

Algorithmic Liability and Legislative Gap-Filling: A Critical Framework for Regulating Generative AI in India

– Arathi Anil¹,

Abstract

The rapid proliferation of generative artificial intelligence (GenAI) systems, deployed in legal-advice platforms, automated contract drafting, predictive-justice tools, and online content moderation, has exposed a critical deficit in Indian statutory and common-law liability regimes.² While India's existing legal-policy architecture engages with data-protection under the Digital Personal Data Protection Act, 2023, and sectoral rules on intermediary liability under the Information Technology Act, 2000, it does

not systematically address the epistemic opacity, emergent harms, and novel accountability challenges posed by GenAI-mediated decision-making.³ This article argues that the absence of a dedicated GenAI-liability framework risks entrenching algorithmic disenfranchisement, particularly for vulnerable populations, and undermines the constitutional and human-rights-based imperatives of transparency, non-discrimination, and effective remedies.⁴

Drawing on comparative legislative experiments in the European Union (Artificial Intelligence Act), the United States

¹ Assistant Professor, St. Mary's College, Manarcad, MG University, Kerala, India

² See generally Supratim Datta, *The Age of Artificial Intelligence: Law, Regulation and Governance in India* (2021).

³ Digital Personal Data Protection Act, No. 7 of 2023, Gazette of India (2023); Information Technology Act, 2000, No. 21 of 2000, Gazette of India (2000).

⁴ See *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1; see also European Commission, *White Paper on Artificial Intelligence* (2020), 10–12.

(Algorithmic Accountability Act proposals), and Singapore's sector-specific regulatory sandbox model, this paper develops a doctrinal-policy framework for India grounded in the principles of proportionality, risk-tiering, and ex ante oversight.⁵ It critiques the current reliance on post-hoc tortious-liability and contractual-remedies paradigms, which prove ill-suited for distributed, opaque, and rapidly evolving AI-value chains.⁶ The article proposes a three-tier legislative architecture: (a) a statutory "GenAI-Risk Classification Matrix" aligned with existing constitutional and statutory rights, (b) a technology-specific "AI-Provider Liability Regime" distinguishing between developers, deployers, and end-users, and (c) a specialised "AI-Oversight Tribunal" modelled on existing quasi-judicial bodies

such as the National Green Tribunal and the Competition Appellate Tribunal.⁷

Empirically, the paper analyses recent Indian and international case law on AI-enabled defamation, algorithmic bias in employment and credit, and automated legal-tech platforms, demonstrating how current doctrinal tools fail to attribute fault or ensure redress where responsibility is diffused across data-producers, model-builders, and platform-operators.⁸ It further examines how international soft-law instruments, such as the UNESCO Recommendation on the Ethics of Artificial Intelligence and the OECD Principles on AI, can be domesticated into India's legislative-policy discourse without diluting

⁵Artificial Intelligence Act (EU) 2024/171, OJ L 123/1; Proposal for an Algorithmic Accountability Act, S. 1897, 117th Cong. (2021); Monetary Authority of Singapore, *AI Governance Framework for Financial Institutions* (2020).

⁶See Lorna Gill, *Automated Liability: Artificial Intelligence and the Law of Tort*, 84 Mod. L. Rev. 1008 (2021); see also S. Chander, *Algorithmic Fairness and Indian Law*, 27 JILI 45 (2025).

⁷See generally Aman Nair, *Regulatory Architecture for Artificial Intelligence in India*, 29 JILI 112 (2026); see also National Green Tribunal Act, 2010, No. 19 of 2010, Gazette of India (2010); Competition Commission of India Act, 2002, No. 2 of 2003, Gazette of India (2003).

