimate uses including employment; compliance with legal obligations; state functions; medical emergencies; public health emergencies; and safety of the individual. Unlike the GDPR, the DPDP Act does not adopt the GDPR's taxonomy of lawful bases including 'legitimate interests', a departure that has significant implications for the lawfulness of commercial ADM.¹¹

B. The DPDP Act and Automated Decision-Making: A Critical Absence

The most striking feature of the DPDP Act from the perspective of ADM governance is what it does not contain. Unlike the GDPR, which in Article 22 provides a specific prohibition on solely automated decisions that produce legal or similarly significant effects, subject to limited exceptions, the DPDP Act contains no provision specifically addressing automated decision-making. This is not an oversight: the absence of an Article 22 equivalent was a deliberate choice, noted by commentators during the consultation process. Its consequences are, however, severe.

In the absence of an ADM-specific provision, the only DPDP Act mechanisms potentially applicable to algorithmic accountability are: Section 11, which grants the data principal the right to a summary of the personal data processed and the identities of other data fiduciaries with whom it has been shared; Section 12, which grants the right to correction and erasure of inaccurate personal data; and Section 13, which grants the right to grievance redressal. None of these provisions specifically addresses the right to know that an automated decision was made, the right to understand its logic, or the right to contest its substantive outcome. A data principal adversely affected by an ADM system's decision has, under the DPDP Act, no right to know that an algorithm decided their fate.¹²

C. Data Fiduciary Obligations and Their Limits

The DPDP Act imposes on data fiduciaries a set of obligations including accuracy, storage limitation, and security of personal data. Section 8(3) requires data fiduciaries to ensure

the completeness, accuracy, and consistency of personal data, particularly where the data will be used to make decisions affecting the data principal. This provision could be construed to impose an implicit obligation to prevent biased training data from being used in ADM systems — a 'garbage in, garbage out' principle with legal force. However, this reading is speculative, has not been tested by the Data Protection Board, and provides no individual-level remedy for an adversely affected data principal.¹³

The Act also designates certain entities as 'Significant Data Fiduciaries' (SDFs), subject to enhanced obligations including data protection impact assessments and the appointment of a Data Protection Officer. The criteria for SDF designation are to be prescribed by the Central Government. If high-risk ADM deployment were included among the criteria for SDF designation, this could provide a regulatory lever for imposing enhanced algorithmic accountability obligations. As of the date of this paper, no SDF designation criteria have been published.

D. The Consent Framework and Automated Processing

The DPDP Act's primary mechanism for protecting data principals is consent: personal data may not be processed without the data principal's free, specific, informed, unconditional, and unambiguous consent, except in the limited legitimate use cases enumerated in Section 7. In the ADM context, the consent mechanism is structurally inadequate. Studies in behavioural economics and human-computer interaction consistently demonstrate that consent to data processing — especially through click-through consent to privacy policies — does not produce genuine informed authorisation for complex algorithmic processing. A data principal who consents to a financial institution processing their personal data to 'assess creditworthiness' does not thereby give meaningful consent to the use of a machine-learning model that employs proxy variables correlating with protected characteristics.¹⁴

V. THE EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT, 2024: AN ANALYSIS

A. Overview and Risk-Based Architecture

Regulation (EU) 2024/1689 of the European Parliament and of the Council, commonly known as the EU AI Act, entered into force on 1 August 2024 and applies in phased tranches

over a two-year transition period. It constitutes the world's first comprehensive horizontal legislation specifically governing artificial intelligence systems. The Act adopts a risk-based architecture, classifying AI systems into four tiers: prohibited AI practices (Article 5), high-risk AI systems (Articles 6–51), limited-risk AI systems subject to transparency obligations (Articles 50–53), and general-purpose AI models (Articles 51–56).¹⁵

The risk-based architecture is the EU AI Act's most significant structural contribution to the global debate on AI governance. Rather than imposing uniform obligations on all AI systems — which would be both disproportionate and administratively unworkable — the Act concentrates its most demanding obligations on the systems that pose the greatest risk to fundamental rights, health, safety, and democracy.

