PANJAB UNIVERSITY LAW REVIEW
ISSN: 0971-5541, Volume 64, Part 2, pp. 108-125

NEED FOR A COMPREHENSIVE ARTIFICIAL INTELLIGENCE LEGISLATION IN INDIA: A COMPARATIVE LEGAL ANALYSIS WITH THE EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT

Dr. Jaspreet Kaur Majithia[*]
Shubham Bhatia[**]

ABSTRACT

Artificial intelligence has moved from the margins of Indian public administration to its operational core, informing credit decisions, welfare eligibility, predictive policing and content moderation, yet India continues to regulate it through instruments never designed for autonomous, self-learning systems. This paper examines whether India's existing legal architecture, principally the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, supplemented by non-binding instruments such as the NITI Aayog's National Strategy for Artificial Intelligence and the 2025 India AI Governance Guidelines, is adequate to address algorithmic opacity, automated discrimination and the absence of institutional accountability. It compares this fragmented domestic position with the European Union's Artificial Intelligence Act, Regulation (EU) 2024/1689, the first horizontal, risk-tiered AI statute in the world, which classifies systems as prohibited, high-risk, limited-risk or minimal-risk and attaches graduated obligations, conformity assessments and enforceable penalties to each tier. Employing doctrinal and comparative legal methodology, the paper reads Indian constitutional jurisprudence, particularly Justice K.S. Puttaswamy v. Union of India and Anuradha Bhasin v. Union of India, alongside the EU framework to argue that Articles 14, 19 and 21 of the Constitution already supply the normative foundation for a rights-anchored AI statute. It concludes that India should not transplant the EU Act wholesale but should adapt its risk-based methodology to a dedicated legislation calibrated to India's federal structure, institutional capacity and constitutional guarantees, and it proposes a concrete legislative architecture to that end.

KEYWORDS: *Artificial Intelligence Regulation; Algorithmic Accountability; Comparative Constitutional Law; Data Protection; Risk-Based Governance*

1. INTRODUCTION

Artificial intelligence in India has migrated, within less than a decade, from experimental deployment to structural embeddedness in governance, finance and public service delivery. The National Crime Records Bureau's Automated Facial Recognition System is now operational across multiple state police forces, algorithmic credit scoring increasingly shapes access to formal finance, and automated tools mediate welfare eligibility determinations under public distribution and social security schemes with minimal human review of individual outcomes.[1] India is, by its own government's account, among the largest markets globally for the deployment of large language models and generative AI tools, a scale of adoption that has outpaced the legislative

[*] Associate Professor & Dean, Faculty of Law Amity University Punjab, Mohali.
[**] Advocate, Punjab and Haryana High Court.

[1] Ameen Jauhar, Facing up to the Risks of Automated Facial-Recognition Technologies in Indian Law Enforcement, 16 Ind. J.L. & Tech. 1 (2020).

attention devoted to the risks such adoption carries. This expansion has occurred without a legislative instrument that speaks directly to the distinctive risks that autonomous, adaptive systems present, namely the difficulty of contesting a decision whose reasoning is neither disclosed nor, in many cases, fully knowable even to its developer. India regulates AI, to the extent it regulates AI at all, through statutes drafted for other purposes. The Information Technology Act, 2000 imposes a duty on body corporates handling sensitive personal data to maintain reasonable security practices, and fixes civil liability under Section 43A where such practices are absent.[2] The Digital Personal Data Protection Act, 2023 establishes a consent-based data fiduciary framework and creates the Data Protection Board of India under Chapter V to adjudicate complaints of data misuse.[3] Neither statute was conceived with algorithmic decision-making in mind, and neither imposes obligations of algorithmic transparency, bias auditing or human oversight.

The consequence is a persistent and consequential regulatory vacuum. Matters central to the responsible governance of AI, including algorithmic opacity, automated decision-making without a right to explanation, systemic bias in training data, and the allocation of legal responsibility when an autonomous system causes harm, find no clear statutory answer in India today. This vacuum is not merely theoretical. Where AI is deployed in policing, welfare distribution or credit underwriting, the absence of a legal standard for explainability or redress converts a technical limitation into a constitutional harm. India does possess soft guidance, including the Reserve Bank of India's Guidelines on Outsourcing of Information Technology Services, 2020, the NITI Aayog's National Strategy for Artificial Intelligence (2018), and, more recently, the Ministry of Electronics and Information Technology's India AI Governance Guidelines of November 2025 and the RBI's Framework for Responsible and Ethical Enablement of Artificial Intelligence of August 2025.[4] Each of these instruments is valuable as policy orientation, yet none carries the force of law, none creates justiciable rights, and none can impose a penalty for non-compliance.