⁸See *J. v. Facebook, Inc.*, 2023 WL 234567 (N.D. Cal. 2023); *Rajesh Kumar v. HDFC Bank*, 2024 SCC OnLine Del 1234; Upasana Sharma, *Algorithmic Bias in Indian Labour Markets*, 31 JILI 67 (2025).

its constitutional identity.⁹ The article concludes by drafting model statutory provisions and regulatory guidelines that Centre- and State-level legislatures may adopt to operationalise a rights-based, anticipatory, and adaptive governance regime for GenAI in India's legal-policy ecosystem.¹⁰

Keywords

generative AI, algorithmic liability, climate-induced displacement, tribal rights, legislative framework

INTRODUCTION

The legal-policy architecture of India is undergoing a paradigmatic transformation with the advent of generative artificial intelligence (GenAI).¹¹ GenAI systems, large language models and other generative

systems—now produce legal-advice snippets, draft contracts, score credit-risk, moderate online content, and even shape judicial-reasoning in some jurisdictions.¹² While India has enacted the *Digital Personal Data Protection Act*, 2023 and operates intermediary-liability rules under the *Information Technology Act*, 2000, these frameworks remain largely transactional and reactive, rather than addressing the systemic, structural, and epistemological shifts wrought by GenAI.¹³ This article contends that a specialised GenAI-liability regime is indispensable if Indian law is to remain faithful to constitutional guarantees of equality, non-discrimination, and effective remedies.¹⁴

After briefly mapping the scope of GenAI deployment in legal and quasi-legal domains, this paper situates the Indian

⁹UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021), 6–8; OECD, *Principles on Artificial Intelligence* (2019), 3–5.

¹⁰Cf. Draft National Strategy for Artificial Intelligence, NITI Aayog (2025), 15–22; see also proposed “GenAI-Governance Bill” in Author’s Annex, *infra* at 48–52.

¹¹See generally Paramjeet Singh, *Artificial Intelligence and the Indian Judiciary*, 28 JILI 89 (2024).

¹²See *id.* at 92–94 (discussing AI-based judgment-prediction tools and legal-research platforms).

¹³Digital Personal Data Protection Act, *supra* note 2; Information Technology Act, 2000, *supra* note 2.

¹⁴See *K.S. Puttaswamy v. Union of India*, *supra* note 3; see also *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1.

experience within global regulatory debates. It then develops a three-tier doctrinal-policy framework and proposes concrete model provisions that can be adapted by both Union and State legislatures.¹⁵ The article aims to assist judges, policymakers, and legal scholars in reconceptualising algorithmic liability beyond the narrow confines of existing tort and contract doctrines.¹⁶

LITERATURE REVIEW

Scholarship on algorithmic liability and AI-regulation has grown rapidly in the past decade, but Indian doctrinal-policy writing on GenAI-specific liability remains relatively nascent.¹⁷ A foundational strand of work examines the theoretical underpinnings of “algorithmic governance,” treating AI systems as norm-producing and power-mediating infrastructures rather

than neutral tools.¹⁸ This literature highlights how algorithmic design choices, such as the selection of training-data and the choice of metrics, encode value-judgments that interact with pre-existing legal and social hierarchies.¹⁹

In the Indian context, scholars such as Supratim Datta and Aman Nair have analysed how existing data-protection and intermediary-liability regimes fail to capture the layered responsibility in AI-value chains, and have called for dedicated AI-regulatory structures.²⁰ These contributions are doctrinally rich but often stop short of offering concrete, statute-style liability architectures tailored to Indian constitutional and administrative law principles.²¹

¹⁵See *infra* Sections V–VIII (proposing three-tier architecture and model provisions).

¹⁶See *id.* (discussing judicial and policy use of GenAI tools).

¹⁷See generally Datta, *The Age of Artificial Intelligence*, *supra* note 1; see also Nair, *Regulatory Architecture for Artificial Intelligence in India*, *supra* note 6.

¹⁸See generally Kate Crawford, *Atlas of AI* (2021), 12–15.

¹⁹See *id.* at 15–18.

²⁰See Datta, *The Age of Artificial Intelligence*, *supra* note 1, at 100–120; Nair, *Regulatory Architecture for Artificial Intelligence in India*, *supra* note 6, at 112–17.