B. Prohibited AI Practices

Article 5 of the EU AI Act prohibits a set of AI practices that the European legislature has determined to be incompatible with Union values regardless of any risk-benefit assessment. These include: AI systems that deploy subliminal techniques to manipulate behaviour; AI systems that exploit vulnerabilities of specific groups; real-time remote biometric identification in public spaces (subject to narrow law enforcement exceptions); AI systems used for social scoring by public authorities; and AI systems that make risk assessments of individuals based on profiling to predict criminal conduct. The last prohibition is directly relevant to predictive policing and pre-trial risk assessment tools, which several Indian state governments have begun deploying.¹⁶

C. High-Risk AI Systems and Algorithmic Accountability

Annex III of the EU AI Act designates eight categories of AI deployment as inherently high-risk, attracting the Act's most demanding obligations. These include AI systems used in: (i) biometric identification and categorisation; (ii) critical infrastructure management; (iii) education and vocational training; (iv) employment and workers management; (v) access to essential private and public services including creditworthiness assessment; (vi) law enforcement; (vii) migration, asylum, and border control management; and (viii) administration of justice and democratic processes. The breadth of this list reflects a deliberate policy choice to treat ADM in high-stakes social contexts as categorically riskier than its benefits would justify without rigorous safeguards.¹⁷

For high-risk AI systems, the Act imposes obligations that are directly relevant to algorithmic bias and the right to explanation: mandatory risk management systems (Article 9); data governance requirements mandating that training, validation, and testing datasets be free from bias (Article 10); technical documentation requirements (Article 11); automatic logging of operations enabling post-hoc auditability (Article 12); transparency and provision of information to users (Article 13); human oversight mechanisms (Article 14); and accuracy, robustness, and cybersecurity requirements (Article 15).

D. The Right to Explanation under the EU AI Act

The EU AI Act's treatment of the right to explanation is both its most significant contribution and its most significant limitation. Article 86 provides that any person subject to a decision made with the use of a high-risk AI system that produces legal effects or significantly affects them shall have the right to obtain an explanation of the role of the AI system in the decision-making procedure and the main elements of the decision taken. This provision creates, for the first time in primary EU legislation, a specific individual right to algorithmic explanation distinct from the GDPR's existing provisions.¹⁸

However, Article 86's right to explanation is significantly constrained. First, it applies only to 'high-risk AI systems' within the Act's classification — systems used for general commercial decision-making that do not fall within Annex III's enumerated categories may not be covered. Second, the right is to an explanation of 'the main elements of the decision' — a formulation that falls short of requiring disclosure of the model's parameters, training data, or quantitative feature importance. Third, the right is subject to the caveat that the explanation shall not affect 'rights and freedoms of others including trade secrets or intellectual property' — a carve-out that deployers may exploit to withhold meaningful disclosure. Fourth, the right is subject to national implementing legislation, creating the possibility of uneven enforcement across Member States.¹⁹

E. Conformity Assessment and Enforcement

High-risk AI systems under the EU AI Act must undergo a conformity assessment before market deployment. For most high-risk systems, this is a self-assessment against the Act's requirements, documented in technical files maintained by the provider. For certain biometric and law enforcement applications, third-party conformity assessment by a notified

body is required. The conformity assessment regime is analogous to the CE marking system in product safety law and reflects the EU legislature's preference for ex ante market regulation over ex post liability.²⁰

Enforcement authority rests with national market surveillance authorities designated by Member States. The European AI Office, established within the European Commission, has competence over general-purpose AI models and provides coordination across Member States. Maximum administrative fines reach EUR 35 million or 7% of global annual turnover for violations of Article 5 (prohibited practices), EUR 15 million or 3% for other violations, and EUR 7.5 million or 1.5% for providing incorrect information to authorities. These fines are deliberately punitive to create genuine deterrence for large technology companies.

VI. COMPARATIVE ANALYSIS: FOUR DIMENSIONS

A. Scope and Definition of Algorithmic Bias

The EU AI Act's approach to algorithmic bias is substantive and mandatory: Article 10 requires that training, validation, and testing datasets be subject to data governance and management practices that examine the datasets for possible biases, taking into account their geographical, contextual, behavioural, or functional setting. This is not merely aspirational — it is a binding technical requirement, the non-compliance with which triggers the conformity assessment failure and can result in market prohibition. The DPDP Act, by contrast, contains no provision addressing training data quality, bias examination, or demographic fairness in ADM outputs. Section 8(3)'s accuracy obligation is a weak and implicit substitute.

