The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

AI GOVERNANCE IN INDIA: A COMPARATIVE ANALYSIS OF THE FRAGMENTED REGULATORY FRAMEWORK AND THE NEED FOR COMPREHENSIVE AI-SPECIFIC LEGISLATION IN LIGHT OF THE EU AI ACT

~ Deepshikha

Abstract

Artificial Intelligence (AI) is rapidly growing and transforming governance, business, finance, and other sectors but it is also raising concerns regarding privacy, transparency, bias, accountability, safety. The increasing growth of AI has created an urgent need for a comprehensive law for AI governance.

This paper critically examines how AI governance is needed in India and whether the existing frameworks are adequate to address the challenges posed by evolving AI. The study analyses India's current framework in relation to AI Governance including all existing laws, data protection laws, privacy policies and approaches adopted by institutions like RBI and SEBI.

The gap research that this paper is trying to address is that despite existence of various laws, guidelines, frameworks that India has to apply to AI related activities, it lacks a comprehensive AI specific law which can establish clear classification, obligations, accountability standards. Currently the existing laws through which AI Governance is addressed is uncertain and inconsistent across different sectors

The research paper is based on doctrinal and comparative legal methodology. It criticality analyses the existing legal framework in India and compare it with other countries AI acts like EU AI Act.

The research conclusion is that the development of a comprehensive AI governance framework is needed in India. Instead of replicating the EU model, the proposed framework

should address India's specific constitutional, economic, social, and technological need while ensuring innovation, accountability, and the protection of fundamental rights.

Keywords: AI, AI Governance, EU AI act, Indian legal framework, risk-based regulation

1. Introduction

Artificial Intelligence also known as AI has been rapidly growing from the laboratory to infrastructure of everyday life. Machine Learning systems informs and make decisions on credit, employment, healthcare, policing and welfare delivery and generative models have extended automation to the generation of text, audio and code. The legal significance lies less in the novelty of the technology than the character of the decisions it mediates. Decisions that allocate opportunities and burdens among individuals, through processes that the affected person can neither observe nor readily contest.

Every state respond to this in different ways. The European Union has adopted Regulation (EU AI Act), which came into force on 1 August 2024. And is known as first comprehensive horizontal statue to regulate AI, it classifies the level of risks.[1] India has so far taken a different route. In November 2025, the Ministry Electronics and Information Technology has published AI Governance Guidelines, it's a non binding framework which talks about the seven guiding principles which relies on existing frameworks and expressly favours innovation over restraint.[2] India has policy philosophy of AI governance but yet to have a specific framework for AI governance.

The main problem in India is not there is no specific law that dealt with AI but the absence of coherence. Currently the AI related conduct is governed through constitutional doctrine, Digital Personal Data Protection Act, 2023 (DPDP Act), Information Technology Act,2000(IT Act), other acts such as criminal laws, consumer laws and also circulars of sectoral regulatory like RBI, SEBI. However, none of them defines AI, classify AI uses by risk, allocates the responsibility between developers and deployers or rights of an affected persons.

This can be studied through an illustration; a small trader applies for a loan through the lending application but is refused within seconds. No reason or explanation is given. The person has no idea as who is responsible as the developer states that the model is proprietary,

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L2024/1689 (AI Act).
[2] Ministry of Electronics and Information Technology, *India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation* (Government of India, November 2025) (Guidelines).

the bank says that the its based on third party score, personal data supplied through intermediaries before reaching the model. The harm is real but there is no regulations that answers who is responsible, by what standard and with what remedy. The existing framework only dealt with data protection, banking circular, consumer legislation and general constitutional principles.

The gap that this paper tries to address is the lack of sustained doctrinal assessment of whether India's fragmented framework is adequate and, if it is not, of what an Indian AI statute should contain, as distinct from what the EU model prescribes.

The paper resolve around three research questions (a) To what extent do India's existing constitutional, statutory, sectoral and soft-law instruments address the harms that AI systems cause or risk causing? (b) What may India learn, and what should it deliberately decline to adopt, from the EU AI Act, including its recent recalibration? (c) If the existing framework proves inadequate, what should the structure and content of a comprehensive Indian AI statute be? The main object of this paper is to evaluate the Indian Framework, to analyse EU AI Act and to identify the legal gap.

