

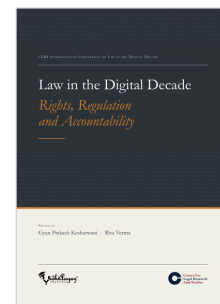
CHAPTER 8

AI and Legal Accountability in India: Rethinking Responsibility for Automated Decisions

Nony Nema

in *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma (VidhiAagaz 2026), pp. 89–98

DOI <https://doi.org/10.63108/VAB.LDD.1.8>



CITATIONS

BLUEBOOK (21ST ED.)

Nony Nema, *AI and Legal Accountability in India: Rethinking Responsibility for Automated Decisions*, in *LAW IN THE DIGITAL DECADE: RIGHTS, REGULATION AND ACCOUNTABILITY* 89 (Gyan Prakash Kesharwani & Ritu Verma eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Nony Nema, ‘AI and Legal Accountability in India: Rethinking Responsibility for Automated Decisions’ in Gyan Prakash Kesharwani and Ritu Verma (eds), *Law in the Digital Decade: Rights, Regulation and Accountability* (VidhiAagaz 2026) 89.

CHICAGO (17TH ED.)

Nema, Nony. “AI and Legal Accountability in India: Rethinking Responsibility for Automated Decisions.” In *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma, 89–98. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.1.8>.

APA (7TH ED.)

Nema, N. (2026). AI and legal accountability in India: Rethinking responsibility for automated decisions. In G. P. Kesharwani & R. Verma (Eds.), *Law in the digital decade: Rights, regulation and accountability* (pp. 89–98). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.1.8>

SOURCE

<https://doi.org/10.63108/VAB.LDD.1.8>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 8

AI and Legal Accountability in India: Rethinking Responsibility for Automated Decisions

NONY NEMA*

In this algorithmic age, AI systems are impacting a wide range of decisions across organizations. The growing use of AI and automated decision-making systems in India has created new challenges for legal accountability. AI systems are increasingly being used in almost every sector. While these systems can make decisions quickly and efficiently, there are chances that they may produce unfair, incorrect or harmful outcomes. This raises an important question: who should be legally responsible when an automated decision causes harm?

The paper examines whether the existing legal framework in India is sufficient to assign responsibility for harmful or unfair decisions made through AI and automated systems. The paper adopts a doctrinal approach to examine relevant legislation, judicial decisions, regulatory developments in India relating to AI, data protection, liability and automated decision-making. The paper argues that although the existing legal frameworks provide some mechanisms to address the harms associated with AI, they do not yet provide a clear and comprehensive framework for allocating legal responsibility for automated decisions. Responsibility is difficult to determine where multiple actors are involved which include developers, deployers, organizations and human users. This may create an accountability gap when an AI system produces an unexpected outcome.

The paper therefore, argues for a clear framework of responsibility based on the degree of control exercised by different actors in the decision-making process. The paper aims to examine how human oversight, transparency, explainability and effective review mechanisms can improve accountability for AI-based decisions in India.

Keywords: Artificial Intelligence, Automated Decision-Making, Legal Accountability, Algorithmic Bias, Human Oversight

1 INTRODUCTION

Artificial Intelligence is defined as the kind of technology that enables computers to perform functions which usually require human intelligence.¹ Artificial Intelligence is now being used in almost every sector be it healthcare, business, finance, education, etc. It is rapidly changing how decisions are being made in these fields. The growing use of AI may lead to algorithmic bias, errors caused due to automated decision-making and even transparency issues. According to Article 22 of the EU's GDPR, a data subject has the right to reject any decision made by automated systems, including algorithmic profiling, if that decision creates serious legal consequences or deeply impacts their life.² While these automated decisions make life faster and more efficient, they also create a major legal problem: who is responsible when an AI makes a mistake? When a technology leads to a financial loss, denies someone a job due to an algorithmic bias

* PhD Scholar at National Law Institute University, Bhopal, Madhya Pradesh, India.