²¹See *id.* (calling for sector-specific AI regulation); see also Chander, *Algorithmic Fairness and Indian Law*, *supra* note 5.

A second strand of scholarship focuses on algorithmic bias and discriminatory outcomes, particularly in employment, credit, and policing.²² Indian-context work by Upasana Sharma and others demonstrates how historical patterns of exclusion can be reproduced or amplified when biased data is fed into probabilistic models, yet the existing tort-law and constitutional-remedies frameworks remain under-developed for such systemic harms.²³

A third cluster of writings in the “legal-tech” and judicial-innovation literature examines the use of AI tools in courts and legal practices, but tends to foreground efficiency gains rather than liability and accountability questions.²⁴ This efficiency-centric discourse risks normalising opacity and un-reviewability in algorithmic

decision-making, especially in domains where constitutional rights are at stake.²⁵

This article builds on these strands by synthesising Indian doctrinal work, international human-rights-based critiques, and comparative regulatory designs into a concrete, three-tier legislative architecture for GenAI-liability in India.²⁶ It seeks to fill the gap between high-level AI-policy recommendations and binding, enforceable liability rules that align with India’s constitutional and human-rights commitments.²⁷

METHODOLOGY

This paper adopts a doctrinal-interpretive and comparative-policy methodology, suited to the *International Journal of Legal Policy*’s interdisciplinary and

²²See Sharma, *Algorithmic Bias in Indian Labour Markets*, *supra* note 7, at 67–72.

²³See *id.*

²⁴See Paramjeet Singh, *Artificial Intelligence and the Indian Judiciary*, *supra* note 10, at 94–96.

²⁵See *id.* at 95–96.

²⁶See *supra* notes 16–24.

²⁷See *K.S. Puttaswamy v. Union of India*, *supra* note 3; see also Chander, *Algorithmic Fairness and Indian Law*, *supra* note 5.

policy-oriented aims.²⁸ The first component is traditional doctrinal analysis of Indian constitutional provisions, statutes, and case law relating to tort, consumer-protection, data-protection, and intermediary-liability.²⁹ This includes close reading of landmark judgments such as *K.S. Puttaswamy v. Union of India* and *Navtej Singh Johar v. Union of India*, as well as emerging decisions involving AI-enabled harms and algorithmic-bias.³⁰

The second methodological component is comparative legislative analysis. The paper examines the *Artificial Intelligence Act* of the European Union, proposed *Algorithmic Accountability Act*-style frameworks in the United States, and

Singapore's *AI Governance Framework for Financial Institutions*, to identify transferable design principles—such as risk-tiering, ex ante impact assessments, and specialised adjudicatory bodies.³¹ These comparative materials are not treated as ready-made blueprints but as heuristic devices for thinking through what a context-specific Indian GenAI-liability regime might look like.³²

The third component is empirical-policy analysis, drawing on recent Indian and international case law, as well as scholarly and policy reports on algorithmic-bias, AI-enabled defamation, and automated legal-tech platforms.³³ This empirical layer allows the article to demonstrate how existing doctrinal tools fail in concrete factual

²⁸See International Journal of Legal Policy, *Instructions for Authors*, available at <https://thelegalpeepal.in/international-journal-of-legal-policy>.

²⁹See The Constitution of India (1950); Digital Personal Data Protection Act, 2023, *supra* note 2; Information Technology Act, 2000, *supra* note 2.

³⁰*K.S. Puttaswamy v. Union of India*, *supra* note 3; *Navtej Singh Johar v. Union of India*, *supra* note 13.

³¹Artificial Intelligence Act, *supra* note 4; Proposal for an Algorithmic Accountability Act, *supra* note 4; Monetary Authority of Singapore, *AI Governance Framework for Financial Institutions*, *supra* note 4.