The central argument is that India present approach is not sufficient as its able to address who is responsible, which standards applies, and what remedy is available. This uncertainty itself is a regulatory cost as it falls hardest on the ordinary person and on small developers. However, at the same time adopting whole EU Model can be a mistake as it presupposes institutional capacity, a compliance culture, and a market structure that India does not yet have. This paper hence argues that India should develop a short, principle-led, risk-sensitive framework statute that sets the spine and leaves the details to sectoral regulators and to rules that can be updated quickly.

The question is also one of timing. Technology regulation faces what David Collingridge described as a dilemma of control: in the early life of a technology its harms cannot yet be known, and by the time they are visible the technology is so entrenched that it is difficult to steer.[3]

The study adopts a doctrinal and comparative methodology. The doctrinal component identifies, systematises and critically analyses the primary sources of Indian law (the

[3] David Collingridge, *The Social Control of Technology* (Frances Pinter 1980) 11–12.

Constitution, statutes, subordinate legislation, regulatory circulars and judicial decisions)together with secondary scholarship, testing them for coherence and for gaps.[4] The comparative component employs the EU AI Act as a functional comparator: the inquiry is not whether the two systems use similar language but whether they address the same regulatory problem, and with what effect.[5]

2. Artificial Intelligence

2.1 What does AI means?

The definitions are the heart of any regulatory framework. In India the term AI is not defined under any regulatory framework. The EU AI Act defines an AI system as a machine-based system designed to operate with varying levels of autonomy that, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.[6] The definition is similar to the definition given by OECD in its Recommendation on Artificial Intelligence, which has become something of a global reference point.[7]

There are two main words in the definition one is “infers”. It separates AI from conventional software, which executes rules that a programmer wrote in advance, from systems that derive their own rules from data. And the other is “varying levels of autonomy”, which acknowledges that AI is a spectrum rather than a category.

As Indian law doesn’t have a statutory definition of AI. And without definition, courts and regulators has to decide case by case and statute by statute whether the system in question is a “computer resource”, “a product”, “a service”, “an algorithm” or just a tool in the hands of human decision making. Each of them trigger a different legal consequences.

2.2 AI and Traditional Legal Framework

Its very tempting and easy to say that AI is just another technology and that the existing framework is sufficient to address it. Somewhere this view is okay like how fraud committed

[4] Terry Hutchinson and Nigel Duncan, ‘Defining and Describing What We Do: Doctrinal Legal Research’ (2012) 17 Deakin Law Review 83.
[5] Konrad Zweigert and Hein Kötz, *An Introduction to Comparative Law* (Tony Weir tr, 3rd edn, Clarendon Press 1998) 34–36.
[6] AI Act (n 1) art 3(1).
[7] OECD, *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449, adopted 2019, amended 2024).

with a deepfake is still a fraud. However there are four features of AI that makes the analogy imperfect.

Opacity: Many high-performing models are difficult even for their designers to interpret. Frank Pasquale's in the "black box society" describes how decisions that shape credit, employment and reputation are increasingly made by systems whose logic is hidden by technical complexity and by trade secrecy.[8] Jenna Burrell separates three sources of opacity: deliberate corporate secrecy, technical illiteracy on the part of those affected, and the genuine mismatch between the way machines represent patterns and the way humans reason.[9] The law can address few of them but not all.

Scale and the reproduction bias: a bias person only harms the candidate they meet however a bias model harm every candidate it scores. Joy Buolamwini and Timnit Gebru has also stated that commercial facial analysis systems had markedly higher error rates for darker-skinned women than for lighter-skinned men,[10] and ProPublica's analysis of a US recidivism tool found that its errors fell differently on Black and white defendants.[11] These studies have clearly established a point that matters for law: discrimination can be produced by a system in which no individual has discriminatory intent, and conventional non-discrimination law, built around intent or identifiable comparators, struggles to see it.[12]

Adaptiveness: Traditional product regulation assumes that a product is fixed at the time it is sold. A model that is retrained or fine-tuned after deployment changes its behaviour over time, so that the thing that was tested is not exactly the thing that is in use.