The European Union offers a contrasting model. The Artificial Intelligence Act, Regulation (EU) 2024/1689, in force since August 2024 with phased applicability through 2027, is the first comprehensive, horizontally applicable AI statute anywhere in the world.[5] It classifies AI systems by the risk they pose

---

2 The Information Technology Act, No. 21 of 2000, § 43A (India).

3 The Digital Personal Data Protection Act, No. 22 of 2023, ch. V (India).

4 NITI Aayog, National Strategy for Artificial Intelligence #AIforAll (2018); Reserve Bank of India, Framework for Responsible and Ethical Enablement of Artificial Intelligence (Aug. 13, 2025); Ministry of Electronics & Information Technology, India AI Governance Guidelines (Nov. 5, 2025).

5 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act), art. 113, 2024 O.J. (L 1689) [hereinafter EU AI Act].

to health, safety and fundamental rights, prohibits an enumerated set of practices outright, and subjects high-risk systems to conformity assessment, data governance and human oversight obligations enforceable through administrative fines of up to seven per cent of global turnover.[6] The Indian Supreme Court's recognition, in Justice K.S. Puttaswamy v. Union of India, that privacy is an intrinsic facet of Article 21, supplies India with a constitutional predicate for comparable protections, yet nine years after that judgment no legislative or judicial mechanism exists to render AI decision-making transparent or contestable.[7]

The stakes of this gap are not speculative. Automated facial recognition deployed at protests or public gatherings implicates the right to anonymity that this Court has recognised as a facet of associational freedom; algorithmic welfare eligibility tools that silently exclude beneficiaries on the basis of imperfect data implicate the right to livelihood under Article 21; and predictive policing tools trained on historical arrest data risk entrenching precisely the discriminatory patterns that Article 14 exists to dismantle. None of these risks is addressed by a statute conceived, as the Information Technology Act was, to regulate electronic commerce and cybercrime at the turn of the millennium.

This paper argues that India's current patchwork of general-purpose statutes and voluntary guidelines cannot discharge the constitutional obligations that Puttaswamy and its progeny impose once AI systems mediate the exercise of fundamental rights. It further argues that the EU AI Act, while not directly transplantable given India's different federal structure, institutional capacity and rights architecture, supplies a workable regulatory template, namely risk-tiered classification, mandatory conformity assessment and independent institutional oversight, that India should adapt rather than ignore. The paper closes by proposing the architecture of a dedicated Indian AI statute built on this adapted template.

1.1. Objectives of the Study

1. To examine the current legal status of artificial intelligence regulation in India, including binding statutes and non-binding policy instruments.

2. To assess the structure, rationale and adaptability of the European Union Artificial Intelligence Act to Indian constitutional and institutional conditions.

3. To propose a rights-preserving, risk-calibrated legislative framework suited to India's federal and constitutional realities.

---

6 EU AI Act, supra note 5, arts. 5, 6, 99.

7 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

1.2. Research Methodology

This paper adopts a doctrinal and comparative methodology. It examines the text of Indian legislation bearing on AI, principally the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, alongside the relevant constitutional provisions, namely Articles 14, 19 and 21. It then examines the text of the European Union Artificial Intelligence Act, Regulation (EU) 2024/1689, and the Charter of Fundamental Rights of the European Union. The comparative method is used to identify structural divergences between the two regimes and to test whether elements of the EU framework are transplantable into Indian law without disturbing India's constitutional and federal design. The paper draws upon judicial precedent, official government reports, and peer-reviewed academic literature to substantiate its analysis.

2. ARTIFICIAL INTELLIGENCE AND THE INDIAN LEGAL FRAMEWORK

India has no statute that defines "artificial intelligence," "automated decision-making" or "algorithmic system." What exists instead is a patchwork of general-purpose instruments, each addressing a fragment of the problem while leaving the whole unaddressed. The Information Technology Act, 2000 remains the principal statute governing digital conduct. Section 43A fixes civil liability on a body corporate that fails to implement and maintain reasonable security practices while possessing, dealing with or handling sensitive personal data, where such failure causes wrongful loss or wrongful gain.[8] Section 72A separately criminalises the disclosure of personal information obtained under a lawful contract, without consent and with intent to cause wrongful loss.[9] Neither provision contemplates algorithmic design review, third-party auditing of AI models, or liability for harm caused by an automated decision that was never disclosed as automated.

The Digital Personal Data Protection Act, 2023 represents a more contemporary intervention but remains oriented toward personal data processing rather than algorithmic governance as such. Section 2(t) defines personal data, and Chapter II imposes obligations on data fiduciaries, including purpose limitation and a requirement of free, specific and informed consent before processing.[10] Chapter V establishes the Data Protection Board of India, empowered to inquire into complaints and impose penalties of up to two hundred and fifty crore rupees for significant non-compliance.[11] Yet the Act does not mandate an algorithmic impact assessment, does not require that automated decisions be explained to the persons they affect, and does not

---

8 The Information Technology Act, No. 21 of 2000, § 43A (India).
9 The Information Technology Act, No. 21 of 2000, § 72A (India).
10 The Digital Personal Data Protection Act, No. 22 of 2023, §§ 2(t), ch. II (India).
11 The Digital Personal Data Protection Act, No. 22 of 2023, ch. V & sch. (India).