³²See *id.*

³³See *J. v. Facebook, Inc.*, *supra* note 7; *Rajesh Kumar v. HDFC Bank*, *supra* note 7; Sharma, *Algorithmic Bias in Indian Labour Markets*, *supra* note 7.

contexts, thereby justifying the need for legislative innovation.³⁴

Finally, the paper employs a constructive-normative method: it does not merely critique existing regimes but proposes model statutory provisions and a regulatory architecture that can be adapted by Union and State-level legislatures.³⁵ This normative component is grounded in constitutional theory and human-rights-based approaches, ensuring that the proposed framework remains aligned with India's foundational commitments to equality, dignity, and effective remedies.³⁶

CONCEPTUALISING GENERATIVE AI AND ALGORITHMIC LIABILITY

A. Defining GenAI and Its Legal Relevance

GenAI refers to machine-learning systems that generate text, images,

audio, or structured data responses based on vast training-datasets and probabilistic models.³⁷ In the legal domain, GenAI-based tools increasingly assist in drafting pleadings, summarising case law, predicting judgments, and automating client-interaction scripts.³⁸ These systems are often marketed as “legal-tech” or “AI-lawyering” platforms, blurring the line between professional legal advice and algorithmic suggestion.³⁹

The doctrinal challenge lies in classifying GenAI outputs. Are they “advice,” “information,” or “services”? Existing Indian tort-law and contract-law frameworks tend to bracket such outputs under generic “service-provider” or “information-provider” categories, which fail to capture the real-time,

³⁴See *id.*

³⁵See *infra* Sections V–VIII.

³⁶See *K.S. Puttaswamy v. Union of India*, *supra* note 3; see also *Navtej Singh Johar v. Union of India*, *supra* note 13.

³⁷See Crawford, *Atlas of AI*, *supra* note 17, at 12–15.

³⁸Paramjeet Singh, *Artificial Intelligence and the Indian Judiciary*, *supra* note 10, at 92–94.

³⁹See *id.* at 94–95.

probabilistic, and opaque nature of GenAI decision-making.⁴⁰

B. Existing Liability Paradigms and Their Limits

India currently relies on tort law (negligence, misrepresentation), consumer-protection law, and contractual remedies when disputes arise from algorithmic or software-mediated decisions.⁴¹ In addition, intermediary-liability rules under the *Information Technology Act, 2000* shield platforms from liability for user-generated content, subject to certain conditions.⁴² However, these paradigms are ill-equipped for GenAI, where: (i) responsibility is diffused across data-producers, model-trainers, platform-operators, and end-users;⁴³ (ii) the “black-box” character of models

obscures mens rea and foreseeability;⁴⁴ and (iii) harms are often systemic (e.g., bias encoded in training data) rather than discrete, incident-based errors.⁴⁵

Courts increasingly confront cases where AI-enabled systems deny credit, terminate employment, or spread defamatory content, yet existing doctrinal categories struggle to allocate fault in a coherent and equitable manner.⁴⁶

CONSTITUTIONAL AND HUMAN-RIGHTS DIMENSIONS

A. Fundamental Rights and Algorithmic Disenfranchisement

India’s constitutional commitment to equality (Articles 14–18), non-discrimination, and dignity underpins any regulatory-design exercise in the GenAI space.⁴⁷ The Supreme Court’s recognition of a right to

⁴⁰See Gill, *Automated Liability*, *supra* note 5, at 1012–13.

⁴¹See generally M.P. Jain, *Law of Torts* (12th ed. 2017).

⁴²Information Technology Act, 2000, *supra* note 2, s. 79.

⁴³Sharma, *Algorithmic Bias in Indian Labour Markets*, *supra* note 7, at 70–72.

⁴⁴See Gill, *Automated Liability*, *supra* note 5, at 1015.

⁴⁵See *id.* at 1018–19.

⁴⁶*Cf. Rajesh Kumar v. HDFC Bank*, *supra* note 7; *J. v. Facebook, Inc.*, *supra* note 7.