Problem of many Hands: Helen Nissenbaum identified, well before the current wave of machine learning, that computerised systems are built by teams, trained on others' data, deployed by third parties and used by individuals, so that when something goes wrong responsibility dissolves across the chain.[13]

---

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

[9] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 Big Data & Society 1.

[10] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77.

[11] Julia Angwin and others, 'Machine Bias' (ProPublica, 23 May 2016).

[12] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI' (2021) 41 Computer Law & Security Review 105567.

[13] Helen Nissenbaum, 'Accountability in a Computerized Society' (1996) 2 Science and Engineering Ethics 25.

3. India's Existing Framework

India does not have a specific law for AI related; there are many laws that governs AI indirectly. Here we will talk about those laws under six heads and they are constitutional law, data protection, information technology law, private and criminal law, intellectual property, and sectoral regulation. It then examines the soft-law architecture that now sits over them.

3.1 constitutional law

Any law derives its power from constitution. Indian source of AI governance is not statutes but a judgement. In Justice K S Puttaswamy (Retd) v Union of India, a nine-judge bench held that privacy is a fundamental right protected under Article 21 and as part of the freedoms guaranteed by Part III.[14] The plurality opinion also set out a test, drawn together from earlier case law, for permissible interference with privacy: the interference must be backed by law, must serve a legitimate aim, and must be proportionate to the need for it.[15] This structure matters as it means that State use of AI for surveillance, welfare targeting or policing must pass a proportionality test, and it gives courts a ready-made vocabulary for assessing algorithmic interference.

Article 14 is also one of the important point as since E P Royappa v State of Tamil Nadu the Supreme Court has treated arbitrariness as antithetical to equality,[16] and in Shayara Bano v Union of India a plurality accepted that legislation can be struck down as manifestly arbitrary.[17] An opaque automated decision that cannot be explained to the person it affects is a natural candidate for this kind of challenge when taken by a public authority.

The Aadhar case judgment is also important under this. The Court there applied a proportionality analysis and read down parts of the Aadhar framework, in a case that turned precisely on large-scale data processing by the State and on the safe guards needed around it.[18]

Fundamental rights are enforced against the State. Yet most AI harms are inflicted by private sectors such as banks, platforms, employers and insurers. In Kaushal Kishor v State of Uttar Pradesh the Court held that certain fundamental rights can be enforced horizontally against

[14] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (Puttaswamy).
[15] ibid para 325 (Chandrachud J).
[16] EP Royappa v State of Tamil Nadu (1974) 4 SCC 3.
[17] Shayara Bano v Union of India (2017) 9 SCC 1.
[18] Justice KS Puttaswamy (Retd) v Union of India (2019) 1 SCC 1 (Aadhaar).

non-State, but the scope of that holding is still being worked out.[19] Hence constitution gives India principles, but fails to supply the obligations, remedies that private sector AI use needs.

3.2 Data protection (DPDP Act)

Digital Personal Data Protection Act, 2023 is the statute that is seen as India's de facto AI law as all AI development begins with data. The Digital Personal Data Protection Rules 2025, notified in November 2025, give operational detail and stagger commencement over a period of months[20]The DPDP Act is consent-centred. It requires notice and consent for processing personal data, recognises a list of "legitimate uses", imposes duties on data fiduciaries, creates rights of access, correction, erasure and grievance redress for data principals, and establishes a Data Protection Board of India.[21]

In terms of AI governance three provisions of the Act is relevant (a) Section 8(3), which requires a data fiduciary to ensure the completeness, accuracy and consistency of personal data where it is likely to be used to make a decision that affects the data principal. However, the act is silent on whether a person has a right to know that a decision was automated, to have it explained, or to have it reviewed by a human. (b) Section 3(c)(ii) excludes the data that the principal herself has made publicly available, or that has been made public under a legal obligation from the scope of the act. In the context of generative AI, where models are commonly trained on material scraped from the open web, that exclusion potentially removes a very large category of training data from the Act's protections. (c) Section 17 talks about exemptions. section17(2)(a) allows the Central Government to exempt State instrumentalities by notification on grounds such as sovereignty and public order and Section 17(2)(b) exempts processing necessary for research, archiving or statistical purposes where the data is not used to take decisions specific to a data principal and where prescribed standards are followed.[22] Read together with section 36, which requires fiduciaries to furnish information the Government calls for, this means that the entities most likely to deploy AI at scale over citizens, namely State agencies, may be the least constrained by the Act.