The EU AI Act's definition of 'AI system' — 'a machine-based system that, for a given set of objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions influencing real or virtual environments' — is broad enough to encompass virtually all commercial ADM systems. India's DPDP Act contains no definition of an AI system or algorithmic decision-making process. This definitional vacuum means that even if the DPDP Act were amended to address ADM, the scope of the amendment would be uncertain.

B. Enforceability of the Right to Explanation

The EU AI Act's Article 86 right to explanation, despite its limitations, is a justiciable

individual right enforceable before national courts and regulatory authorities. The GDPR's Article 22 right not to be subject to solely automated decisions, which operates alongside the AI Act, provides a further layer of protection. Together, these provisions create a multi-layered explainability framework — imperfect, contested, but legally actionable.²¹

India's DPDP Act provides no equivalent. The data principal's rights under Sections 11 to 13 — to a summary of processing, to correction, and to grievance redressal — are procedural rather than substantive. They address the data itself, not the decision made on the basis of the data. An individual denied a loan by an algorithmic credit scoring system has, under the DPDP Act, a right to know what personal data the bank holds about them, but no right to know how that data was weighted, combined, and processed to produce the denial. This is a fundamental gap that no amount of creative statutory interpretation can bridge.

C. Accountability Mechanisms for High-Risk AI

The EU AI Act's high-risk classification system creates a tiered accountability architecture that is calibrated to the magnitude of potential harm. The requirement of human oversight under Article 14 — mandating that high-risk AI systems be designed so as to enable natural persons to effectively oversee their functioning — is particularly significant. It prevents the delegation of irreversible, high-stakes decisions entirely to algorithmic systems, preserving human agency at the point of decision. India has no equivalent provision. Public sector ADM deployment in India — including in tax assessment, welfare eligibility, and law enforcement — proceeds without any mandatory human oversight requirement.²²

The EU AI Act's post-market monitoring obligations (Article 72) require deployers of high-risk AI systems to collect and analyse data on the system's performance after deployment, including the detection of incidents and malfunctions. This creates an ongoing, dynamic accountability obligation — not merely an ex ante conformity assessment. Combined with the mandatory logging requirements of Article 12, which ensure that high-risk AI operations are automatically recorded in a format enabling post-hoc investigation, the EU Act creates the infrastructure for evidence-based accountability that India entirely lacks.

D. Remedial Architecture

The EU AI Act's remedial architecture operates on two levels. At the regulatory level,

national market surveillance authorities have investigatory and enforcement powers, including the power to order market withdrawal of non-compliant systems. At the individual level, Article 86 creates an individual right to explanation, and the GDPR's Article 22(3) requires that where an individual is subject to a solely automated decision, the controller shall implement suitable measures to safeguard the data subject's rights, including at minimum the right to obtain human intervention, to express their point of view, and to contest the decision. Together, these provisions create a meaningful individual remedy.²³

India's remedial architecture for ADM harms is fragmented and inadequate. An individual adversely affected by an algorithmic decision may have recourse to: the Data Protection Board under the DPDP Act for data-related grievances; the Information Technology Act 2000 for certain cyber-related harms; the Consumer Protection Act 2019 for defects in services involving ADM; constitutional writ jurisdiction for state ADM deployment; and ordinary civil tort law for negligence. None of these remedies specifically addresses the distinctive harms of algorithmic bias — the systematic, opaque, and self-reinforcing nature of which makes individual proof of causation extremely difficult in the absence of disclosure obligations.

VII. REFORM PROPOSALS FOR INDIA

A. Amend the DPDP Act to Address ADM Specifically

The most urgent reform is the insertion into the DPDP Act of a provision modelled on GDPR Article 22, prohibiting solely automated decisions that produce legal or similarly significant effects on data principals, subject to limited exceptions for consent and contract necessity, and mandating in all cases the right to human review, the right to express one's point of view, and the right to contest the decision. This provision should apply to both public and private sector ADM deployment and should be unwaivable by consent.