¹ 'Artificial Intelligence' (Oxford Reference) <<https://www.oxfordreference.com/display/10.1093/oi/author-ity.20110803095426960>> accessed 2 October 2026.

² 'Art. 22 GDPR – Automated Individual Decision-Making, Including Profiling' (*General Data Protection Regulation (GDPR)*) <<https://gdpr-info.eu/art-22-gdpr/>> accessed 8 September 2026.

or gives a wrong medical diagnosis, traditional laws struggle to find the party who is to be held responsible.

Modern AI systems that are built on deep learning process massive amounts of data to find patterns and make decisions. Artificial intelligence is a dynamic system which keeps on learning and this makes it difficult to identify the defect or harm caused. The Consumer Protection Act, 2019 provides a way to address AI-related harm through product liability and deficiency of service provisions. However, since the law was not specifically designed for AI-related risks, its application to AI systems may raise certain legal challenges. There are hardly any court decisions which clearly determine whether algorithmic decision-making systems are covered within the ambit of product liability.³

The ‘black-box effect’ refers to advanced AI systems whose internal decision-making processes are completely hidden and unknown and that creates a gap in the existing legal frameworks because if the law can’t trace how a machine reached a conclusion, it cannot fairly determine who to hold accountable for the harm caused. One solution to address this accountability issue is explainability, which involves the process of defining how an algorithm arrived at a particular solution. If an AI system’s decision-making process can be defined and understood in a transparent manner then accountability can be determined easily. The EU’s AI Act has recognized transparency and explainability as important mechanisms for ensuring accountability in AI-assisted decision-making. Under Article 86 of the act, the affected persons are in certain situations entitled to receive meaningful explanations of the role played by a high-risk AI system in the decision-making process.⁴ This approach seeks to ensure that automated systems remain capable of scrutiny and promote fair and accountable decision-making.

The ‘OECD AI Principles’ are guidelines for developing and using AI that is trustworthy and beneficial to society. These principles were first adopted in 2019 and were the first intergovernmental standard on AI. Among these five principles, there are two principles which focus on ‘transparency and explainability’ and ‘accountability’, respectively. Principle 1.3 talks about ‘Transparency and Explainability’, and emphasizes transparency and responsible disclosure in the use of AI systems, ensuring that individuals are aware when they are interacting with AI and have the ability to question or challenge its outcomes. AI actors should provide meaningful and context-appropriate information about AI systems, consistent with current technological standards. This information should help stakeholders understand the capabilities and limitations of AI, recognize when they are interacting with an AI system, and, where practical, understand the data factors, processes or logic that contributed to an AI-generated prediction, recommendation, content or decision. Such transparency should also enable individuals affected negatively by an AI system to understand and challenge its outputs.⁵

According to Principle 1.5 that is the ‘Accountability’ principle, individuals and organizations that are involved in the development, deployment or operation of AI systems should be responsible for ensuring that these systems function appropriately and in accordance with the OECD’s values-based AI principles. AI actors should assume responsibility for the performance of AI systems and compliance with these principles, taking into consideration their respective roles, the context in which the systems are used, and

³ ‘Who Is Liable When Artificial Intelligence Fails’ (4 February 2026) <<https://www.lawctopus.com/academike/who-is-liable-when-artificial-intelligence-fails/>> accessed 13 September 2026.

⁴ ‘Article 86: Right to Explanation of Individual Decision-Making | EU Artificial Intelligence Act’ (*EU AI Act Explorer*) <<https://artificialintelligenceact.eu/article/86/>> accessed 8 September 2026.