The contrast with the European General Data Protection Regulation is instructive. Article22 of the GDPR gives individuals a qualified right not to be subject to decisions made solely on

[19] Kaushal Kishor v State of Uttar Pradesh (2023) 4 SCC 1.
[20] Digital Personal Data Protection Rules 2025 (India) (notified November 2025).
[21] Digital Personal Data Protection Act 2023 (India) (DPDP Act) ss 4–7 (grounds, notice, consent and legitimate uses), ss 8–10 (obligations of data fiduciaries, children, and significant data fiduciaries), ss 11–14 (rights of data principals), ss 18–19 (Data Protection Board of India).
[22] DPDP Act (n 21) ss 17(2)(a)–(b) and 36.

automated processing that produce legal or similarly significant effects.[23] In SCHUFA, it held that the automated generation of a credit score can itself amount to an automated decision where a third party draws strongly on it in deciding whether to grant credit.[24] It governs the inputs, namely personal data, but it was not designed to govern models, outputs or deployment decisions, and it does not reach non-personal data or inferences that are not about an identifiable individual.

3.3 Information Technology Law

Information Technology Act, 2000 is the main legislation for cyber crimes. Several of the provisions of the Act can be applied to AI-related misconduct. section 66C (identity theft),section 66D (cheating by personation using a computer resource), section 67 (publishing obscene material electronically), and section 69A (blocking powers).[25] Section 79 gives intermediaries conditional safe harbour from liability for third-party content, a protection the Supreme Court read down in Shreya Singhal v Union of India by holding that intermediaries lose it only on receiving actual knowledge through a court order or government notification.[26]

The Act has flows also as it was drafted in 2000 for cybercrime which were done through computer or email (electronically). It talks about "computer resources" and "intermediaries", categories that map awkwardly onto a foundation model that is neither a pure conduit for third-party content nor a conventional publisher of its own. Government has done Amendments however still its focuses on cybercrimes and have no where mentioned AI-related problems. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code)Rules 2021 have been amended several times, most significantly for present purposes by the amendment notified on 10 February 2026 and in force from 20 February 2026.[27] The2026 amendment introduced a definition of "synthetically generated information", obliges intermediaries that enable its creation to deploy reasonable technical measures against

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR) art 22.
[24] Case C-634/21 *OQ v Land Hessen (SCHUFA Holding (Scoring))* ECLI:EU:C:2023:957 (SCHUFA).
[25] Information Technology Act 2000 (India), ss 66C, 66D, 67 and 69A.
[26] Shreya Singhal v Union of India (2015) 5 SCC 1.
[27] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India), as amended by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026 (notified 10 February 2026, in force 20 February 2026) (IT Rules 2021).

unlawful content, requires labelling of lawful synthetic content, and sharply shortens takedown timelines for certain categories such as intimate-image abuse and impersonation.[28]

The definition talks about audio, visual and audio-visual material; text-only outputs, including AI-generated text and chat bot responses, appear to fall outside it.[29] An AI-drafted fake news article is therefore treated differently from an AI-generated fake video, even though the harm to an election or a reputation may be identical. More fundamentally, the rules operate through intermediary due diligence, which means the regulatory hook is the platform, not the developer, and the unit of regulation is content, not the system that produced it. A model that is biased, unsafe or unexplainable, but which produces no unlawful content in the narrow sense, is untouched.

3.4 Private law, criminal law and personality rights

The Consumer Protection Act 2019 talks about product liability regime in Chapter VI, imposing liability on manufacturers, service providers and sellers for harm caused by defective products and deficient services.[30] Applying this to AI the line is very blurry to determine whether an AI-powered application a "product", in which case the product liability rules apply, or a "service", in which case the claimant must show deficiency?