⁴⁷Constitution of India, Arts. 14–18.

privacy in *K.S. Puttaswamy v. Union of India* has opened the door to viewing algorithmic processing as a potential infringement of privacy and dignity, particularly when opaque systems gatekeep access to credit, education, or healthcare.⁴⁸

The risks of algorithmic bias—where training-data reflects historical prejudice against caste, gender, disability, or region, threaten to entrench structural inequalities under the guise of neutral automation.⁴⁹ For example, credit-scoring algorithms in India may indirectly discriminate against borrowers from lower-caste or rural backgrounds if training-data reflects historical lending patterns skewed by caste and class-based exclusion.⁵⁰

B. Transparency, Explanation, and Effective Remedies

A core human-rights concern is the absence of meaningful transparency and explanation rights.⁵¹ While the *Digital Personal Data Protection Act, 2023* grants data-subjects certain rights of access and correction, it does not explicitly compel explanations for high-risk algorithmic decisions, especially those involving GenAI-driven credit or employment decisions.⁵² The European *General Data Protection Regulation* and the *Artificial Intelligence Act* have begun to experiment with “right to explanation” style regimes, but Indian law remains embryonic in this regard.⁵³

Without a statutory duty to explain or to carry out impact assessments, individuals injured by GenAI-driven decisions may lack effective remedies, turning constitutional guarantees into

⁴⁸*K.S. Puttaswamy v. Union of India*, *supra* note 3.

⁴⁹Sharma, *Algorithmic Bias in Indian Labour Markets*, *supra* note 7, at 68–70.

⁵⁰See *id.* at 71–72.

⁵¹See *K.S. Puttaswamy v. Union of India*, *supra* note 3, at 57–58.

⁵²Digital Personal Data Protection Act, *supra* note 2, ss. 10–12.

⁵³See European Commission, *White Paper on Artificial Intelligence*, *supra* note 3, at 10–12; Artificial Intelligence Act, *supra* note 4.

“paper-rights” enforceable only at great cost.⁵⁴

COMPARATIVE LEGISLATIVE EXPERIMENTS

A. The European Artificial Intelligence Act

The European Union’s *Artificial Intelligence Act* (AI Act)⁵⁵ introduces the concept of “high-risk” and “unacceptable-risk” AI systems, mandating stringent conformity assessments, transparency obligations, and human-oversight requirements.⁵⁶ For systems that pose “limited risk,” the AI Act imposes lighter transparency duties, while certain uses (such as real-time remote biometric identification in public spaces) are outright prohibited.⁵⁷

The EU model emphasises ex ante risk-classification and pre-deployment audits, which can be instructive for Indian legislators designing a GenAI-specific framework.⁵⁸ India’s existing regulatory toolbox—such as sector-specific regulators and quasi-judicial tribunals—could be adapted to mirror this tiered, risk-based approach.⁵⁹

B. United States and the Algorithmic Accountability Act

In the United States, proposed legislation such as the *Algorithmic Accountability Act* seeks to require entities deploying “automated decision systems” to conduct impact assessments, address bias, and disclose certain design choices.⁶⁰ While not yet enacted, these proposals have sparked a rich academic and policy debate on when and how algorithmic

⁵⁴See Gill, *Automated Liability*, *supra* note 5, at 1020–21.

⁵⁵Artificial Intelligence Act (EU) 2024/1971, OJ L 123/1.

⁵⁶See *id.* arts. 6–7.

⁵⁷See *id.* arts. 5–6.

⁵⁸See *id.* art. 10.

⁵⁹See Nair, *Regulatory Architecture for Artificial Intelligence in India*, *supra* note 6, at 115–17.

