

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Beyond the Black Box: Algorithmic Accountability and the Legal Regulation of Predictive Analytics and Machine Learning in India

GAYATHRI* AND DR. RAJVENDRA KUMAR CHAUDHARI**

ABSTRACT

The proliferation of predictive analytics and machine-learning systems has transformed decision-making across banking, insurance, healthcare, employment, policing, welfare administration, education and advertising in India. Algorithms no longer merely inform human choices; with increasing frequency they determine outcomes that affect individuals' rights, livelihoods and opportunities. This transformation has produced what is commonly described as the "black box" problem: decisions are generated through processes that are technically complex, commercially proprietary and cognitively opaque, leaving affected persons unable to understand, contest or seek redress against them. Algorithmic systems trained on historical data further risk reproducing and amplifying existing patterns of discrimination against already disadvantaged groups. India's existing legal architecture, anchored principally in the Digital Personal Data Protection Act, 2023, offers meaningful safeguards for the processing of personal data but does not comprehensively regulate the algorithmic decisions that such data ultimately produces. Constitutional guarantees of equality and non-arbitrariness under Article 14 and of privacy, dignity and personal liberty under Article 21 supply an important normative foundation for extending accountability beyond data governance. This paper undertakes a doctrinal examination of algorithmic accountability in India through the interconnected lenses of privacy, equality, transparency, explainability, human oversight and effective remedy, and identifies significant regulatory gaps in the current framework. It concludes by proposing a rights-based, risk-sensitive and lifecycle-oriented framework for algorithmic accountability grounded in Indian constitutional principles rather than transplanted wholesale from foreign models.

Keywords: *Algorithmic Accountability, Predictive Analytics, Machine Learning, Artificial Intelligence, Algorithmic Bias, Explainability, Data Protection, Automated Decision-Making, Privacy, India*

* Author is a Research Scholar at Faculty of Law, Mansarovar Global University, Sehore, Madhya Pradesh, India.

** Author is an Associate Professor at Faculty of Law, Mansarovar Global University, Sehore, Madhya Pradesh, India.

I. INTRODUCTION

Decision-making in contemporary India is undergoing a silent but sweeping change. Decisions once made through human intuition, judgment or deliberation are increasingly delegated, wholly or partly, to statistical models trained on large volumes of data.¹ Predictive analytics and machine-learning systems now establish creditworthiness, set insurance premiums, evaluate job applicants before a human recruiter has seen their résumés, flag suspicious banking transactions and advise doctors on treatment. In many fields, rapid advances in personalisation are driven by algorithms and programs that either open up new areas or extend their success in established domains.² This transition raises a peculiar legal issue, usually captured by the metaphor of the ‘black box’. A machine-learning system may produce an outcome in a specific case (the rejection of a loan application, the refusal of a job, the assignment of a risk score), yet neither the person concerned nor, often, the organisation deploying the system can explain what data were used, which variables carried decisive weight, how those variables were combined, why this input produced this outcome, and who or what is responsible for the result.³ The central legal question that arises is whether a decision can be legally accountable when the reasoning behind it cannot be understood, reproduced or challenged.

In this paper, algorithmic accountability denotes a set of related legal and institutional obligations: making the existence and functioning of automated systems transparent, explaining particular outcomes, identifying the party responsible for harm, auditing the underlying model, ensuring human supervision of critical decisions, enabling unfavourable outcomes to be challenged, ensuring that outcomes are not discriminatory, and providing effective remedies.⁴ Algorithmic accountability is much wider than personal data protection, although it is closely connected to it and often conflated with it in Indian policy discussions.

¹ PRASHANT MAHAJAN, THE SOUL OF THE AI: GOVERNANCE, ETHICS, AND THE FUTURE OF HUMAN-AI INTEGRATION (Zenodo 2025), <https://doi.org/10.5281/zenodo.15789678>; https://www.researchgate.net/publication/393281204_The_Soul_of_the_AI_Governance_Ethics_and_the_Future_of_Human-AI_Integration (last visited Aug. 9, 2026).

² Aditi Bhutoria, *Personalized Education and Artificial Intelligence in the United States, China, and India: A Systematic Review Using a Human-in-the-Loop Model*, 3 COMPUTERS & EDUC.: ARTIFICIAL INTELLIGENCE 100068 (2022), <https://doi.org/10.1016/j.caeai.2022.100068>.

³ Benjamin van Giffen, Dennis Herhausen & Tobias Fahse, *Overcoming the Pitfalls and Perils of Algorithms: A Classification of Machine Learning Biases and Mitigation Methods*, 144 J. BUS. RES. 93 (2022), <https://doi.org/10.1016/j.jbusres.2022.01.076>.

⁴ Loso Judijanto, Rustiyana & Rusdi, *AI-Governance and Algorithmic Accountability: Rethinking Legal Standards in the Age of Autonomous Decision-Making*, 5 INT’L J. HUMAN. SOC. SCI. & BUS. 11 (2026), <https://injoqast.net/index.php/JOSSS/article/view/762>; https://www.researchgate.net/publication/399961047_AI-GOVERNANCE_AND_ALGORITHMIC_ACCOUNTABILITY_RETHINKING_LEGAL_STANDARDS_IN_THE_AGE_OF_AUTONOMOUS_DECISION-MAKING.