In tort, the law of negligence is flexible enough in principle to accommodate AI, but a claimant must establish a duty, breach and causation, and each of these runs into the opacity problem. How does a claimant prove that a developer failed to take reasonable care in training a model whose logic she cannot inspect?

The Bharatiya Nyaya Sanhita 2023 talks about offences, such as cheating by personation and defamation that can capture AI-assisted wrongdoing.[31] The main difficulty is proving mens rea. Criminal liability attaches to persons who intend or know. It does not obviously attach to the developer of a general-purpose tool that a third party later misuses.

The most dynamic area in practice has been personality rights. The Delhi High Court in Anil Kapoor v Simply Life India granted an injunction against the use of an actor's name, likeness

[28] ibid r 2(1)(wa) (definition) and r 3 (due diligence). For commentary see ‘Government Notifies Information Technology Amendment Rules 2026’ (SS Rana & Co, February 2026).
[29] IT Rules 2021, as amended (n 27) r 2(1)(wa); Ministry of Electronics and Information Technology, ‘Frequently Asked Questions on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026’ (MeitY, 10 February 2026).
[30] Consumer Protection Act 2019 (India), ch VI (ss 82–87).
[31] Bharatiya Nyaya Sanhita 2023 (India), s 319 (cheating by personation) and s 356 (defamation).

and voice, including by AI-generated and deepfake content.[32] and the Bombay High Court in Arijit Singh v. Codible Ventures LLP restrained the use of AI voice-cloning tools to imitate a singer.[33] From these cases it can be seen that India need of specific framework.

3.5 Intellectual Property

Generative AI presents two intellectual property questions: whether training on copyrighted works is infringing, and who, if anyone owns what the model produces. On the first, the Copyright Act 1957 contains a closed list of fair dealing exceptions in section52 and no express text and-data-mining exception.[34] The same question is now before the Delhi High Court in ANI Media Pvt Ltd v Open AI Inc, in which a news agency alleges that its content was used to train a large language model without authorisation.[35] The case is still pending, and any assessment of how it will be resolved would be speculation.

On the second question, section 2(d)(vi) of the Copyright Act defines the author of a computer-generated work as the person who causes the work to be created. That wording predates generative AI by decades. It is capable of accommodating a user who prompts a model, but it leaves open whether an output that a human did not meaningfully shape attracts any protection at all.

3.6 Sectoral Regulation

The parliament has yet to address this however the most developed sectoralthinking is in finance.

The Reserve Bank of India's FREE-AI Committee (Framework for Responsible and Ethical Enablement of AI) submitted its report in August 2025. It set out seven principles, called "sutras", and a set of recommendations covering governance, model validation, disclosure and consumer protection for regulated entities.[36]

The Securities and Exchange Board of India has also moved. A 2019 circular required market infrastructure institutions to report AI and machine learning applications and systems they

[32] Anil Kapoor v Simply Life India 2023 SCC OnLine Del 6914.
[33] Arijit Singh v Codible Ventures LLP 2024 SCC OnLine Bom 2445.
[34] Copyright Act 1957 (India), s 52.
[35] ANI Media Pvt Ltd v OpenAI Inc CS(COMM) 1028/2024 (Del HC).
[36] Reserve Bank of India, *Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI) Committee Report* (August 2025).

offer or use,[37] and in June 2025 SEBI issued a consultation paper proposing guidelines for the responsible use of AI and ML in securities markets, with proposals on governance, testing, fairness and accountability.[38]

Even in health, the Indian Council of Medical Research has issued ethical guidelines for the application of AI in biomedical research and healthcare,[39] while AI-based diagnostic software may be regulated as a medical device under the Medical Devices Rules 2017.[40]

4. The EU AI Act

The Act came into force on 1 August, 2024 and it categorise risk into different levels.[41] Relying on the internal-market competence in Article 114 TFEU, it is in structure a product-safety regulation adapted to software.[42] It categorise AI uses into four tiers: prohibited practices, such as social scoring and untargeted scraping of facial images;[43] high-risk systems, being safety components of regulated products or uses in eight listed areas including employment, education, essential services and law enforcement;[44] transparency duties for systems that interact with people or generate synthetic content;[45] and an unregulated residue. A separate chapter regulates general-purpose models.[46]