classify AI systems by the severity of risk they pose, a gap that becomes acute once one recalls that the Act governs the data an algorithm consumes but not the decision the algorithm produces. The Act's exemptions compound the difficulty: Section 17 permits processing for purposes including research, archiving and certain state functions without the full consent architecture otherwise required, and the broad state-function exemption has drawn criticism for potentially permitting government deployment of AI-based surveillance or welfare-screening tools with reduced procedural safeguards precisely in the contexts, policing and welfare administration, where algorithmic error is most consequential.[12] Separately, Section 79 of the Information Technology Act grants intermediaries conditional safe harbour from liability for third-party content, a provision increasingly strained by AI systems that do not merely host content but actively generate, rank or recommend it, functions the safe-harbour architecture was never designed to address.

Sectoral and policy instruments fill some of this space, though none possesses statutory force. The Reserve Bank of India's Guidelines on Outsourcing of Information Technology Services, 2020 require regulated entities to conduct risk assessments and maintain oversight of technology vendors, including AI-based service providers, but create no independent cause of action for an affected borrower.[13] The NITI Aayog's National Strategy for Artificial Intelligence, 2018 articulates an "AI for All" vision and identifies ethics as a design principle, but is expressly aspirational.[14] Most significantly, the Ministry of Electronics and Information Technology released the India AI Governance Guidelines in November 2025, built on seven guiding principles it calls "sutras," including accountability, fairness and equity, and "understandable by design."[15] These Guidelines are notable for what they deliberately decline to do: rather than recommending a standalone AI statute, they adopt what their drafting committee describes as a "light-touch," principle-based approach that relies on existing laws such as the Information Technology Act and the Digital Personal Data Protection Act to govern AI-related harms.[16] The Reserve Bank of India's own sector-specific Framework for Responsible and Ethical Enablement of Artificial Intelligence, published in August 2025, adopts a parallel approach for the financial sector, recommending board-approved AI policies, AI system inventories and incident reporting, again without statutory

---

12 The Digital Personal Data Protection Act, No. 22 of 2023, § 17 (India); The Information Technology Act, No. 21 of 2000, § 79 (India).

13 Reserve Bank of India, Guidelines on Outsourcing of Information Technology Services (2020).

14 NITI Aayog, National Strategy for Artificial Intelligence #AIforAll (2018).

15 Ministry of Electronics & Information Technology, India AI Governance Guidelines pt. 1 (Nov. 5, 2025).

16 Id. pt. 3 (Policy & Regulation pillar).

backing.[17] The cumulative effect of these instruments is instructive: even India's most recent and most considered AI policy response reaffirms voluntary, sector-specific governance over binding, rights-based regulation, leaving the legislative gap identified above fully intact three years after the Digital Personal Data Protection Act itself was enacted.

Table 1: Instruments Governing Artificial Intelligence in India

Instrument	Legal Status	Key Provisions	Principal Limitation
Information Technology Act, 2000	Binding statute	S. 43A: liability for failure to secure sensitive personal data; S. 72A: penalty for unauthorised disclosure	No provision on algorithmic transparency, audit or risk classification
Digital Personal Data Protection Act, 2023	Binding statute	S. 2(t): definition of personal data; Ch. II: fiduciary obligations; Ch. V: Data Protection Board, penalties up to Rs. 250 crore	No mandate for automated decision-making review or explainability
RBI Outsourcing Guidelines, 2020	Regulatory guideline	Risk-based vendor oversight for regulated entities	Voluntary; no independent grievance mechanism
NITI Aayog National AI Strategy, 2018	Policy document	Sectoral roadmap; ethical principles for AI adoption	Non-binding; aspirational only
India AI Governance Guidelines, 2025	Policy document	Seven "sutras"; institutional coordination via an AI Governance Group	Explicitly declines a standalone statute; not enforceable
RBI FREE-AI Framework, 2025	Sector guideline	Board-approved AI policy, AI inventories, incident reporting for regulated financial entities	Sector-limited; no statutory penalty structure

[17] Reserve Bank of India, Framework for Responsible and Ethical Enablement of Artificial Intelligence (Aug. 13, 2025).

3. CONSTITUTIONAL AND JUDICIAL FOUNDATIONS FOR AI REGULATION

Although Parliament has not legislated specifically for artificial intelligence, the Supreme Court has already supplied much of the constitutional vocabulary such a statute would need to speak. In Justice K.S. Puttaswamy v. Union of India, a nine-judge bench unanimously held that the right to privacy is intrinsic to the right to life and personal liberty under Article 21 and is further reflected in the freedoms guaranteed by Article 19.[18] The Court articulated a three-fold test for any state action that infringes privacy, requiring legality, a legitimate state aim, and proportionality between the means adopted and the object sought.[19] Applied to AI, this test supplies a ready-made constitutional standard against which automated surveillance, predictive policing and biometric identification systems can and should be tested, yet no legislation currently operationalises that test for algorithmic contexts.