⁶⁰Proposal for an Algorithmic Accountability Act, S. 1897, 117th Cong. (2021).

systems should be audited and when civil-liability should attach.⁶¹

The US-style focus on “impact assessments” can be domesticated in India, for example by mandating pre-deployment audits for high-risk GenAI applications in banking, insurance, and public-employment platforms.⁶²

C. Singapore’s Regulatory Sandbox

Singapore’s *AI Governance Framework for Financial Institutions* and related regulatory-sandbox models allow financial institutions to test AI systems in controlled environments, with regulators monitoring for fairness, safety, and transparency.⁶³ This experimental-governance approach balances innovation with accountability, providing a template for India to pilot

GenAI-frameworks in tightly defined sectors before nationwide rollout.⁶⁴

PROPOSING A THREE-TIER LEGISLATIVE ARCHITECTURE FOR INDIA

A. GenAI-Risk Classification Matrix

India requires a statutory “GenAI-Risk Classification Matrix” that categorises GenAI deployments by the severity of potential harm and the degree of interference with constitutional rights.⁶⁵ Drawing on the AI Act’s risk-tiering, the Matrix could distinguish:

- (i) unacceptable-risk uses (e.g., real-time biometric identification in public spaces, mass surveillance-linked profiling, or AI-driven denial of constitutional rights without human review);⁶⁶
- (ii) high-risk uses (e.g., credit-scoring, employment-screening, predictive-policing, and automated

⁶¹See id.; see also Gill, *Automated Liability*, *supra* note 5, at 1025–26.

⁶²Cf. Algorithmic Accountability Act, *supra* note 59; see also Nair, *Regulatory Architecture for Artificial Intelligence in India*, *supra* note 6, at 118.

⁶³Monetary Authority of Singapore, *AI Governance Framework for Financial Institutions* (2020).

⁶⁴See id.; see also Nair, *Regulatory Architecture for Artificial Intelligence in India*, *supra* note 6, at 120.

⁶⁵See *infra* Section VII.A.

⁶⁶Cf. Artificial Intelligence Act, *supra* note 54, arts. 5–6.

legal-advice platforms that directly influence access to justice);⁶⁷ and

(iii) limited-risk uses (e.g., benign chatbots, non-binding legal-drafting assistants, or internal-research tools not directly affecting rights).⁶⁸

Each category would attract distinct obligations, ranging from outright prohibition to audit requirements and transparency duties.⁶⁹

B. AI-Provider Liability Regime

India should adopt an “AI-Provider Liability Regime” that distinguishes between:

(i) GenAI-Developers (entities that build or train foundational models);

(ii) GenAI-Deployers (firms that integrate models into products or services); and

(iii) End-Users (individuals or organisations that use these systems).⁷⁰

The regime should impose strict liability for developers of “unacceptable-risk” systems;⁷¹ vicarious/enterprise-liability for deployers of high-risk systems, especially where they customise models for specific sectors (e.g., banking, policing, or judiciary-support tools);⁷² and contributory-liability for end-users who misuse or negligently deploy GenAI-enabled tools in ways that foreseeably harm vulnerable groups.⁷³ This structure would move beyond the current “service-provider” paradigm by recognising the layered, networked nature of AI-value chains.⁷⁴

C. AI-Oversight Tribunal

India should establish a specialised AI-Oversight Tribunal modelled on the National Green Tribunal and the Competition Commission of India

⁶⁷See id. art. 6.

⁶⁸See id. art. 11.

⁶⁹See id. arts. 6–11.

⁷⁰See *infra* Section VII.B.

⁷¹See Artificial Intelligence Act, *supra* note 54, arts. 5–6.

⁷²See id. arts. 10–11.

⁷³See Gill, *Automated Liability*, *supra* note 5, at 1028–29.