As high risk system carry heavy obligations the providers must meet requirements on risk management, data governance, documentation, logging, human oversight, accuracy and robustness, pass a conformity assessment and register the system:[47] deployers must follow instructions, assign competent human oversight, keep logs and, in specified cases, assess

---

[37] Securities and Exchange Board of India, *Reporting for Artificial Intelligence (AI) and Machine Learning (ML) Applications and Systems Offered and Used by Market Infrastructure Institutions (MIIs)* (SEBI circular SEBI/HO/MRD/DOP1/CIR/P/2019/24, 31 January 2019).

[38] Securities and Exchange Board of India, *Consultation Paper on Guidelines for Responsible Usage of AI/ML in Indian Securities Markets* (June 2025).

[39] Indian Council of Medical Research, *Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare* (ICMR 2023).

[40] Medical Devices Rules 2017 (India).

[41] AI Act (n 1) art 113.

[42] AI Act (n 1) recital 1; Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 (TFEU) art 114; Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22 Computer Law Review International 97.

[43] AI Act (n 1) art 5(1).

[44] AI Act (n 1) art 6 and annexes I and III.

[45] AI Act (n 1) art 50.

[46] AI Act (n 1) arts 51–55.

[47] AI Act (n 1) arts 8–15, 16, 43 and 49.

fundamental-rights impact.[48] Compliance with harmonised standards raises a presumption of conformity.[49]

The Act has two main limits. First, its product-safety logic regulates the system and the provider more closely than it protects the affected person, who has no substantive enforceable rights under the Act itself; critics also note its reliance on providers' self-assessment, including the Article 6(3) derogation.[50] Second, it presupposes harmonised standards, conformity-assessment bodies and national authorities that had to be built from scratch.[51]

5. Comparative Analysis between India and European Union

The comparison between two countries are not easy specially when one country have dedicated AI regulation and another has none. India does regulate AI-related conduct but indirectly through its existing legislation and EU regulates it directly through EU AI Act.[52] The comparison is made under four heads legal form, definition, classification; obligations and responsibility; individual rights and public sector use and Generative AI, enforcement and innovation.

Legal form, definition and classification

The EU AI Act is a regulation so it is binding directly on the member state without a national legislation to give it effect.[53] While India doesn't anything to compare as its guidelines are voluntary and the government stated its position that the existing laws are sufficient to handle AI-risk for now.[54]

The main difference is the definitions . EU AI Act defines an AI system in Article 3(1), following the OECD formulation.[55] In India there is no general definition. The nearest definition is of "synthetically generated information" in the amended IT Rules, which covers

[48] AI Act (n 1) arts 26–27.
[49] AI Act (n 1) art 40.
[50] AI Act (n 1) art 6(3); Veale and Zuiderveen Borgesius (n 42); Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' (2024) 26 Yale Journal of Law & Technology 671.

[51] AI Act (n 1) arts 64–65 and 70.
[52] AI Act (n 1); Guidelines (n 2).
[53] TFEU (n 42) art 288; AI Act (n 1) art 113.
[54] Guidelines (n 2) pt 2 (Policy and Regulation).
[55] AI Act (n 1) art 3(1); OECD (n 7).

only audio, visual and audio-visual content and was written for intermediaries, not for AI as such.[56]

After the definition the next is classification. The EU Act sorts systems into four tiers, from prohibited practices down to minimal risk, and each tier has its own consequences.[57] India has no general classification, so risk is handled sector by sector, if at all. The RBI's FREE-AI framework, for example, speaks only to regulated financial entities.[58]

Obligations and responsibility

The EU AI Act clearly states the obligations and responsibilities of each person (developers, deployers). Providers of high-risk systems have to run a risk-management system, keep technical documentation, build in human oversight and pass a conformity assessment, and deployers have their own duties on oversight, monitoring and logs.[59] The act also states that a deployer that modifies a system or changes its purpose is treated as a provider, and suppliers of components must agree with the provider what information they will pass on.[60]