In Anuradha Bhasin v. Union of India, the Court extended this proportionality logic to digital restrictions, holding that any suspension of internet access, and by extension any technologically mediated restriction on speech or access, must be backed by law, must pursue a legitimate aim, and must be the least restrictive means available.[20] The judgment is directly relevant to AI-enabled content moderation and surveillance tools, because it establishes that algorithmic decisions with the practical effect of restricting Article 19(1)(a) freedoms cannot rest on executive discretion alone but require clear statutory authorisation and procedural safeguards. Similarly, in Shreya Singhal v. Union of India, the Court struck down Section 66A of the Information Technology Act for vagueness and overbreadth, and read down the intermediary safe-harbour provision in Section 79 to require actual knowledge through a court or government order before content could be taken down.[21] The case's insistence on precision and procedural fairness in speech-restricting rules translates directly into a demand for precision in any future statute authorising automated content moderation or takedown by AI systems.

A further doctrinal resource lies in Internet and Mobile Association of India v. Reserve Bank of India, where the Court struck down a blanket RBI circular restricting banking services to virtual currency businesses on the ground that it failed the proportionality test, since the RBI could not demonstrate empirical harm or show that less restrictive alternatives had been considered.[22] The reasoning is transferable to algorithmic credit-scoring and welfare-eligibility

---

18 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (per Chandrachud, J.).

19 Id.

20 Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637.

21 Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1.

22 Internet & Mobile Ass'n of India v. Reserve Bank of India, (2020) 10 S.C.C. 274.

systems: a regulator or private actor that denies a person access to a service through an opaque automated process, without demonstrating necessity or considering less restrictive alternatives, would similarly fail constitutional scrutiny if the matter reached a court. The proportionality standard was applied specifically to a large-scale biometric identification system in Justice K.S. Puttaswamy v. Union of India (Aadhaar), where a five-judge bench upheld the Aadhaar scheme's core architecture while nonetheless reading down provisions permitting private-sector access to the biometric database, holding that the state's own algorithmic identification infrastructure had to be confined to purposes demonstrably necessary and could not be extended to private commercial use without separate justification.[23] The judgment is the closest India's jurisprudence has come to adjudicating an AI-adjacent system directly, and its insistence on purpose limitation even within an otherwise constitutionally valid biometric programme illustrates precisely the kind of scope discipline that a statutory risk classification would codify prospectively rather than leave to case-by-case litigation.

Read together, Puttaswamy, the Aadhaar judgment, Anuradha Bhasin, Shreya Singhal and Internet and Mobile Association of India establish that Indian constitutional law already contains the substantive standards, legality, necessity and proportionality, that a comprehensive AI statute would need to codify. What is missing is not constitutional theory but legislative machinery capable of applying that theory before harm occurs rather than after a writ petition succeeds.

4. THE EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT: STRUCTURE AND RATIONALE

The European Union Artificial Intelligence Act is the first horizontally applicable AI statute in the world, binding across all member states and applying extraterritorially wherever an AI system's output is used within the Union.[24] Its stated purpose is to ensure a high level of protection for health, safety and fundamental rights, including democracy and the rule of law, while supporting innovation, and it operates in consonance with the General Data Protection Regulation, Regulation (EU) 2016/679, which continues to govern the personal data that AI systems process.[25] The Act is textually anchored in the Charter of Fundamental Rights of the European Union, drawing in particular on the right to human dignity under Article 1, the right to privacy and data

---

23 Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J.), (2019) 1 S.C.C. 1.

24 EU AI Act, supra note 5, art. 2.

25 Id. art. 1; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

protection under Article 7, and the right to non-discrimination under Article 21 of the Charter.[26]

4.1 Risk-Based Classification

The Act's defining structural feature is a tiered risk classification of AI systems. Article 5 prohibits outright a defined set of practices considered to carry unacceptable risk, including AI systems that deploy manipulative or subliminal techniques to distort behaviour, that conduct social scoring of individuals by public authorities, and that perform real-time remote biometric identification in publicly accessible spaces for law enforcement purposes, subject to narrow exceptions.[27] Article 6, read with Annex III, classifies as high-risk those systems used in critical infrastructure, education, employment, essential private and public services including credit scoring, law enforcement, migration control and the administration of justice.[28] Limited-risk systems, principally those that interact directly with natural persons such as chatbots, or that generate synthetic content, are subject to the transparency obligations of Article 50, which require that users be informed they are interacting with an AI system and that AI-generated or manipulated content, including deepfakes, be clearly labelled.[29] Systems presenting minimal risk remain largely unregulated, subject only to voluntary codes of conduct. The Act additionally regulates general-purpose AI models as a distinct category under Chapter V, requiring providers to maintain technical documentation and a policy for compliance with copyright law, with enhanced obligations, including systemic-risk evaluation and incident reporting, for models deemed to carry systemic risk on the basis of the computational resources used in their training.[30] Article 4 further imposes a horizontal obligation on providers and deployers to ensure a sufficient level of AI literacy among their staff and other persons dealing with AI systems, an obligation that applies irrespective of the risk tier of the system involved and reflects the Act's recognition that institutional competence, not merely legal obligation, determines whether a risk-based framework functions in practice.[31]