The problem analysed in this paper is the conflict between technological progress and efficiency on the one hand, and privacy, equality, dignity, fairness and accountability on the other. At present, Indian law in this field is developing mainly around data protection and data governance, whereas algorithmic decision-making raises a different and broader issue: the fairness of the decision made, and not merely the legality of the data used to make it.

The literature, in India and globally, has addressed the ethics of AI, the right to privacy, data protection law, the technical aspects of machine learning, the sociology of algorithmic bias and related questions. What is missing is a unified analysis of predictive analytics and machine learning focused on algorithmic accountability, one that holds privacy, equality, explainability, transparency, human oversight and remedies within a single analytical framework in the context of Indian law.

A. Research questions

1. To what extent does existing Indian law regulate predictive analytics and machine-learning-based decision-making?
2. Does India's existing legal framework adequately address algorithmic opacity, bias, discrimination and the absence of explainability?
3. How can the constitutional principles of equality, privacy and non-arbitrariness be applied to algorithmic decision-making?
4. What legal and institutional mechanisms are necessary to establish an effective framework for algorithmic accountability in India?

B. Objectives

1. To examine the legal regulation of predictive analytics and machine learning in India.
2. To analyse the legal implications of algorithmic opacity and automated decision-making.
3. To assess the adequacy of existing Indian data-protection and constitutional safeguards.
4. To identify regulatory gaps concerning bias, transparency, explainability and accountability.
5. To propose a rights-based framework for algorithmic accountability in India.

II. PREDICTIVE ANALYTICS, MACHINE LEARNING AND THE BLACK BOX PROBLEM

Predictive analytics is the use of past trends and data, together with statistical and computational algorithms, to generate insights about present characteristics or to classify them. In India, banks and non-banking financial companies use predictive models for credit scoring and for automated fraud detection, including in payment systems.⁵ What matters from a legal point of view is not the prediction technique itself but the fact that institutions treat its results as sufficient for conclusive decisions on whether to grant a loan or whether a transaction is fraudulent.

Although machine learning is often treated as a form of predictive analytics, it differs in one important respect: the analyst does not specify the rules by which conclusions are drawn; instead, the system identifies patterns in the data as it is trained on a dataset.⁶ Whether the method is supervised learning or another learning technique, what is legally significant is that the relationship between input and output is determined by the model itself rather than by its human designers, which makes it much harder to reconstruct the model's logic afterwards.

For the purposes of accountability, three modes of human involvement may be distinguished: a human decision assisted by an algorithm, where the machine supplies information that a human considers before deciding; an algorithmic recommendation that a human must approve or reject; and full automation, with no human participation in the decision.⁷ The legal responsibility assigned to a human, and with it the strength of the case for algorithmic regulation, varies across these three modes.

Legal analysis must also distinguish several sources of algorithmic opacity. Technical opacity concerns the difficulty of interpreting complex, high-dimensional models such as deep neural networks, whose parameters do not correspond to any reason a human can understand. Proprietary or commercial opacity arises when information about a system's construction,

⁵ Khirod Chandra Panda & Shobhit Agrawal, *Predictive Analytics: An Overview of Evolving Trends and Methodologies*, 8 J. SCI. & ENG'G RES. 175 (2021), <https://jsaer.com/download/vol-8-iss-10-2021/JSAER2021-8-10-175-180.pdf>;

https://www.researchgate.net/publication/380399051_Predictive_Analytics_An_Overview_of_Evolving_Trends_and_Methodologies.

⁶ *Machine Learning: An Overview*, SCIENCE DIRECT TOPICS, <https://www.sciencedirect.com/topics/computer-science/machine-learning> (last visited Aug. 9, 2026).

⁷ Kaśka Porayska-Pomsta & Gnanathusharan Rajendran, *Accountability in Human and Artificial Intelligence Decision-Making as the Basis for Diversity and Educational Inclusion*, in ARTIFICIAL INTELLIGENCE AND INCLUSIVE EDUCATION 39 (Jeremy Knox, Yuchen Wang & Michael Gallagher eds., 2019), https://doi.org/10.1007/978-981-13-8161-4_3; https://www.researchgate.net/publication/333760281_Accountability_in_Human_and_Artificial_Intelligence_Decision-Making_as_the_Basis_for_Diversity_and_Educational_Inclusion.

training data or logic is withheld for commercial reasons.⁸ Institutional opacity is the practical impossibility of obtaining information that does exist, because no one is under a duty to disclose it. These forms of opacity bear differently on legal responsibility: the first tests the limits of explainability as a remedy, while the latter two are amenable to legal intervention.

Bias in machine learning arises from one or more of the following sources: historical data reflecting past discriminatory practices; incomplete or unrepresentative datasets that leave out certain groups; facially neutral proxy variables that are stable correlates of protected attributes (such as postal code or level of education); design choices about the target of prediction; and feedback loops, in which the data used to train a model come to include the model's own earlier decisions.⁹ Experience in other countries shows automated recruitment processes producing discriminatory results against women candidates, credit-scoring systems disadvantaging applicants from under-banked communities, and predictive-policing systems directing police towards areas that are already over-policed.