⁵ ‘Transparency and Explainability (OECD AI Principle)’ <<https://oecd.ai/en/dashboards/ai-principles/P7>> accessed 23 September 2026.

the level of technological development available. To support this accountability, appropriate traceability mechanisms should be maintained throughout the AI lifecycle, including records concerning the datasets, processes and decisions involved. This enables AI outputs and responses to be examined and assessed when required. Furthermore, AI actors should adopt a continuous and systematic approach to risk management across all stages of the AI lifecycle. Depending on their responsibilities and ability to influence the system, they should take appropriate measures to identify and mitigate risks associated with AI. This may involve cooperation among developers, technology and data providers, users and other relevant stakeholders. Such risks may include algorithmic bias, threats to human rights, safety and security concerns, privacy risks, and issues relating to labor and intellectual property rights.⁶

In India, this lack of clarity regarding accountability creates a serious gap in the legal system. Existing laws such as the IT Act, 2000 and the Digital Personal Data Protection Act, 2023 were implemented to address cybercrimes and data privacy issues but they fail to address the errors caused by an AI system's automated decision-making. As the existing laws do not view AI as a 'person', policymakers find it difficult to figure out who should be held responsible among the software developers, the company deploying the AI, and the end-users.

The research paper aims to examine the current legal landscape with respect to AI accountability in India and highlight the limitations of our existing statutes. The paper aims to analyze how India can close these regulatory gaps and also highlights the need to develop a clear legal framework that balances technological innovation with strict liability and mandatory human oversight.

2 BACKGROUND

At present, India currently lacks a comprehensive statutory framework specifically tailored to regulate artificial intelligence, leaving critical issues such as algorithmic bias, automated decision-making and the problem of explainability unaddressed. The IT Act, 2000 and the DPDP Act, 2023 are the primary legislation in India addressing digital governance. However, they do not directly address the legal complexities introduced by autonomous algorithms.

The IT Act, 2000 was enacted long before the advent of machine learning and primarily focuses on cybercrimes and safe harbor immunities for intermediaries, failing to explain AI decision-making and accountability issues. Similarly, while the DPDP Act, 2023 mandates structural compliances for data processing and user consent, it remains silent on automated profiling and fails to grant individuals the right to seek an explanation for automated decisions.⁷

Algorithmic opacity represents a major risk of these AI systems as they function as 'black boxes'; their decision-making process is frequently unexplainable even to their own developers which creates legal difficulties. If an individual falls victim to an erroneous automated decision – whether through a denied loan, a platform suspension or systemic profiling – a critical question remains: how can decisions made by AI algorithms be contested and what legal channels exist to challenge an invisible algorithm? AI systems are built and used by different actors. Where one person develops the base model, some other person is responsible for supplying training data, someone embeds the model in a service and another

⁶ 'Accountability (OECD AI Principle)' <<https://oecd.ai/en/dashboards/ai-principles/P9>> accessed 23 September 2026.

⁷ 'AI AND DATA PROTECTION: CHALLENGES IN AUTOMATED DECISION-MAKING - IISPPR' (28 February 2025) <<https://iisppr.org.in/ai-and-data-protection-challenges-in-automated-decision-making/>> accessed 9 September 2026.

person uses the output in order to make decisions. In case of harm, the actors may state that the responsibility lies somewhere else. Current laws are used to finding a single person at fault, so they fail to assign blame clearly in such cases.⁸

In the case of *Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd.* 2026, the NCLT relied on six fabricated case citations generated by an AI tool, which were later discovered and challenged before the Supreme Court. The case highlighted that AI-generated legal content must be independently verified by humans. Responsibility remains with the human decision-maker or lawyer using the AI output while submitting unverified AI-generated material may amount to professional misconduct, and reliance on such material can invalidate a judicial order.⁹

3 ANALYSIS

3.1 What Is Automated Decision-Making?

Automated decision-making involves the use of technology to make decisions autonomously without any human involvement in the process and is supervised by machine learning algorithms. AI systems gather data, analyze and evaluate it and make decisions solely.¹⁰ Automated decision-making systems range from simple rule-based systems that follow pre-set rules, to machine learning models that use patterns from past data to make predictions about new cases, and deep learning systems that use complex layers of mathematical processing that can be difficult even for their developers to understand.¹¹

Although the existing legal framework in India does not specifically define the term ‘automated decision-making’, section 2(b) of the DPDP Act, 2023 defines the term ‘automated’, as ‘any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data’.¹²

AI and machine-learning systems can be difficult to understand because there is a lack of clarity regarding how they arrive at decisions. Organizations often build decision-making codes directly into their systems. Over time, these rules can spread across different systems, making them difficult to maintain.¹³