B. Introduce a Statutory Right to Explanation

India should enact a statutory right to explanation for ADM, distinct from the right to contest, that entitles the data principal to receive: (i) confirmation that an automated system was used to reach the decision; (ii) a plain-language explanation of the principal factors and their relative weights in the decision; (iii) disclosure of the categories of data used; and (iv)

information about the accuracy and error rates of the system as applied to persons in the data principal's demographic profile. This right should be enforceable before the Data Protection Board and before civil courts, with the burden of proof on the data fiduciary to demonstrate compliance.²⁴

C. Establish a Risk-Based AI Governance Framework

India should develop a risk-based AI governance framework, potentially as a standalone AI Act or as amendments to the DPDP Act and the Information Technology Act 2000, that designates high-risk AI applications in a manner analogous to EU AI Act Annex III. Priority categories for India should include: AI systems used in credit and insurance underwriting; AI systems used in public employment and university admissions; AI systems used in healthcare triage and diagnosis; AI systems used in law enforcement and pre-trial risk assessment; and AI systems used in welfare eligibility determination. Each category should attract mandatory bias audits, human oversight requirements, and enhanced explainability obligations.

D. Mandate Algorithmic Impact Assessments

Analogous to the DPDP Act's Data Protection Impact Assessment requirement for Significant Data Fiduciaries, India should mandate Algorithmic Impact Assessments (AIAs) for any entity deploying a high-risk ADM system. An AIA should assess: (i) the purpose and scope of the ADM system; (ii) the demographic composition of the affected population and the risk of disparate impact; (iii) the quality and representativeness of training data; (iv) the technical measures implemented to detect and mitigate bias; (v) the human oversight mechanisms in place; and (vi) the grievance and appeal procedures available to affected individuals. AIAs should be published in summary form to enable civil society oversight.²⁵

E. Establish an Algorithmic Accountability Tribunal

The Data Protection Board as currently constituted under the DPDP Act lacks the technical expertise to adjudicate complex claims of algorithmic bias. India should consider establishing a specialist Algorithmic Accountability Tribunal or empowering the Data Protection Board with a dedicated algorithmic accountability division, staffed by members with interdisciplinary expertise in law, computer science, statistics, and social science. This body

should have the power to order algorithmic audits by court-appointed technical experts, to award compensation to individuals adversely affected by biased ADM, and to impose injunctive relief suspending the operation of non-compliant systems.

F. Engage Proactively with International Standards Development

India is a member of ISO/IEC JTC 1/SC 42, the international standards committee on artificial intelligence, and participates in OECD discussions on AI governance. India should use these forums to advocate for AI governance standards that are appropriate for developing economies — standards that account for the limited administrative capacity of many developing country regulators, the risk that overly prescriptive standards could inhibit beneficial AI deployment, and the distinctive bias risks that arise in the specific socio-economic contexts of the Global South. India's experience with ADM in social welfare delivery, electoral processes, and financial inclusion provides a unique and valuable comparative perspective.²⁶

VIII. CONCLUSION

Algorithmic bias and the absence of a right to explanation are not technical problems awaiting a technical solution. They are legal and political problems that require legal and political responses — responses that take seriously the constitutional commitment to equality, dignity, and fair procedure that lies at the heart of democratic governance. India's Constitution, through Puttaswamy's recognition of informational privacy, Navtej's embrace of indirect discrimination doctrine, and Maneka Gandhi's expansive conception of fair procedure, provides a constitutional foundation for algorithmic accountability that is at least as robust as the EU's Charter of Fundamental Rights. What India lacks is not constitutional authority but statutory implementation.

The EU AI Act is an imperfect instrument — its right to explanation is narrower than it appears, its conformity assessment regime places excessive trust in self-declaration, and its enforcement architecture will take years to operationalise. But it represents a serious and systematic attempt to bring the rule of law to bear on one of the most consequential developments in the history of governance: the delegation of decisions about human lives to machines that nobody fully understands. India cannot afford to approach this challenge with the DPDP Act's current combination of ambition and silence.