III. RESEARCH METHODOLOGY AND LEGAL FRAMEWORK

This paper follows the doctrinal method of legal research, supported by interdisciplinary material from computer science, information ethics and regulatory theory. The primary sources consulted are constitutional provisions, statutes, delegated legislation, judicial decisions and regulatory guidelines; the secondary sources are government policy documents, committee reports, international regulatory instruments and academic writing.¹⁰ The doctrinal method suits the paper's aim, which is not to build empirical models of algorithmic bias but to assess how well existing legal concepts, developed long before algorithmic decision-making emerged, respond to it.

The Indian legal framework is analysed through a rights-based and accountability-based lens built on the seven principles set out in Table 1. The principles are not treated as independent concepts; each forms part of a single accountability relationship running from the designers and deployers of an algorithm to the person whose rights are affected by its outcomes.

Principle	Central Question
Privacy	Is personal data adequately protected across the algorithmic lifecycle?

⁸ Bram Vaassen, *AI, Opacity, and Personal Autonomy*, 35 PHIL. & TECH. 88 (2022), <https://link.springer.com/article/10.1007/s13347-022-00577-5>.

⁹ Jingxi Liu, Xiaojun Luo & Guan H. Tang, *Bridging Fairness in Machine Learning: A Legal Critique of Technical Strategies*, 61 COMPUTER L. & SEC. REV. 106339 (2026), <https://doi.org/10.1016/j.clsr.2026.106339>.

¹⁰ HIGHLINE COLLEGE LIBRARY, *Introduction to Law: Primary and Secondary Sources*, <https://library.highline.edu/c.php?g=344547&p=2320319> (last visited Aug. 9, 2026).

Principle	Central Question
Equality	Can algorithmic decisions produce direct, indirect or proxy discrimination?
Transparency	Can the existence and general operation of the decision-making process be understood?
Explainability	Can an affected person understand the reasons for a particular outcome?
Accountability	Which actor bears legal responsibility for the outcome produced?
Human Oversight	Can the decision be meaningfully reviewed or overridden by a human being?
Remedy	Can affected persons challenge the decision and obtain effective redress?

Table 1: Analytical framework for assessing algorithmic accountability

IV. EXISTING INDIAN LEGAL FRAMEWORK

Article 14 of the Constitution guarantees equality before the law and the equal protection of the laws. Indian constitutional doctrine reads Article 14 as a guarantee against arbitrary state action, and requires any classification to rest on an intelligible differentia bearing a rational nexus to the object it seeks to achieve. Algorithmic decision-making puts Article 14 under strain, because it raises the question whether a statistical classification produced by an opaque algorithm rests on a relevant and rationally connected basis, and whether either the affected person or the body applying the algorithm can give any rational account of how the classification was made.¹¹ It follows that a governmental algorithm that fails the requirement of transparency may amount to an unjustified exercise of state power.

Article 21 provides that no person shall be deprived of life or personal liberty except according to procedure established by law. The Supreme Court has read Article 21 expansively to include the dignity and autonomy of every person and the right to privacy. Its recognition of informational privacy, or informational self-determination, supplies a normative basis for the claim that people must be told when, and on what basis, an algorithm has taken a decision about them, since profiling engages the very autonomy the Court has protected.¹² Further, the

¹¹ *Right to Equality under the Indian Constitution: A Study of Articles 14–18*, LAWCTOPUS, <https://www.lawctopus.com/clatalogue/constitutional-law/right-to-equality-under-constitution-of-india/> (last visited Aug. 9, 2026); see also *State of W.B. v. Anwar Ali Sarkar*, AIR 1952 SC 75 (reasonable classification); *E.P. Royappa v. State of T.N.*, (1974) 4 SCC 3 (arbitrariness as the antithesis of equality).

¹² Tannu Manoj Mishra, *Article 21 and End-of-Life Autonomy: A Legal Examination of India's Right to a Dignified Death*, VINTAGE LEGAL (Aug. 6, 2025), <https://www.vintagelegalvl.com/post/article-21-and-end-of-life-autonomy-a-legal-examination-of-india-s-right-to-a-dignified-death> (last visited Aug. 9, 2026); see *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (recognising privacy, including informational privacy, as a fundamental right protected by Article 21 and Part III).

proportionality test articulated in *Puttaswamy* offers a standard against which automated profiling, at least by the State and those exercising public power, can be assessed.¹³

Indian courts apply the principles of natural justice (*audi alteram partem*, the duty to give reasons and the broader requirement of procedural fairness) well beyond formal adjudicatory tribunals, to administrative action generally. In *Maneka Gandhi v. Union of India*, the Supreme Court held that any procedure depriving a person of personal liberty under Article 21 must be right, just and fair, and not arbitrary, fanciful or oppressive.¹⁴