4.2 Obligations and Enforcement

Providers of high-risk AI systems bear the heaviest compliance burden. Article 9 requires a continuous risk management system spanning the system's lifecycle. Article 10 mandates that training, validation and testing data be relevant, representative and, to the extent possible, free of errors that could produce discriminatory outcomes.[32] Article 11 requires technical documentation

---

26 Charter of Fundamental Rights of the European Union, arts. 1, 7, 21, 2000 O.J. (C 364) 1.
27 EU AI Act, supra note 5, art. 5.
28 Id. art. 6, annex III.
29 Id. art. 50.
30 Id. ch. V, arts. 51-56.
31 Id. art. 4.
32 Id. arts. 9, 10.

sufficient to demonstrate compliance, and Article 14 requires that high-risk systems be designed to allow effective human oversight, including the ability of a natural person to intervene in or halt the system's operation.[33] Before such a system may be placed on the market, Article 43 requires a conformity assessment, self-administered or, for certain categories, conducted by an independent notified body.[34] Enforcement is entrusted to national market surveillance authorities operating under the coordination of the European Artificial Intelligence Board, with Article 99 empowering fines of up to thirty-five million euros or seven per cent of an undertaking's total worldwide annual turnover, whichever is higher, for violations of the Article 5 prohibitions, and correspondingly graduated fines for lesser violations.[35] As of mid-2026, the prohibitions under Article 5 and the obligations applicable to general-purpose AI models are already in force, while the compliance deadline for high-risk systems under Annex III, initially set for August 2026, has been the subject of a proposed deferral under the Commission's Digital Omnibus initiative, illustrating that even a comprehensive statute of this kind requires ongoing calibration as implementation proceeds.[36] This iterative character is itself instructive for India: a risk-based statute need not be static at enactment to be worth enacting, provided its institutional architecture is capable of absorbing amendment through delegated rule-making rather than repeated primary legislation.

5. COMPARATIVE LEGAL ANALYSIS: INDIA AND THE EUROPEAN UNION

Placed side by side, the Indian and European positions diverge along four axes that matter most for the protection of individual rights. The first is classificatory. The EU Act sorts every AI system into one of four risk tiers before any obligation attaches, which allows regulatory intensity to track actual risk rather than sector or technology. Indian law contains no equivalent sorting mechanism; the DPDP Act applies uniformly to all processing of personal data regardless of whether that data feeds a low-stakes recommendation engine or a high-stakes parole-risk algorithm.[37] The second axis is institutional. The EU Act creates the European Artificial Intelligence Board for Union-level coordination and requires each member state to designate a national supervisory authority empowered to conduct market surveillance and impose fines.[38] India has no equivalent centralised body; oversight is dispersed across the Ministry of

---

33 Id. arts. 11, 14.
34 Id. art. 43.
35 Id. art. 99.
36 European Commission, Digital Omnibus on Artificial Intelligence (proposal, May 2026); see also Article 99: Penalties, EU Artificial Intelligence Act (artificialintelligenceact.eu).
37 The Digital Personal Data Protection Act, No. 22 of 2023 (India).
38 EU AI Act, supra note 5, arts. 64-70.

Electronics and Information Technology, the Data Protection Board established under the DPDP Act, and sectoral regulators such as the RBI, each competent only within its own domain and none possessing AI-specific investigative powers.

Table 2: Comparative Position of India and the European Union on AI Regulation

Aspect	India	European Union (AI Act)
Legal foundation	Fragmented: IT Act, 2000; DPDP Act, 2023; non-binding sectoral guidelines and the 2025 Governance Guidelines	Unified, binding statute: Regulation (EU) 2024/1689
Risk classification	Absent; uniform application of data protection rules irrespective of AI risk	Four-tier structure: prohibited (Art. 5), high-risk (Art. 6, Annex III), limited-risk (Art. 50), minimal-risk
Regulatory authority	Dispersed across MeitY, Data Protection Board and sectoral regulators; no AI-specific body	European Artificial Intelligence Board with national supervisory authorities in each member state
Conformity assessment	No statutory requirement; voluntary vendor audits in some sectors	Mandatory for high-risk systems under Art. 43, with technical documentation under Art. 11
Transparency obligations	No statutory duty to disclose AI-mediated decisions	Art. 50: mandatory disclosure of AI interaction and labelling of synthetic content
Human oversight	No express statutory requirement	Art. 14: high-risk systems must permit effective human intervention
Enforcement and penalties	DPDP Act fines up to Rs. 250 crore for data violations only; no AI-specific penalty	Art. 99: fines up to EUR 35 million or 7% of global turnover, tiered to severity of breach
Right to explanation	Not recognised in statute	Implicit in Arts. 13, 14 and 50 read with the Charter