The reforms proposed in this paper — a statutory ADM provision, an individual right to explanation, a risk-based AI governance framework, mandatory algorithmic impact assessments, and a specialist accountability tribunal — are neither utopian nor prohibitively costly. They are calibrated responses to a specific and urgent governance gap, drawing on the best of comparative international practice while remaining cognisant of India's constitutional framework, administrative reality, and development context. The question is not whether India will need to address algorithmic accountability — it will, and urgently. The question is whether it will do so proactively and deliberately, or reactively and inadequately, after the harms have accumulated and the political pressure becomes irresistible. This paper advocates, strongly, for the former.

Endnotes:

¹ Writ Petition (Civil) No. 11498/2022 (Delhi High Court) (unreported). The facts described are based on the author's research into publicly available case filing records and do not reproduce any confidential information.

² The paper adopts a doctrinal methodology supplemented by comparative analysis. All statutory citations are to the Digital Personal Data Protection Act 2023 (Act No. 22 of 2023) and Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 as published in the Official Journal of the European Union, L 2024/1689.

³ Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76, 77–78.

⁴ Harini Suresh and John Guttag, 'A Framework for Understanding Sources of Harm throughout the Machine Learning Life Cycle' (2021) Proceedings of the 1st ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization 1; Solon Barocas and Moritz Hardt, 'Fairness in Machine Learning' (NeurIPS Tutorial 2017).

⁵ Rashida Richardson, Jason Schultz and Kate Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice' (2019) 94 New York University Law Review Online 192 (discussing feedback loop bias in predictive policing).

⁶ Tom Tyler, *Why People Obey the Law* (Princeton University Press 1990) 3–7; Antoinette Rouvroy and Thomas Berns, 'Algorithmic Governmentality and Prospects of Emancipation' (2013) 177 *Rezeaux* 163.

⁷ Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 (Supreme Court of India) [Chandrachud J] paras 114–127.

⁸ Navtej Singh Johar v Union of India (2018) 10 SCC 1 (Supreme Court of India) [Chandrachud J] para 383 (indirect discrimination); cf Nitisha v Union of India (2021) 15 SCC 534 (Supreme Court of India) (adopting disparate impact analysis).

⁹ Maneka Gandhi v Union of India (1978) 1 SCC 248 (Supreme Court of India) [Bhagwati J] (procedure must be 'fair, just and reasonable').

¹⁰ Digital Personal Data Protection Act 2023 (Act No. 22 of 2023), received Presidential assent 11 August 2023. See also Ministry of Electronics and Information Technology, 'Note on the Digital Personal Data Protection Bill 2023' (2023).

¹¹ Digital Personal Data Protection Act 2023, s 4 (grounds for processing); cf Regulation (EU) 2016/679 (GDPR), Art 6 (six lawful bases including legitimate interests under Art 6(1)(f)).

¹² Digital Personal Data Protection Act 2023, ss 11–13; cf GDPR Art 22 (right not to be subject to solely automated

decisions). For the absence of an ADM provision, see Rishab Bailey and Nehaa Chaudhari, 'The Digital Personal Data Protection Act 2023: A Critical Review' (Centre for Internet and Society, 2023).

¹³ Digital Personal Data Protection Act 2023, s 8(3); cf GDPR Art 5(1)(d) (accuracy principle).

¹⁴ Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54(2) *Journal of Economic Literature* 442; Yannis Bakos, Florencia Marotta-Wurgler and David Trossen, 'Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts' (2014) 43(1) *Journal of Legal Studies* 1.

¹⁵ Regulation (EU) 2024/1689 (EU AI Act), Art 1; entered into force 1 August 2024, OJ L 2024/1689.

¹⁶ EU AI Act, Art 5(1)(d) (social scoring by public authorities); Art 5(1)(e) (criminal risk prediction). For Indian predictive policing, see Srinivas Kodali, 'Predictive Policing in India' (Internet Freedom Foundation, 2021).

¹⁷ EU AI Act, Annex III (high-risk AI systems list); Art 6 (classification rules).

¹⁸ EU AI Act, Art 86(1); cf GDPR Art 22(3) (right to human intervention, expression of view, and contest for solely automated decisions).

¹⁹ EU AI Act, Art 86(2) (trade secrets carve-out); Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For' (2017) 16 *Duke Law and Technology Review* 18.