The Digital Personal Data Protection Act, 2023 is India's first comprehensive law in this area, regulating the processing of digital personal data on the basis of consent or of certain specified legitimate uses.¹⁵ The Act obliges "data fiduciaries" to process personal data only for lawful and specified purposes and with appropriate safeguards, and places additional obligations on those notified as "significant data fiduciaries". It gives "data principals" rights to obtain information about, correct and erase their personal data and to have their grievances redressed, and it establishes the Data Protection Board of India to inquire into breaches of the Act. The provisions constituting the Board came into force when the Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025, but the duties of data fiduciaries and the rights of data principals take effect only eighteen months later, in May 2027.¹⁶ These are meaningful safeguards. The Act, however, is concerned with the lawfulness of processing personal data as an input; it does not regulate the fairness, reliability or explicability of the automated decision-making process that uses that data.¹⁷ Unlike the European Union's General Data Protection Regulation, which gives individuals a right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects, together with safeguards that include the right to obtain human intervention and to contest the decision, the 2023 Act confers no specific right in respect of automated decisions as a category.¹⁸ This is a

¹³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (requiring legality, a legitimate aim and proportionality for any restriction of privacy); see also *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar)*, (2019) 1 SCC 1 (applying the proportionality test to the Aadhaar scheme).

¹⁴ *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

¹⁵ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 4, 7.

¹⁶ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 8, 10, 11–13, 18; MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, Notification G.S.R. 843(E) (Nov. 13, 2025) (bringing §§ 18–26 into force at once, and §§ 3–17, save § 6(9), eighteen months after publication); Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), r. 1 (Nov. 13, 2025).

¹⁷ *But see* Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), r. 13(3) (Nov. 13, 2025) (requiring a significant data fiduciary, from May 2027, to observe due diligence to verify that technical measures, including algorithmic software, adopted by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of data principals).

¹⁸ Vani Bhushan, *Empowering Individuals: A Deep Dive into the Digital Personal Data Protection Act, 2023*, 12 INT'L J. ADVANCED RES. 891 (2024), <https://doi.org/10.21474/IJAR01/18799>; https://www.researchgate.net/publication/381383119_EMPOWERING_INDIVIDUALS_A_DEEP_DIVE_INTO

central question for this paper: does regulating the processing of personal data amount to regulating the algorithmic decision that follows from it? The analysis here indicates that it does not. Data regulation is a necessary but insufficient part of algorithmic accountability.

The Information Technology Act, 2000 is relevant to algorithmic systems mainly through its provisions on compensation for failure to protect sensitive personal data, punishment for disclosure of information in breach of a lawful contract, and the liability of intermediaries and their safe-harbour protection.¹⁹ These provisions were designed to regulate electronic records, cyber security and the conduct of intermediaries; they offer no guidance on how a decision-making algorithm works or whether its decisions are accurate or discriminatory. The Act is therefore of limited relevance to machine-learning-based systems.

Sector-specific regulation of algorithms is limited, as Table 2 summarises. The most extensively regulated sector is banking and digital lending. The Reserve Bank of India (Digital Lending) Directions, 2025, which consolidate the Reserve Bank's 2022 Guidelines on Digital Lending, require the regulated lender to obtain, and keep on record for audit, information on the borrower's economic profile before assessing creditworthiness, require loan offers from multiple lenders to be displayed by lending platforms in an unbiased and objective manner, mandate standardised disclosure through a key fact statement, and require lenders and their service providers to designate nodal grievance-redressal officers. They do not, however, expressly require disclosure of the logic of algorithmic credit decisions. Algorithms in the insurance industry are regulated only indirectly, through general e-commerce and regulatory-sandbox rules. Employment, healthcare and predictive policing have no specific regulation, and general law remains the only instrument available for them.²⁰

THE DIGITAL PERSONAL DATA PROTECTION ACT 2023; cf. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 22, 2016 O.J. (L 119) 1.

¹⁹ Rahul Kailas Bharati, *Cyber Security, Data Protection, and the IT Act*, in *HANDBOOK ON THE INFORMATION TECHNOLOGY ACT, 2000: OFFENCES, PENALTIES, AND THE IMPACT OF NEW CRIMINAL LAWS* 292 (Deep Sci. Publ'g 2025), https://www.researchgate.net/publication/394378693_Cyber_Security_Data_Protection_and_the_IT_Act; see The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), §§ 43A, 72A, 79; The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021). Section 43A is omitted by § 44(2) of the Digital Personal Data Protection Act, 2023 once that provision commences in May 2027.

²⁰ RESERVE BANK OF INDIA, *Reserve Bank of India (Digital Lending) Directions, 2025*, RBI/2025-26/36, DOR.STR.REC.19/21.07.001/2025-26, ¶¶ 6(iv), 7, 8, 11 (May 8, 2025), <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12848&Mode=0>.