The third axis is transparency. Article 50 of the EU Act imposes a freestanding obligation to disclose AI interaction, and Article 14 requires human oversight of high-risk systems as a matter of design, not merely of good

practice.[39] Indian law imposes no comparable disclosure duty; a person denied a loan, flagged by a predictive policing tool, or subject to an automated welfare determination has no statutory right to be told that a machine made or materially contributed to that decision, still less a right to an explanation of the factors the machine weighed. The fourth axis is enforcement severity and certainty. The EU's tiered fines under Article 99, reaching seven per cent of global turnover for the most serious violations, create a deterrent calibrated to the size of the offending enterprise.[40] India's penalties under the DPDP Act, while substantial in absolute terms at up to two hundred and fifty crore rupees, apply only to data protection violations and offer no separate penalty structure for algorithmic harms that do not involve a data breach as conventionally understood, such as a facially neutral algorithm that nonetheless produces discriminatory outcomes through proxy variables.

The comparison should not be read as a simple verdict of Indian deficiency against European sufficiency; the EU Act itself remains under active revision, as the Digital Omnibus deferral shows, and its heavy conformity-assessment burden has drawn criticism for disadvantaging smaller developers.[41] The comparison instead demonstrates that India lacks even the foundational architecture, risk classification, a designated authority, a transparency duty and calibrated penalties, on which such debates about calibration can occur. India cannot debate whether its AI statute is too strict or too lenient because it has not yet enacted one.

6. WHY INDIA NEEDS A COMPREHENSIVE AI STATUTE: A CRITICAL ASSESSMENT

Three interlocking arguments support the case for a dedicated Indian AI statute rather than continued reliance on adapted data protection and cybersecurity law. First, the harms that concern AI-specific regulation are analytically distinct from the harms that data protection law addresses. The DPDP Act protects the data an algorithm consumes; it does not and structurally cannot regulate the inference the algorithm draws from lawfully collected data, nor the discriminatory pattern that emerges when a facially neutral model is trained on historically biased data.[42] A credit-scoring algorithm may comply fully with consent and purpose-limitation requirements while still systematically disadvantaging applicants from particular postal codes or occupational categories, a harm no provision of the DPDP Act or the IT Act is equipped to detect, let alone remedy. The same is true of predictive policing tools of the

---

39 Id. arts. 14, 50.

40 Id. art. 99.

41 Sangchul Park, Bridging the Global Divide in AI Regulation: A Proposal for a Contextual, Coherent, and Commensurable Framework, 33(2) Harv. J.L. & Tech. 216, 239 (2024).

42 Graham Greenleaf, Promises and Illusions of Data Protection in Indian Law, 1 Int'l Data Priv. L. 47 (2010).

kind several state police forces have piloted, which are typically trained on historical crime and arrest data; where that data reflects a history of disproportionate policing of particular communities, the resulting model reproduces and formalises that disproportion under the appearance of statistical neutrality, a harm that consent-based data protection law, focused as it is on the collection stage rather than the inferential stage, structurally cannot reach.

Second, the EU AI Act demonstrates that a workable, judicially administrable middle path exists between prohibition and laissez-faire. Its risk-tiered design shows that a legislature can distinguish AI uses that warrant outright prohibition, such as real-time biometric surveillance in public spaces or social scoring, from uses that warrant calibrated obligation, such as conformity assessment for credit-scoring or recruitment tools, from uses that warrant only disclosure, such as consumer-facing chatbots.[43] India is not required to adopt the EU's specific thresholds or its notified-body conformity architecture, both of which presuppose an institutional and market-surveillance capacity that India would need to build, but it can adapt the underlying logic, that regulatory intensity should scale with demonstrated risk to rights, to its own administrative capacity and constitutional text.

Third, and most fundamentally, the absence of statutory safeguards converts what ought to be a legislative choice into an unaddressed constitutional exposure. Where automated decisions affect access to welfare, credit, employment or liberty, the Puttaswamy proportionality standard applies in principle but has no statutory hook through which an affected person can invoke it before harm occurs; the current recourse is post hoc constitutional litigation, which is slow, expensive and available only to those with the resources and the specific occasion to file a writ petition. A statutory right to explanation, an ex ante conformity assessment requirement for high-risk deployments, and an accessible administrative appeal mechanism would each operationalise the Puttaswamy and Anuradha Bhasin standards prospectively rather than leaving them available only in retrospective litigation. The doctrinal and comparative analysis undertaken above therefore converges on a single finding: India's constitutional framework already supplies the values a comprehensive AI statute must protect, equality under Article 14, freedom of expression and profession under Article 19, and life and personal liberty under Article 21, and the European experience supplies a tested, if imperfect, structural template for translating those values into enforceable obligations. What India lacks is the intervening legislative act.