3.2 Existing Legal Framework in India

3.2.1 *Information Technology Act, 2000*

The IT Act is the principal legislative framework governing cyber law in India. The IT Act, 2000 was enacted with the main aim of promoting electronic commerce and addressing cybercrimes. The

⁸ Record Of Law, ‘Algorithmic Power and Legal Accountability: The Case for AI Regulation in India’ (*Record Of Law*, 2 August 2026) <<https://recordoflaw.in/algorithmic-power-and-legal-accountability-the-case-for-ai-regulation-in-india/>> accessed 9 September 2026.

⁹ Tulip Kanth, ‘Zero-Tolerance For Using AI-Generated Precedents Without Verification: Supreme Court Sets Aside NCLT, NCLAT Orders Citing Fake Judgments’ (2 July 2026) <<https://www.verdictum.in/supreme-court/pooja-ramesh-singh-v-jammu-and-kashmir-bank-ltd-2026-insc-668-ai-generated-precedents-1616998>> accessed 23 September 2026.

¹⁰ ‘What Is Automated Decision-Making?’ (7 February 2025) <<https://decisions.com/blog/what-is-automated-decision-making>> accessed 10 September 2026.

¹¹ IJLLR Journal, ‘Algorithm Bias, Automated Decision-Making, And The Right To Explanation: Comparative Analysis Of India’s DPDP Act 2023 And The EU AI Act 2024’ (*IJLLR Journal*, 19 July 2026) <<https://www.ijllr.com/post/algorithm-bias-automated-decision-making-and-the-right-to-explanation-comparative-analysis-of-ind>> accessed 10 September 2026.

¹² Digital Personal Data Protection Act 2023, s 2(b).

¹³ Sparkling Logic, ‘What Is Automated Decision-Making (ADM)?’ (*Sparkling Logic*, 11 October 2024) <<https://www.sparklinglogic.com/what-is-automated-decision-making-adm/>> accessed 10 September 2026.

provisions of the act focus on traditional digital issues like hacking, identity theft, data breaches, etc. The act fails to address the complexities caused by AI systems and issues like algorithmic bias, automated decision-making and lack of transparency; uncertainties regarding who should be held responsible for harm caused by AI remain unresolved.¹⁴

A major gap in the IT Act is the absence of any provision related to artificial intelligence, machine learning or automated systems. The Act fails to define these technologies nor does it outline their scope which results in ambiguity in statutory interpretation. In the absence of clear definitions, courts and regulatory authorities may face difficulties in applying existing legal provisions to AI-driven activities resulting in inconsistent interpretations and legal uncertainty. When AI systems function autonomously, there is difficulty in assigning responsibility in cases of harm as the IT Act does not clearly identify and state whether the liability in such cases should rest with the developers, manufacturers or users of such AI systems. The act does not impose specific obligations of transparency or explainability in relation to algorithmic decision-making processes. Consequently, individuals affected by automated decisions are not given a clear statutory right to challenge such decisions or obtain reasons for the outcomes, raising concerns regarding procedural fairness, accountability and due process.¹⁵

Algorithmic decision-making is often opaque, making it difficult for data subjects to understand how and why particular decisions are reached. The inability of such systems to provide meaningful explanations can further impede individuals from effectively exercising rights such as access, correction and objection. Fundamentally this lack of transparency raises concerns regarding fairness, accountability and due process.¹⁶

When harmful or misleading AI-generated content spreads online, determining who should be held responsible becomes difficult. The existing legal framework mainly provides remedies after harm has occurred such as content takedown, criminal action and civil remedies. However, these measures may not be sufficient to address risks such as deepfakes, automated misinformation and algorithmic discrimination, which can spread rapidly with little or no human involvement. As a result, gaps in accountability may arise, leaving affected individuals with limited and delayed remedies.¹⁷

While the IT Act, 2000 does not clearly address accountability issues caused by AI decision-making, there are certain provisions in the act which address general digital accountability:

- Section 43A – This section requires a body corporate to implement reasonable security practices to protect sensitive personal data but it does not regulate automated profiling or decision-making.¹⁸
- Section 79 – This section provides safe harbor protection for intermediaries, requiring them to practice due diligence, which has been expanded via IT Rules to cover deepfakes and synthetically

¹⁴ Tushar Sahu and Rajeev, 'Inadequacy of the IT Act, 2000 in Governing Artificial Intelligence: Need for Legal Reform' (2026) 8 IJFMR - International Journal For Multidisciplinary Research <<https://doi.org/10.36948/ijfmr.2026.v08i02.73091>> accessed 10 September 2026.

¹⁵ Ibid

¹⁶ Gautam Sharma, 'ARTIFICIAL INTELLIGENCE AND DATA PRIVACY: ETHICAL AND LEGAL CHALLENGES' (*Vintage Legal*, 26 December 2025) <<https://www.vintagelegalvl.com/post/artificial-intelligence-and-data-privacy-ethical-and-legal-challenges>> accessed 12 September 2026.

¹⁷ Arpita Mishra, Dr Monica Yadav and Dr Pooja Batra Nagpal, 'Autonomy, Accountability And Algorithms: India's Cyber Law At A Crossroad' [2026] INTERNATIONAL JOURNAL OF ADVANCES IN SIGNAL AND IMAGE SCIENCES 2390 <<https://doi.org/10.29284/bjwegg22>>.

¹⁸ IT Act 2000, s 43A.

generated content, but it still falls short of governing accountability of AI decision-making algorithms.¹⁹

3.2.2 *Digital Personal Data Protection Act, 2023*

The DPDP Act, 2023 is one of the most significant laws relevant to AI regulation in India currently. But the act does not specifically address automated decision-making of AI systems nor does it require AI systems to provide explanations for their decisions and also fails to provide individuals with a specific right to challenge decisions made by these systems. In contrast, Article 22 of the GDPR provides protection in relation to decisions based solely on automated processing. The absence of similar safeguards in India leaves gaps in algorithmic accountability and may limit the legal remedies available to individuals affected by AI-driven decisions.

Determining liability is a major issue in AI-driven decision-making. When an AI system makes an erroneous decision, like rejecting a job application, denying someone a loan or giving a completely wrong diagnosis of a patient, then who is responsible? Is it the developer, the deploying organization or the government that needs to be blamed? India does not have a dedicated AI-related law currently that assigns liability for AI-related harm. Some legal scholars support a ‘human-in-the-loop’ approach, under which AI-generated decisions are subject to meaningful human oversight, while others favor specific AI-liability frameworks that would hold AI developers and users legally responsible for errors, harmful decisions, and discriminatory outcomes resulting from the use of AI systems.

There is no separate chapter dedicated to AI in the act. However, the act does mention the processing of digital personal data and the term ‘processing’ under section 2(x) of the act is defined broadly enough to include automated operations involving digital personal data.²⁰ The DPDP Act does not contain a standalone provision that expressly prohibits organizations from relying exclusively on automated decision-making. However, such decision-making may still be subject to various provisions of the Act.

Section 8(3) of the DPDP Act requires a data fiduciary to ensure that personal data is complete, accurate and consistent where such data is likely to be used to make a decision affecting a data principal or is intended to be disclosed to another data fiduciary.²¹ This provision is particularly relevant to AI systems deployed in contexts involving consequential decisions, including recruitment and employment, credit assessment, insurance underwriting, eligibility determinations, customer profiling and fraud detection. Accordingly, organizations should ensure that personal data used by AI systems is of appropriate quality and is reliable particularly where such data may inform decisions that significantly affect individuals.²²

The DPDP framework has some relevance to the use of AI and automated decision-making, although it doesn’t establish a standalone regulatory regime governing automated decisions nor does it contain any provision relating to the right to demand human review of an automated decision. The act also does not recognize the rights of data principals to obtain an explanation for decisions made through AI-driven

¹⁹ IT Act 2000, s 79.

²⁰ Digital Personal Data Protection Act 2023, s 2(x).