Sector	Illustrative Use of Predictive Analytics / ML	Governing Instrument(s)
Banking & Finance	Algorithmic credit scoring and digital-lending risk assessment	RBI (Digital Lending) Directions, 2025 (consolidating the 2022 Guidelines on Digital Lending)
Insurance	Automated underwriting and risk-based premium pricing	IRDAI e-commerce & sandbox guidelines
Employment	Automated resume screening and candidate ranking	No dedicated statute; DPDP Act, 2023 (data only)
Healthcare	ML-assisted diagnostic support and treatment recommendation	No dedicated statute; general tort and DPDP Act, 2023
Policing	Predictive-policing and crime hot-spot identification	No dedicated statute; constitutional review only

Table 2: Sectoral snapshot of algorithmic regulation in India

Alongside legislation, India has produced a body of policy documents setting out approaches to AI. NITI Aayog's National Strategy for Artificial Intelligence envisions "AI for All" and identifies healthcare, agriculture, education, smart cities and smart mobility among its priority sectors. Its two-part Responsible AI approach document sets out principles for the responsible design and deployment of AI. The Report of the Committee of Experts on Non-Personal Data Governance Framework, constituted by the Ministry of Electronics and Information Technology, also examines the data-sharing infrastructure that could be used to train algorithms.²¹ The significant limitation of these documents is that they are policy instruments and not law: they create no justiciable rights for individuals affected by algorithmic decisions and impose no obligations enforceable by courts or regulators.

V. ALGORITHMIC ACCOUNTABILITY: EMERGING LEGAL CHALLENGES

A primary question is whether people should be entitled, as of right, to notice that an automated system was used to make a decision about them, what kind of data was applied, what factors generally drove the inference, and who operates the system. It is useful to distinguish two levels of transparency: system-level transparency, which concerns information about a system's existence, purpose and logic of operation, and individual-level transparency, which concerns

²¹ Robert Gianni, Santtu Lehtinen & Mika Nieminen, *Governance of Responsible AI: From Ethical Guidelines to Cooperative Policies*, 4 FRONTIERS COMPUTER SCI. 873437 (2022), <https://doi.org/10.3389/fcomp.2022.873437>; https://www.researchgate.net/publication/360846007_Governance_of_Responsible_AI_From_Ethical_Guidelines_to_Cooperative_Policies (last visited Aug. 9, 2026); see NITI AAYOG, *National Strategy for Artificial Intelligence* (June 2018); NITI AAYOG, *Responsible AI: Approach Document for India, Part 1: Principles for Responsible AI* (Feb. 2021); NITI AAYOG, *Responsible AI: Approach Document for India, Part 2: Operationalizing Principles for Responsible AI* (Aug. 2021); MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, *Report by the Committee of Experts on Non-Personal Data Governance Framework* (rev. Dec. 2020).

what influenced the decision in a particular person's case.²² At present Indian law addresses only a few instances of the first level, for example in digital credit and lending.

Transparency concerns knowing how a system functions in general; explainability concerns understanding how a particular decision was reached in an individual case. A system may be transparent, in that its structure and training process are public, and yet remain unaccountable at the level of the individual outcome, especially where the model is complex. The difference matters legally, because a right to system-level transparency will not help a person contest an adverse decision in his or her own case.

Direct discrimination occurs when a protected characteristic is used in the decision itself; indirect discrimination occurs when a neutral condition has an unfavourable impact on a protected group; and proxy discrimination occurs when a variable correlated with a protected characteristic is used, intentionally or not, as a stand-in for it. Since Indian equality jurisprudence already recognises indirect and disproportionate impact as a form of discrimination, there is a reasonable legal basis for extending Article 14 scrutiny to discriminatory algorithmic outcomes produced by government bodies, or by entities licensed by them, even in the absence of intentional discrimination.²³ Applying the same standard to private algorithmic actors is far more problematic, given the limited horizontal application of Part III of the Constitution, a gap that anti-discrimination legislation could close.

Predictive analytics depends on the collection and processing of massive volumes of data, which creates risks that go beyond the protection of any individual's data. Studies have identified threats arising from the profiling of people in different contexts, predictions about them, function creep (data collected for one purpose being used for another), and the inference of sensitive characteristics (such as health conditions, sexual orientation, political opinions or caste) from innocuous data through statistical correlation.²⁴ Importantly, an algorithm can derive

²² Mohamed Kentour & Joan Lu, *Analysis of Trustworthiness in Machine Learning and Deep Learning*, in PROCEEDINGS OF THE ELEVENTH INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATIONS AND COMPUTATION (INFOCOMP 2021) 1 (IARIA 2021), https://www.thinkmind.org/index.php?view=article&articleid=infocomp_2021_1_10_60003; https://www.researchgate.net/publication/359858765_Analysis_of_trustworthiness_in_machine_learning_and_deep_learning.

²³ Manasi Shah, *Supreme Court Review 2024: Recognising 'Substantive Equality' to Address Systemic Barriers*, SUPREME COURT OBSERVER (Jan. 2, 2025), <https://www.scobserver.in/journal/supreme-court-review-2024-recognising-substantive-equality-to-address-systemic-barriers/> (last visited Aug. 9, 2026); see also *Nitisha v. Union of India*, (2021) 15 SCC 125 (recognising indirect discrimination).