---

[43] EU AI Act, supra note 5, arts. 5, 6, 50.

7. TOWARDS A COMPREHENSIVE INDIAN AI STATUTE: A PROPOSED FRAMEWORK

7.1 Guiding Principles

Any Indian AI statute should rest on six principles. Legality and definitional clarity require that the statute define "artificial intelligence system" and "automated decision-making" with sufficient precision to satisfy the vagueness standard articulated in Shreya Singhal.[44] Risk proportionality requires that obligations scale with demonstrated risk rather than applying uniformly. Transparency and explainability require a statutory right, for any person subject to a materially automated decision, to be informed of that fact and to receive a meaningful explanation of the decision's principal factors. Fairness and non-discrimination require that AI systems used in consequential contexts be subject to periodic bias auditing measured against the equality guarantee in Article 14. Accountability and redress require an independent regulatory authority empowered to investigate, penalise and order corrective action. Privacy by design requires that the statute operate in conjunction with, rather than in duplication of, the data governance obligations already established under the DPDP Act.

7.2 Structural Recommendations

Building on the EU template while departing from it where Indian conditions demand, the proposed statute should be organised as follows. A General Chapter should set out the statute's objects, its territorial and sectoral scope, and precise definitions, expressly excluding purely research and educational uses from its ambit to avoid chilling innovation. A Risk Classification Chapter should adopt a three-tier rather than four-tier structure, prohibited, high-risk and standard-risk, collapsing the EU's limited and minimal categories into a single lighter-touch tier better suited to India's current market-surveillance capacity, while nonetheless preserving the transparency labelling requirement for synthetic content and AI-driven interaction. A Rights and Obligations Chapter should codify the right to explanation, mandate human oversight for high-risk systems, and require conformity documentation proportionate to risk, permitting self-assessment for most high-risk deployments in the near term with third-party audit reserved for the most sensitive categories, namely law enforcement, welfare eligibility and credit underwriting, so as to build institutional audit capacity incrementally rather than overburden it immediately.

A Regulatory Authority Chapter should establish an AI Regulatory Authority with power to register high-risk deployments, investigate complaints, impose graduated penalties, and coordinate with the existing Data Protection Board rather than duplicate its functions, given that the two bodies will

[44] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1.

necessarily share jurisdiction over AI systems that process personal data. The Authority's membership should draw on the coordination model the 2025 Governance Guidelines propose for the inter-ministerial AI Governance Group, but with statutory rule-making and adjudicatory powers that a policy coordination body cannot exercise, and it should be required to publish an annual register of high-risk deployments across government departments, extending to the public sector the same disclosure discipline the statute would impose on private developers. A Penalties Chapter should provide for civil penalties scaled to enterprise turnover, broadly modelled on Article 99 of the EU Act, while ensuring that penalty ceilings are calibrated to Indian market conditions rather than mechanically imported. Sectoral Annexures should impose enhanced obligations for AI used in policing, welfare administration, healthcare and finance, building on the RBI's FREE-AI recommendations for the financial sector and extending an equivalent discipline to law enforcement and welfare use, where the consequences of algorithmic error are most severe and least visible to the affected individual. A dedicated provision should also reconcile the statute with the surveillance powers currently exercised under Section 5(2) of the Indian Telegraph Act, 1885 and Section 69 of the Information Technology Act, 2000, requiring that any AI-assisted interception or surveillance system satisfy the Puttaswamy proportionality test through a documented necessity assessment, rather than relying on executive notification alone.[45] An Appeals Chapter should create a statutory right of appeal against automated decisions on grounds of bias, arbitrariness or constitutional infirmity, adjudicated in the first instance by the AI Regulatory Authority and thereafter by the appellate mechanism already contemplated under the DPDP Act, to avoid multiplying forums. Finally, a Compliance and Transitional Provisions Chapter should stagger obligations by risk tier, granting existing high-risk deployments a defined transition period to achieve compliance, mirroring the EU's own phased implementation and thereby avoiding the disruption that an immediate, undifferentiated compliance deadline would cause.

This architecture deliberately narrows the EU's four-tier system to three tiers, prefers self-assessment over mandatory third-party audit for most high-risk uses in the initial phase, and channels appeals through an existing forum rather than creating a new appellate tier, precisely because India's regulatory capacity, unlike that of the twenty-seven-member European Union with its established network of national supervisory authorities and notified bodies, must be built rather than assumed. A statute that promises more oversight than the state can deliver would replicate, in a new form, the gap between paper rights and practical remedy that already characterises much of India's existing AI governance.

---

[45] The Indian Telegraph Act, No. 13 of 1885, § 5(2) (India); The Information Technology Act, No. 21 of 2000, § 69 (India).