²¹ Digital Personal Data Protection Act 2023, s 8(3).

²² Dhruv Kaushal, ‘How Does the DPDP Act Regulate AI Training in India?’ (*King Stubb & Kasra*, 9 September 2026) <<https://ksandk.com/data-protection-and-data-privacy/dpdp-act-ai-training-automated-decision-making/>> accessed 12 September 2026.

systems unlike the GDPR framework which contains more extensive transparency requirements in relation to automated decision-making.

The DPDP Act under section 10(1) enables the Central Government to designate certain data fiduciaries, or classes of data fiduciaries as significant data fiduciaries (SDFs), based on factors such as the volume and sensitivity of personal data processed, the risks to data principals, and the potential impact on matters including the sovereignty and integrity of India, electoral democracy, security of the state and public order. SDFs are subject to enhanced compliance requirements which may become particularly relevant where AI or algorithmic systems are used to process personal data.²³

Under Rule 13 of the DPDP Rules, SDFs must conduct a Data Protection Impact Assessment (DPIA) and an audit every 12 months and submit reports containing significant observations to the Board. They must also exercise due diligence to ensure that the technical measures they employ including algorithmic software used for specified processing activities are not likely to pose a risk to the rights of data principals.²⁴ Accordingly, where an AI system forms part of a data-processing operation falling within these requirements, the DPIA, audit and algorithmic due diligence operations may operate as mechanisms for identifying and mitigating risks arising from such systems. However, these provisions do not directly address accountability of AI systems in the decision-making process. The act is relevant primarily through the broader regulation of personal data processing and the additional risk-governance obligations imposed on SDFs.

In 1950, Alan Turing asked the famous question, “Can Machines Think?” in his paper ‘Computing Machinery and Intelligence’. This question raises concerns regarding accountability and responsibility. While machines are responsible for executing algorithms, the responsibility for algorithmic outcomes rests with human designers of such systems. The principles of transparency and human oversight in automated decision-making reflect the idea that responsibility for a machine’s decisions ultimately rests with the organization that deploys and controls it.²⁵

3.2.3 India AI Governance Guidelines, 2025

The guidelines mention seven guiding principles also referred to as ‘sutras’ which aim to regulate India’s AI governance. The fifth principle refers to the principle of ‘accountability’ which states that AI developers and deployers must operate transparently and remain accountable for the systems they create or use. Accountability should be allocated according to the role performed, the potential risk of harm and the applicable due diligence requirements. Accountability can be supported through a combination of regulatory, technical and market-based mechanisms.²⁶

These guidelines mention accountability as the backbone of AI governance. There exists a lack of clarity regarding how liability should be allocated across developers, deployers and end-users. There is a lack of grievance redressal mechanisms available for users. Also, transparency in the design of AI systems, the flow of data and the decision-making processes of organizations remains limited. The probabilistic and adaptive nature of AI may lead to unforeseen outcomes. This creates a need for a governance

²³ Ibid

²⁴ Digital Personal Data Protection Rules 2025, rule 13.

²⁵ Adv (Dr) Prashant Mali, ‘AI and Machine Learning Under DPDP: Compliance Guide for Organizations’ (*DPDPA.com*) <https://www.dpdpa.com/blogs/ai_machine_learning_dpdpa_compliance_guide.html> accessed 12 September 2026.

²⁶ ‘India AI Governance Guidelines’ <<https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2228315>> accessed 13 September 2026.

framework that ensures appropriate oversight and accountability while allowing sufficient space for responsible innovation. The Committee in its recommendations mentions that there is a need to introduce graded obligations and liability frameworks that are proportionate to the functions performed by AI actors, the risks associated with their activities and the extent of due diligence undertaken. Enforcement and accountability need to be strengthened through mechanisms like transparency reporting, independent audits, and self-certification requirements.²⁷

The AI Governance Committee mentions certain practical guidelines for industry and innovators in order to enable responsible implementation of the AI Governance Framework and recommends that all persons involved in the development or deployment of AI systems in India should adhere to the following principles:

- AI developers and deployers should comply with all the applicable laws and regulations in India, including those relating to information technology, data protection, copyright, consumer protection, and the protection of women, children and other vulnerable groups.
- Show compliance with applicable laws and regulations when required by authorities or regulators.
- Adopt voluntary principles, codes and standards to promote privacy, security, fairness, inclusivity, non-discrimination, and transparency, along with appropriate technical and organizational safeguards.
- Set up a grievance system to report AI-related harms and resolve complaints within a reasonable time.²⁸
- Publish transparency reports assessing the risks AI systems may pose to individuals and society in India. Sensitive or confidential information should be shared privately with the relevant regulators.
- Make use of technology and legal measures to reduce AI risks, such as privacy tools, machine un-learning, algorithmic audits, and automated bias detection.²⁹

3.2.4 Sector-Specific Rules

RBI Model Risk Management Guidance, 2026

The Central Bank released its draft, 'Guidance on Regulatory Principles for Model Risk Management, 2026' which are a set of detailed guidelines for models adopted by banks, NBFCs, and other regulated institutions and also includes AI and machine learning systems. These draft guidelines require organizations to implement model risk management frameworks after being approved by the Board, validate models independently, maintain inventories of algorithms that are used for decision-making and set up human oversight regarding AI-driven decisions. According to RBI, a model includes any system that uses data and analytical techniques (includes AI and ML), in order to produce outputs to be used in decision-making and business operations. This definition also includes algorithms, applications, analytics,

²⁷ Ibid

²⁸ 'Decoding the India AI Governance Guidelines - Saikrishna & Associates' (*Saikrishna & Associates - A Tier-1 Full Service Firm*, 10 November 2025) <<https://www.saikrishnaassociates.com/decoding-the-india-ai-governance-guidelines/>> accessed 13 September 2026.

²⁹ Ibid

spreadsheet-based tools and decision-based rules if they impact business decisions like customer pricing and lending rates.³⁰

The draft guidance has also mentioned certain requirements for AI and ML systems which are: assessing risks arising from hallucinations, bias, discrimination in outcomes, adversarial attacks, data drift, etc. Entities are also required to test models under certain conditions and implement required safeguards. RBI has also suggested that regulated entities should establish mandatory human oversight for AI models especially in cases involving automated decision-making by AI models. A complete human-in-the-loop approach, override capabilities and mechanisms for system suspension and deactivation, including kill switches, need to be implemented in order to ensure effective human oversight and control over AI systems. The Central Bank has also cautioned regarding automation bias and overdependence on model outputs.³¹

SEBI (Intermediaries) (Amendment) Regulations, 2025

‘Regulation 16C’ was inserted under these regulations, which makes any SEBI-regulated entity solely responsible for any AI/ML tools used by them, whether it has been developed in-house or externally. This regulation was notified in February, 2025 and closely follows SEBI’s consultation paper of November, 2024, which proposed that every person regulated by SEBI that uses AI shall be solely responsible for protection and security of investor data, responsibility of any AI-generated output it relies on, and compliance with all applicable laws. This rule applies regardless of the extent of AI use, meaning that even limited or third-party use can result in full responsibility. SEBI may also take enforcement action and impose sanctions for any violation under its general powers.³²

Previously, AI-related risks could fall into regulatory grey areas, particularly when determining whether responsibility lies with the technology provider or the user. Regulation 16C removes this uncertainty by placing clear responsibility and liability on intermediaries for all AI systems used in their operations. Another concern is regarding ‘auditability’. Although intermediaries bear responsibility for AI-related outcomes, regulators still need sufficient visibility into how these systems function. This can be challenging because advanced AI systems, particularly complex machine-learning and generative AI models, often operate as ‘black-boxes’, making their decision-making processes difficult to understand or inspect. If SEBI is unable to examine the model’s logic or data flows, placing full liability on the intermediary may create practical difficulties.³³

3.2.5 Artificial Intelligence (Ethics and Accountability) Bill, 2025

The Bill was introduced in the Lok Sabha in December, 2025 and is the first dedicated bill with respect to AI. The Bill establishes a legal ‘right to explanation’ for individuals affected by automated decisions

³⁰ www.ETBFSI.com, ‘RBI Proposes AI Governance Framework for Banks, Mandates Human Oversight of Model Driven Decisions’ (ETBFSI.com) <<https://bfsi.economictimes.indiatimes.com/articles/rbi-unveils-ai-governance-framework-mandating-human-oversight-in-banking/131970975>> accessed 23 September 2026.