²⁴ Gold Nmesoma Okorie et al., *Ethical Considerations in Data Collection and Analysis: A Review: Investigating Ethical Practices and Challenges in Modern Data Collection and Analysis*, 6 INT'L J. APPLIED RES. SOC. SCI. 1 (2024), <https://doi.org/10.51594/ijarss.v6i1.688>; https://www.researchgate.net/publication/378789304_ETHICAL_CONSIDERATIONS_IN_DATA_COLLECTION_AND_ANALYSIS_A_REVIEW_INVESTIGATING_ETHICAL_PRACTICES_AND_CHALLENGES_IN_MODERN_DATA_COLLECTION_AND_ANALYSIS (last visited Aug. 9, 2026).

sensitive information about people who never supplied it, and consent-based regulation does not account for this, because consent is usually given for the data actually collected rather than for the inferences drawn from it.

A recurring regulatory requirement is that a human should be involved in significant algorithm-generated decisions. The literature notes, however, that “human-in-the-loop” oversight risks becoming a formality in which the person simply approves the algorithm’s output without independent evaluation. For human supervision to be meaningful rather than formal, there must be independent evaluation of the case, the ability to override the machine’s recommendation, access to the information needed for that evaluation, and assignment of responsibility for the decision to the human being. Indian sectoral regulation has not yet absorbed this: the Reserve Bank of India’s digital-lending directions require the regulated lender to obtain the information needed to assess creditworthiness and to keep it on record for audit, but they do not expressly require human review of automated credit decisions.²⁵

Responsibility for algorithmic harm must be seen as shared among several parties: the developer who builds the model, the vendor that licenses it, the data controller who supplies data for its training and deployment, and the person who acts on its outputs. Figure 1 represents this accountability problem. Assigning liability becomes harder as the number of actors grows, and depends on how far the harmful outcome can be traced to the model’s own contribution.²⁶

Existing tort, contract and data-protection law in India offers some means of determining the liability of individual parties, but no clear framework for allocating responsibility across the chain of events that leads to a harmful outcome. On whether an individual can challenge an unfavourable algorithmic decision, several questions arise: which party should explain the decision, whether the algorithm can be independently evaluated by a third party, what information an affected individual can obtain from the institution that deployed the algorithm, and what role courts and regulators should play.

²⁵ Hannah Ruschemeier & Lukas J. Hondrich, *Automation Bias in Public Administration: An Interdisciplinary Perspective from Law and Psychology*, 41 GOV’T INFO. Q. 101953 (2024), <https://doi.org/10.1016/j.giq.2024.101953>; see RESERVE BANK OF INDIA, *Digital Lending Directions*, *supra* note 20, ¶ 7.

²⁶ Kirsten Martin, *Ethical Implications and Accountability of Algorithms*, 160 J. BUS. ETHICS 835 (2019), <https://doi.org/10.1007/s10551-018-3921-3>; https://www.researchgate.net/publication/324896361_Ethical_Implications_and_Accountability_of_Algorithms.