In India, duties are there howsoever, they are scattered and none of them were specifically written for AI. Data fiduciaries owe duties under the DPDP Act,[61] and intermediaries owe due diligence under the IT Rules.[62] The data-quality duty in section 8(3) of the DPDP Act concerns the accuracy of data, not the quality of a decision.[63]

Individual rights and public-sector use

EU AI Act has claims for the affected person under the act. A person can complain to the concerned authority and, where a high-risk system contributed to a decision with significant adverse effects, can ask for a clear explanation of the system's role.[64] The GDPR adds a qualified right against solely automated decisions in Article 22,[65] which the Court of Justice

[56] IT Rules 2021, as amended (n 27) r 2(1)(wa).
[57] AI Act (n 1) arts 5, 6 and 50 and annexes I and III.
[58] RBI, FREE-AI Committee Report (n 36).
[59] AI Act (n 1) arts 8–16, 26 and 43.
[60] ibid art 25(1) and (4).
[61] DPDP Act (n 21) ss 4–10.
[62] IT Rules 2021, as amended (n 27) r 3.
[63] DPDP Act (n 21) s 8(3).
[64] AI Act (n 1) arts 85–86.
[65] GDPR (n 23) art 22.

has read broadly enough to catch a credit score on which a lender relies heavily.[66] What the AI Act does not give is a right to damages, which stays with national law.[67]

India's rights are tied to data, not to decisions. A data principal can seek access, correction, erasure and grievance redress,[68] but has no right to know that a decision was automated, to have it explained, or to have a human look at it again.

The AI Act prohibits certain practices, such as social scoring, and requires public deployers of high-risk systems to assess the impact on fundamental rights before first use.[69] In India the main constraint is the *Puttaswamy* proportionality test, applied in the Aadhar case to large-scale State data processing.[70] The DPDP Act points the other way, as section 17(2)(a) lets the Central Government exempt State instrumentalities by notification.[71]

Generative AI, enforcement and innovation

The EU has a separate chapter on general-purpose models. All providers must keep documentation, adopt a copyright policy and publish a summary of training data, and providers of models that pose systemic risk must also evaluate and mitigate those risks and report serious incidents.[72] India has no model-level duties. Its only binding rules on generative AI are the labelling and takedown obligations that the 2026 IT Rules place on intermediaries, and these cover audio-visual content only.[73]

In the EU, national market surveillance authorities supervise most obligations, the AI Office supervises general-purpose models, and fines for prohibited practices can reach EUR 35 million or 7 per cent of worldwide turnover.[74] In India, enforcement stays with sectoral regulators inside their own fields.

6. The Gaps in India's Framework

Till now in this paper six gaps has emerged.

---

[66] *SCHUFA (n 24).*
[67] Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives' (n 50).
[68] DPDP Act (n 21) ss 11–14.
[69] AI Act (n 1) arts 5(1) and 27.
[70] *Puttaswamy (n 14); Aadhaar (n 18).*
[71] DPDP Act (n 21) ss 17(2)(a) and 36.
[72] AI Act (n 1) arts 51–55.
[73] IT Rules 2021, as amended (n 27) rr 2(1)(wa) and 3.
[74] AI Act (n 1) arts 64–65, 70 and 99(3).

1. No definition of AI system, without a statutory definition and without agreed categories such as developer, deployer and user, every rule must define its own scope or leave it unstated.
2. No allocation of responsibility, this is one of the most important question as to who is answerable for harm, the developer who trained the model, the company that fine-tuned it, the deployer who put it in front of customers, or the individual user. Indian law offers no answer, and a court faced with the question will have to improvise using the general law of tort, contract and consumer protection.
3. No right to an explanation, to contest or to human review. The DPDP Act's rights concern personal data, not decisions.
4. Weak constraints on state use of AI. The State is both the largest potential deployer of AI over citizens, in welfare targeting, policing and facial recognition, and the actor best insulated by the DPDP Act's exemptions. Smriti Parsheera's work on facial recognition in India documents how such systems have been adopted in the absence of clear legal authority or safeguards[75]
5. No model level duties for general purpose and generative AI. Indian rules address what a generative model produces, and only in respect of synthetic audio-visual content. They do not address how the model was built, what data it was trained on, what testing it underwent, or what systemic risks it poses.
6. No institution with a clear mandate. The Guidelines propose an AI Governance Group, a Technology and Policy Expert Committee and an AI Safety Institute. These are sensible bodies, but as proposed they coordinate, advise and evaluate. None is given the statutory power to require information, to investigate or to impose a sanction.