³¹ ‘Press Releases | Official Website of Reserve Bank of India’ <https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=5089> accessed 23 September 2026.

³² ‘SEBI | Securities and Exchange Board of India (Intermediaries) (Amendment) Regulations, 2025’ <https://www.sebi.gov.in/legal/regulations/feb-2025/securities-and-exchange-board-of-india-intermediaries-amendment-regulations-2025_91809.html> accessed 23 September 2026.

³³ ‘SEBI’s AI Liability Regulation: Accountability and Auditability Concerns’ (The HNLU CCLS Blog, 3 October 2025) <<https://hnluccls.in/2025/10/03/sebis-ai-liability-regulation-accountability-and-auditability-concerns/>> accessed 23 September 2026.

that have significant legal or commercial consequences. It further introduces the concept of ‘transparency by design’, requiring developers to document aspects such as the model’s architecture, sources of training data, and measures adopted to reduce bias before the system is deployed. The Bill also aims to regulate developers, deployers and users and mentions a civil penalty of Rs. 5 Crore for non-compliance with developer or deployer duties. The Bill also provides compensation to individuals who can establish that they have suffered harm as a result of an algorithmic system. Despite these provisions, the Bill fails to determine the allocation of liability for AI-generated content, leaving uncertainty as to whether responsibility should rest with the developer, deployer or user.³⁴

4 CONCLUSION & SUGGESTIONS

AI is changing how decisions are made, creating new challenges for legal accountability in India. While there is no specific law regulating artificial intelligence in India, existing laws may address certain AI-related harms, yet they do not provide a clear framework for automated decision-making. India therefore needs a balanced approach that clearly assigns responsibility to AI developers and deployers, ensures transparency and human oversight, and manages risks without slowing responsible innovation.

While the AI Governance Guidelines address the accountability issue of automated decision-making systems to a certain extent, there is a need for an AI-specific law which clearly allocates liability and accountability among the developers, deployers and users of an AI system along with clearly mentioning their responsibilities. A human-in-the-loop approach should be followed to ensure that a designated person retains the authority to review, question or challenge AI-generated recommendations. There is also a need to create traceable workflows, and accountability for automated decisions should be established by assigning clear human ownership and defining explicit decision-making processes, rather than attributing responsibility to the algorithm itself.³⁵

India could move towards a structured AI governance framework through proposed legislative measures such as the Digital India Act, which may introduce risk-based regulation, greater transparency, and accountability for AI and emerging technologies. The proposed Artificial Intelligence (Ethics and Accountability) Bill, 2025, also reflects growing interest in stronger safeguards including ethical reviews, bias audits, developer responsibilities, and grievance mechanisms. Although these mechanisms are not yet an established law, they indicate a shift towards clearer legal accountability for AI systems while seeking to support innovation.³⁶

* * *

³⁴ Dhruv, ‘AI Ethics and Accountability Bill 2025 Explained’ (*iPleaders*, 14 May 2026) <<https://blog.iplayers.in/ai-ethics-and-accountability-bill-2025-indias-first-dedicated-ai-bill-explained/>> accessed 23 September 2026.

³⁵ ‘Build Accountability into AI to Drive Business Value | TechTarget’ (*AI & Emerging Tech*) <<https://www.tech-target.com/ai/tip/Build-accountability-into-AI-to-drive-business-value>> accessed 23 September 2026.

³⁶ ‘AI Laws and Regulations in India as of 2026’ <<https://www.prashantmali.com/cyber-law-blog-india/ai-laws-and-regulations-in-india-as-of-2026>> accessed 13 September 2026.