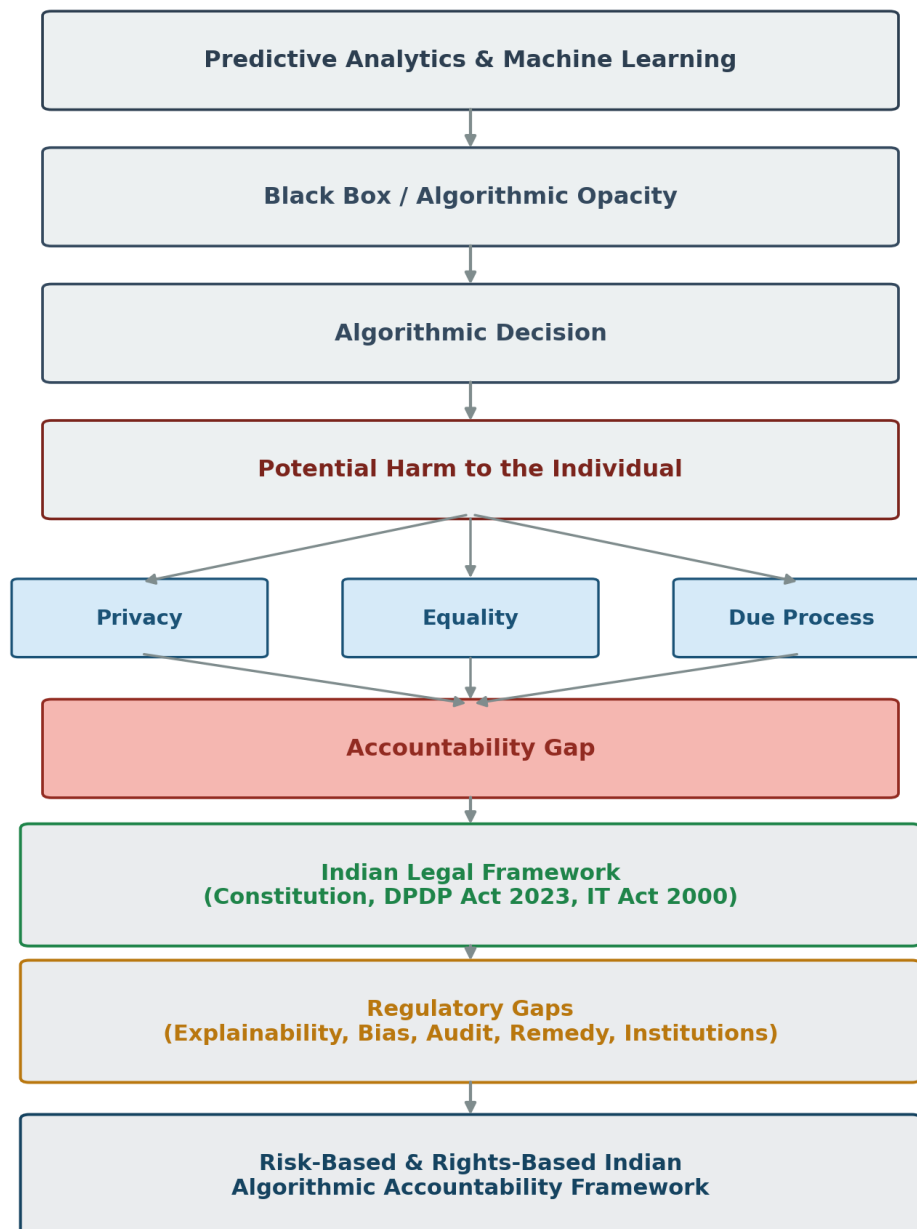


Figure 1: Structure of the argument, from algorithmic opacity to an accountability framework

VI. CRITICAL ASSESSMENT OF INDIA'S REGULATORY FRAMEWORK

Rather than treating the deficiencies identified in the two preceding sections as a miscellaneous list, it is more useful to organise them into seven distinct, though interrelated, regulatory gaps, summarised in Table 3.

Gap	Description
Accountability Gap	No clearly defined allocation of legal responsibility across the developer–vendor–deployer–decision-maker lifecycle.
Explainability Gap	No legally enforceable right to an individualised explanation of significant automated decisions.

Gap	Description
Bias & Discrimination Gap	Data-protection compliance does not, without more, prevent or remedy discriminatory algorithmic outcomes.
High-Risk AI Gap	Absence of a comprehensive statutory risk-classification model comparable to dedicated AI-specific regulatory regimes.
Audit Gap	Limited legal framework for independent algorithmic impact assessments or third-party audits.
Remedy Gap	Individuals lack accessible, specialised mechanisms to challenge harmful algorithmic decisions.
Institutional Gap	Fragmentation across data protection, cybersecurity, consumer protection, financial and competition regulation.

Table 3: Principal regulatory gaps in India's algorithmic governance framework

VII. TOWARDS AN INDIAN FRAMEWORK FOR ALGORITHMIC ACCOUNTABILITY

The proposed framework places algorithmic systems in four risk classes, drawing on comparative experience with risk-tiering instruments such as the European Union's Artificial Intelligence Act while adapting the substantive categories to Indian constitutional requirements, as shown in Figure 2. Low-risk systems, such as ordinary recommendation systems, would be subject only to minimal transparency requirements. Moderate-risk systems, which influence outcomes significantly but not decisively, would be subject to documentation and grievance mechanisms. High-risk systems used in employment, credit, healthcare, education, policing, criminal justice, welfare and other essential public services would be subject to the full set of requirements discussed below. In addition, a small category of unacceptable-risk applications that violate constitutional rights would be prohibited.²⁷

²⁷ Cristina Peterson, *EU AI Act Risk Categories: Which Tier Is Your AI System?*, AIRIA (Apr. 14, 2026), <https://airia.com/blog/eu-ai-act-risk-categories-which-tier-is-your-ai-system/> (last visited Aug. 9, 2026); see Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), arts. 5, 6, 50 & annex III, 2024 O.J. (L 1689) 1.