²⁰ EU AI Act, Arts 43–44 (conformity assessment); Arts 74–77 (market surveillance and enforcement).

²¹ EU AI Act, Art 86; GDPR Art 22; Case C-634/21 SCHUFA Holding AG (Scoring) EU:C:2023:957 (CJEU, 7 December 2023) (credit scoring constitutes solely automated decision-making under GDPR Art 22).

²² EU AI Act, Art 14 (human oversight); cf Antoinette Rouvroy, 'The End(s) of Critique: Data Behaviourism vs Due Process' in Mireille Hildebrandt and Katja de Vries (eds), *Privacy, Due Process and the Computational Turn* (Routledge 2013).

²³ EU AI Act, Art 86; GDPR Art 22(3); cf Regulation (EU) 2022/2065 (Digital Services Act), Art 17 (analogous individual redress for content moderation decisions).

²⁴ For the content of a right to explanation, see Finale Doshi-Velez and others, 'Accountability of AI Under the Law: The Role of Explanation' (2017) arXiv:1711.01134; Berk Ustun and Cynthia Rudin, 'Supersparse Linear Integer Models for Optimized Medical Scoring Systems' (2016) 59(4) *Machine Learning* 349.

²⁵ David Reisman and others, 'Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability' (AI Now Institute, 2018); cf Canadian Government, *Directive on Automated Decision-Making* (2019) (AIA requirement for federal government ADM).

²⁶ OECD, 'Recommendation of the Council on Artificial Intelligence' OECD/LEGAL/0449 (2019); ISO/IEC 42001:2023 (Artificial Intelligence Management System); Chinmayi Arun, 'AI and the Global South: Designing for Other Worlds' (2020) 167 *University of Pennsylvania Law Review Online* 56.

BIBLIOGRAPHY

A. Primary Sources: Legislation and Regulatory Instruments

Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) (India).

Information Technology Act, 2000 (Act No. 21 of 2000) (India).

Consumer Protection Act, 2019 (Act No. 35 of 2019) (India).

Constitution of India, 1950, Arts 14, 15, 16, 19, 21.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (EU AI Act), OJ L 2024/1689.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), OJ L 119/1.

OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (22 May 2019).

ISO/IEC 42001:2023, Artificial Intelligence — Management System (International Organization for Standardization, 2023).

Canadian Government, Directive on Automated Decision-Making (Treasury Board of Canada Secretariat, 1 April 2019).

B. Primary Sources: Cases

Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 (Supreme Court of India).

Navtej Singh Johar v Union of India (2018) 10 SCC 1 (Supreme Court of India).

Nitisha v Union of India (2021) 15 SCC 534 (Supreme Court of India).

Maneka Gandhi v Union of India (1978) 1 SCC 248 (Supreme Court of India).

Case C-634/21 SCHUFA Holding AG (Scoring) EU:C:2023:957 (CJEU, 7 December 2023).

Loomis v Wisconsin 881 NW 2d 749 (Wisconsin Supreme Court 2016) (COMPAS risk assessment).

C. Books

Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publishers 2016).

Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press 2018).

Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press 2015).

Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015).

Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).

Tom Tyler, *Why People Obey the Law* (Princeton University Press 1990).

D. Articles and Reports

Wachter S, Mittelstadt B and Floridi L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) *International Data Privacy Law* 76.

Edwards L and Veale M, 'Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For' (2017) 16 *Duke Law and Technology Review* 18.

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

Doshi-Velez F and others, 'Accountability of AI Under the Law: The Role of Explanation' (2017) arXiv:1711.01134.

Suresh H and Gutttag J, 'A Framework for Understanding Sources of Harm throughout the Machine Learning Life Cycle' (2021) *ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization*.

Richardson R, Schultz J and Crawford K, 'Dirty Data, Bad Predictions' (2019) 94 New York University Law Review Online 192.

Reisman D and others, 'Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability' (AI Now Institute 2018).

Arun C, 'AI and the Global South: Designing for Other Worlds' (2020) 167 University of Pennsylvania Law Review Online 56.

Bailey R and Chaudhari N, 'The Digital Personal Data Protection Act 2023: A Critical Review' (Centre for Internet and Society 2023).

WIPO, 'Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence' WIPO/IP/AI/2/GE/20/1 (2020).