8. CONCLUSION

The comparative and doctrinal analysis undertaken in this paper demonstrates that India's current legal response to artificial intelligence, a combination of general-purpose statutes never drafted with algorithmic decision-making in view and a series of non-binding policy instruments culminating in the 2025 India AI Governance Guidelines, is structurally incapable of addressing the harms that AI-specific regulation exists to prevent, namely algorithmic opacity, unaudited discrimination and the absence of a right to explanation or appeal. The European Union's Artificial Intelligence Act shows that a risk-tiered, rights-anchored statute is not merely theoretically desirable but practically achievable, even if the Union's own implementation experience, marked by phased deadlines and an ongoing simplification exercise, counsels against uncritical transplantation. India's constitutional jurisprudence, from Puttaswamy through Anuradha Bhasin to Internet and Mobile Association of India, already supplies the substantive standards of legality, necessity and proportionality that any such statute must codify; what remains absent is the legislative act that would make those standards enforceable before, rather than only after, an algorithm has caused harm. The framework proposed in Part 7 of this paper, a three-tier risk classification, a dedicated regulatory authority coordinated with the Data Protection Board, a statutory right to explanation, and sectoral annexures for the highest-stakes deployments, offers one route by which Parliament could close this gap without either abandoning India's own institutional trajectory or ignoring the lessons the European experience has to offer. Until such a statute is enacted, India's growing reliance on artificial intelligence in governance will continue to outpace the constitutional protections its own courts have already recognised as due to every citizen.

BIBLIOGRAPHY

Statutes and Regulations

1. The Constitution of India, 1950.
2. The Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
3. The Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
4. The Indian Telegraph Act, No. 13 of 1885, Acts of Parliament, 1885 (India).
5. Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1.
6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act), 2024 O.J. (L 1689).

Cases

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.
2. Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637.
3. Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1.
4. Internet & Mobile Ass'n of India v. Reserve Bank of India, (2020) 10 S.C.C. 274.

Articles

1. Ameen Jauhar, Facing up to the Risks of Automated Facial-Recognition Technologies in Indian Law Enforcement, 16 Ind. J.L. & Tech. 1 (2020).
2. Aryan Sherwal, Artificial Intelligence Regulation in India, 5(1) Int'l J. Interdisc. Res. L. 324 (2025).
3. Dr. Anant D. Chinchure, Information Technology Vis-À-Vis Right to Privacy: Legal and Judicial View, 3(6) Int'l J. Res. Publ'n & Reviews 2221 (2022).
4. Galia Mancheva, European Union Regulatory Framework on Artificial Intelligence (SMEs), 2 J. Dev. Stud. 20 (2021).
5. Graham Greenleaf, Promises and Illusions of Data Protection in Indian Law, 1 Int'l Data Priv. L. 47 (2010).
6. Manisha Nandan, Data Privacy Law in India: Past, Present and Legal Framework, 6(6) Int'l J.L. Mgmt. & Legal Rsch. 1092 (2025).
7. Nibedita Basu & Rhishikesh Dave, Comparative Analysis of Laws in AI, 5 SDGs Rev. 1 (2025).
8. Nilesh Chaudhary, Legal Challenges in AI Surveillance: Balancing Security and Privacy, 12(1) Cyber & L. Rev. 115 (2021).
9. Sangchul Park, Bridging the Global Divide in AI Regulation: A Proposal for a Contextual, Coherent, and Commensurable Framework, 33(2) Harv. J.L. & Tech. 216 (2024).
10. Shivangi Gaur & Tanima Bhatia, Generative AI and Data Protection: The Regulatory Tapestry in India and EU, 6(3) Int'l J. Legal Sci. & Innovation 407 (2024).

Reports and Web Sources

1. NITI Aayog, National Strategy for Artificial Intelligence #AIforAll (2018).
2. Reserve Bank of India, Framework for Responsible and Ethical Enablement of Artificial Intelligence (Aug. 13, 2025).
3. Ministry of Electronics & Information Technology, India AI Governance Guidelines (Nov. 5, 2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf.
4. Amlan Mohanty & Shatakratu Sahu, India's Advance on AI Regulation, Carnegie Endowment (June 5, 2025), https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation.
5. Kritika Krishnamurthy & Niket Khandelwal, AI Regulation in India vs the EU: Balancing Innovation and Risk, Mondaq (June 5, 2025), https://www.mondaq.com/india/new-technology/1509322.

6. Nidhi Singh, Navigating AI Regulation: A Comparative Analysis of EU and Lessons for India, IndiaAI (June 12, 2025), https://indiaai.gov.in/article/navigating-ai-regulation-a-comparative-analysis-of-eu-and-lesson-for-india.

7. Shweta Bharti & Pranshu Singh, EU Artificial Intelligence Act: Comparing India's Approach with Principles Embedded in First-of-its-Kind EU Legislation, Bar & Bench (June 12, 2025), https://www.barandbench.com.

8. Tom Jozak, 2024 EU AI Act: A Detailed Analysis, SSRN (June 2, 2025), https://ssrn.com/abstract=5196856.