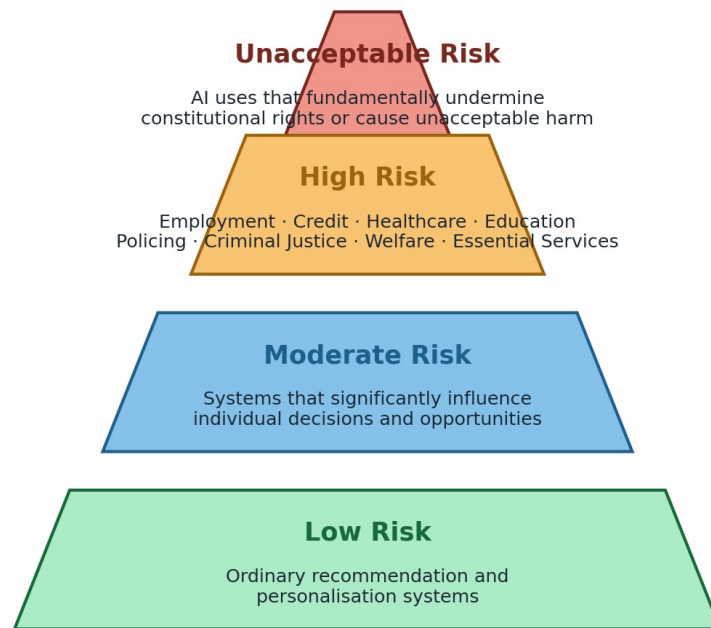


Figure 2: Proposed risk-based classification of AI systems

High-risk systems should undergo an Algorithmic Impact Assessment (AIA) before deployment and periodically afterwards, examining privacy, the potential for discrimination, accuracy and reliability, security, the effect on fundamental rights, the degree of explainability and prospective social harm. An AIA would give algorithmic systems a mechanism comparable to environmental impact assessment in environmental law: a structured, documented, prior evaluation that creates a public record against which later claims can be tested. High-risk systems should also be subject to transparency rules: individuals should know that an algorithmic system was used in their case and what basic factors it takes into account in decisions of that kind. The organisation that built the system should be identified, and sufficient technical records should be kept to allow the development of the system used in the particular case to be reconstructed.²⁸

The framework proposes a legally binding right for every individual affected by an automated or semi-automated decision to obtain a personalised explanation. The explanation should address the particulars of the individual case and not merely describe the system used. Affected persons should also be able to have the decision reviewed by a human being with the competence and authority to reconsider it, and to obtain a fresh decision. High-risk systems should be tested periodically by an independent certified auditor or by the sector regulator for

²⁸ Heike Felzmann et al., *Transparency You Can Trust: Transparency Requirements for Artificial Intelligence Between Legal Norms and Contextual Concerns*, 6 BIG DATA & SOC'Y 1 (2019), <https://doi.org/10.1177/2053951719860542>; https://www.researchgate.net/publication/333918635_Transparency_you_can_trust_Transparency_requirements_for_artificial_intelligence_between_legal_norms_and_contextual_concerns.

bias and discrimination, accuracy, security, reliability and explainability. Audit findings bearing significantly on systemic risk must be reported to the relevant sector regulator or to a central algorithmic-accountability authority, and adverse findings should place heightened obligations on the deploying entity.

The framework proposes a lifecycle-based model of liability running from developer to provider to deployer to human decision-maker. Responsibility for a specific harm would depend on the degree of control each actor had over the relevant design or deployment choice, whether it had actual or constructive knowledge of the associated risk, the foreseeability of the harm that materialised, the extent of its involvement in the particular decision, and its practical ability to prevent the harm. This avoids placing the whole burden of liability on the deploying institution, which is usually best placed to mitigate harm at the point of application but least equipped to detect flaws introduced at the design stage.

Finally, courts should be recognised as residual but significant actors in reviewing algorithmic decisions made by the State, or by private actors performing public functions, through established doctrinal tools: the Article 14 non-arbitrariness test, proportionality and privacy review under Article 21, and the principles of natural justice and reasoned decision-making discussed in this paper.

VIII. CONCLUSION

This paper has argued that while Indian law offers a substantial basis for controlling the data processed by predictive analytics and artificial intelligence systems, data stewardship alone cannot secure accountability for the algorithms themselves. The Digital Personal Data Protection Act, 2023 provides useful safeguards on how personal data is collected, processed and secured, although its principal obligations take effect only in May 2027; the Constitution, through Articles 14 and 21 and the principles of natural justice, supplies essential reference points against capricious and incomprehensible state action; and a few sector regulators, principally the Reserve Bank of India, have begun to impose obligations on automated processes in the sectors they govern.²⁹ None of these instruments, separately or together, provides a mechanism that regulates algorithmic decisions as a whole, addressing the transparency, bias, human involvement, audit and remediation issues that arise when an algorithm makes a decision.

²⁹ Shubham Saurabh, *The Digital Personal Data Protection Act of 2023: Strengthening Privacy in the Digital Age*, 3 INT'L J.L. CHANGING WORLD 77 (2024), <https://doi.org/10.54934/ijlcw.v3i2.84>; https://www.researchgate.net/publication/387550185_THE_DIGITAL_PERSONAL_DATA_PROTECTION_ACT_OF_2023_STRENGTHENING_PRIVACY_IN_THE_DIGITAL_AGE.

Effective regulation therefore requires a shift from the data-protection paradigm towards the regulation of algorithms. The framework proposed here gives effect to that shift through the risk-based classification of algorithms, mandatory algorithmic impact assessment, rights to transparency, explanation and human review, independent audit, a lifecycle model of liability and constitutional review.³⁰ The paper has sought to show that privacy, equality, transparency, explainability, human involvement, audit, accountability, liability and remediation can be integrated in a way that is both logically coherent and practically viable within India's existing legal framework.

Finally, the paper deliberately rejects the wholesale transplantation of foreign regulatory solutions, such as the European Union's risk-based AI Act. Indian solutions should grow out of India's own constitutional inheritance, namely the principles of equality, dignity, privacy, non-arbitrariness and procedural fairness, adapted to the scale, nature and socio-economic circumstances of the population that algorithms will govern.

³⁰ Ben Green, *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, 45 COMPUTER L. & SEC. REV. 105681 (2022), <https://doi.org/10.1016/j.clsr.2022.105681>.