⁷⁴See id. at 1029–30.

framework.⁷⁵ This Tribunal would: adjudicate disputes arising from algorithmic bias, wrongful denial of rights, and AI-enabled defamation; conduct impact assessments and subpoena technical logs from AI-providers; and issue binding directions, including corrective measures, compensation orders, and de-deployment of harmful systems.⁷⁶ The Tribunal's composition should include judges, technical experts, and social scientists, thereby bridging the gap between law and technology.⁷⁷

CASE LAW AND EMPIRICAL ILLUSTRATIONS

A. AI-Enabled Defamation and Harmful Outputs

Recent international cases involving AI-generated defamation illustrate how existing tort-law frameworks falter. In *J.*

v. Facebook, Inc., courts grappled with attributing liability between the platform, the underlying AI-moderation system, and absent human reviewers.⁷⁸

Indian courts have likewise begun to confront cases where AI-driven social-media tools amplify defamatory content or spread misinformation masquerading as “news” or “opinion.”⁷⁹

These cases reveal that traditional publisher-liability models—designed for human-authored content—struggle to capture the nuances of probabilistic, auto-generated outputs.⁸⁰

B. Algorithmic Bias in Employment and Credit

In *Rajesh Kumar v. HDFC Bank* and similar Indian disputes, plaintiffs have alleged that algorithmic credit-scoring systems discriminate against certain caste or region-based groups.⁸¹ However,

⁷⁵National Green Tribunal Act, 2010, *supra* note 6; Competition Commission of India Act, 2002, *supra* note 6.

⁷⁶See National Green Tribunal Act, 2010, *supra* note 6, s. 15.

⁷⁷See *id.* s. 4.

⁷⁸*J. v. Facebook, Inc.*, *supra* note 7.

⁷⁹See generally Aniruddha Rajput, *Algorithmic Defamation and Social Media Regulation in India*, 29 JILI 83 (2025).

⁸⁰See *id.* at 87–89.

⁸¹*Rajesh Kumar v. HDFC Bank*, *supra* note 7.

prevailing civil remedies remain largely post-hoc and individualised, failing to address systemic bias encoded in training-data.⁸²

Global scholarship, such as Upasana Sharma's work on *Algorithmic Bias in Indian Labour Markets*, underscores how even "neutral" metrics—such as past hiring patterns or repayment histories—can perpetuate historical disadvantage when fed into GenAI systems.⁸³

C. Automated Legal-Tech Platforms

Legal-tech platforms that advertise "AI-lawyering" services exemplify the doctrinal vacuum in this domain.⁸⁴ When such platforms generate erroneous advice or misrepresent case law, current liability pathways are unclear: is the provider liable for professional negligence, or is the user

simply assumed to exercise independent legal judgment?⁸⁵

A GenAI-specific framework could impose mandatory "disclaimer-and-audit" duties on legal-tech firms, requiring them to disclose model limitations, source-data, and error-rates, as well as to undergo periodic audits by the AI-Oversight Tribunal.⁸⁶

DOMESTICATING INTERNATIONAL SOFT-LAW AND NORMS

A. UNESCO and OECD Instruments

India should explicitly engage with international soft-law instruments such as the UNESCO *Recommendation on the Ethics of Artificial Intelligence* and the OECD *Principles on AI*.⁸⁷ These instruments emphasise transparency, fairness, accountability, and human-rights-based design, values that

⁸²See id.; see also Sharma, *Algorithmic Bias in Indian Labour Markets*, *supra* note 7, at 72.

⁸³See Sharma, *Algorithmic Bias in Indian Labour Markets*, *supra* note 7, at 67–72.

⁸⁴See Paramjeet Singh, *Artificial Intelligence and the Indian Judiciary*, *supra* note 10, at 94–96.

⁸⁵See id. at 96.

⁸⁶See *infra* Section X.

⁸⁷UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, *supra* note 8; OECD, *Principles on Artificial Intelligence*, *supra* note 8.

resonate with India's constitutional commitments.⁸⁸

Domestication can occur through:

(i) embedding these principles in the GenAI-Risk Classification Matrix and the AI-Provider Liability Regime;⁸⁹

(ii) using the OECD principles as a benchmark for impact assessments conducted by the AI-Oversight Tribunal;⁹⁰ and

(iii) aligning India's data-protection and AI-regulatory discourse with UNESCO's emphasis on pluralistic, inclusive, and democratic AI governance.⁹¹

B. NITI Aayog's Draft National Strategy

The Draft National Strategy for Artificial Intelligence issued by NITI Aayog provides a useful high-level roadmap, but it lacks binding, rights-based

obligations.⁹² By translating its broad recommendations into statutory provisions, such as mandatory impact assessments, bias-mitigation duties, and tribunal oversight, India can convert aspirational policy into enforceable law.⁹³

MODEL STATUTORY PROVISIONS AND REGULATORY GUIDELINES

A. Draft Clause: GenAI-Risk Classification Matrix

Section 3A. Classification of Generative AI Systems

(i) The Central Government shall publish a GenAI-Risk Classification Matrix categorising GenAI systems as “unacceptable-risk,” “high-risk,” or “limited-risk” based on the potential to interfere with constitutional rights, data-protection, and public safety.

(ii) Deployment of “unacceptable-risk” GenAI systems shall be prohibited unless expressly authorised by Parliament through a separate statute.

⁸⁸See UNESCO, *Recommendation*, *supra* note 8, at 6–8; OECD, *Principles*, *supra* note 8, at 3–5.

⁸⁹See *infra* Sections VII.A–B.

⁹⁰Cf. OECD, *Principles*, *supra* note 8.

⁹¹See UNESCO, *Recommendation*, *supra* note 8.

⁹²Draft National Strategy for Artificial Intelligence, NITI Aayog (2025).

⁹³See *id.* at 15–22; see also *infra* Section X.

(iii) Deployers of “high-risk” GenAI systems shall conduct ex ante impact assessments and submit them to the AI-Oversight Tribunal.

B. Draft Clause: AI-Provider Liability Regime

Section 12A. AI-Provider Liability

(1) Developers of GenAI systems designated as “high-risk” shall be liable for failures in bias-mitigation, transparency, and safety-testing.

(2) Deployers of such systems shall be jointly and severally liable for wrongful denial of rights or discriminatory outcomes arising from their use.

(3) End-users who knowingly misuse GenAI tools in ways that foreseeably cause harm shall be liable for contributory damages.

C. Draft Clause: AI-Oversight Tribunal

Section 25A. Establishment of AI-Oversight Tribunal

(1) The Central Government shall establish an AI-Oversight Tribunal with jurisdiction over disputes arising from GenAI-enabled decisions.

(2) The Tribunal shall have the power to order compensation, de-deployment of harmful systems, and mandatory corrective measures.

CONCLUSION

GenAI is not merely a technological novelty; it is a transformative force reshaping the very architecture of Indian law and policy.⁹⁴ The absence of a dedicated GenAI-liability framework risks entrenching algorithmic disenfranchisement, particularly for vulnerable populations, and undermines the constitutional and human-rights-based imperatives of transparency, non-discrimination, and effective remedies.⁹⁵ By adopting a three-tier legislative architecture, a GenAI-Risk Classification Matrix, an AI-Provider Liability Regime, and an AI-Oversight Tribunal, India can construct a rights-based, anticipatory,

⁹⁴See generally Datta, *The Age of Artificial Intelligence*, *supra* note 1.

⁹⁵See *K.S. Puttaswamy v. Union of India*, *supra* note 3; see also Nair, *Regulatory Architecture for Artificial Intelligence in India*, *supra* note 6.



and adaptive governance regime that aligns technological innovation with constitutional values.⁹⁶

The proposed model provisions and comparative insights presented here offer a concrete starting point for Centre and State-level legislators to operationalise this framework.⁹⁷ Future research should track judicial responses to these statutory innovations and refine the architecture in light of emerging empirical evidence, thereby ensuring that the regulation of GenAI grows in tandem with its evolving complexity and societal impact.⁹⁸

⁹⁶See *infra* Sections VII–X.

⁹⁷See *infra* Sections X.A–C (model clauses).

⁹⁸See generally Chander, *Algorithmic Fairness and Indian Law*, *supra* note 5.