7. Towards an Indian AI Framework Statute

7.1 what India can take from the EU

The EU AI Act can be most useful as a source of structure. The provion that can be taken from the act are (a) general definition of an AI system. Article 3(1) follows the OECD formulation,[76] and something similar in India would give courts and regulators one threshold question to ask, instead of deciding each time whether the system before them is a “computer resource”, a “product” or a “service”. (b) the division of roles between providers and deployers, which tells each actor what it owes.[77] (c) the tiered approach to risk, which lets

[75] Smriti Parsheera, ‘Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?’ (Data Governance Network Working Paper 05, 2019).
[76] AI Act (n 1) art 3(1); OECD (n 7).
[77] AI Act (n 1) arts 16 and 26.

obligations follow the seriousness of the use.[78] (d) the separate set of duties for general-purpose models,[79] which reaches a layer of the technology that India's content-focused IT Rules do not touch.

7.2 What shouldn't be taken

There are few parts as the EU AI Act that is not suited for India. First is the dependence on harmonised standards and conformity assessment, which presumes institutions India has yet to build.[80] The EU itself has struggled here. Its AI Omnibus entered into force on 27 July 2026 and moved the compliance date for stand-alone Annex III high-risk systems, including credit and employment uses, from August 2026 to December 2027. The aim was to have the necessary standards and support infrastructure in place before enforcement begins,[81] and the risk-based framework itself was left unchanged.[82] If the EU could not have its standards ready on time, India should not make its framework wait on them.

The second is the scale of penalties. Fines of up to EUR 35 million or 7 per cent of worldwide turnover[83] suit multinational providers, but here sanctions should be graduated by size and conduct.

The third is the Act's orientation. Its product-safety logic gives the affected person few enforceable rights.[84] An Indian statute should start instead from the person refused a loan in Section 1 and ask what that person can demand.

7.3 The proposed Framework

India should adopt a short, principle-led statute, leaving detail to rules and sectoral regulators. It should

(a) define "AI system" on the OECD model and fix the roles of developer, deployer and user;[85]

[78] AI Act (n 1) arts 5, 6 and 50 and annex III.
[79] AI Act (n 1) arts 51–55.
[80] AI Act (n 1) arts 40, 43 and 70.
[81] Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) [2026] OJ L2026/1744; 'EU Digital Omnibus on AI Enters into Force' (Mondaq).
[82] 'EU AI Act: Key Amendments Adopted Under the Digital Omnibus Package' (Loyens & Loeff).
[83] AI Act (n 1) art 99(3).
[84] AI Act (n 1) arts 85–86; Veale and Zuiderveen Borgesius (n 42).
[85] AI Act (n 1) art 3(1); OECD (n 7).

(b) prohibit a narrow set of practices, state criteria for high-risk uses, and let RBI, SEBI and the ICMR designate those uses in their own fields,[86] with State deployers bound by the *Puttaswamy* test[87] notwithstanding section 17(2)(a) of the DPDP Act;[88]

(c) allocate duties between developers and deployers, easing the claimant's evidential burden through a rebuttable presumption of causation on breach;

(d) give persons affected by significant decisions rights to notice, explanation, contest and human review;[89]

(e) impose proportionate duties on general-purpose models above a threshold; and

(f) empower a lead authority to require information, investigate and sanction, since the bodies proposed in the Guidelines only advise.[90]

Obligations should attach only to high-risk uses and larger models, with lighter duties for small developers and periodic review of the rules.

8. Conclusion

India does not lack law that touches AI; it lacks law that fits together. *Puttaswamy* and Article 14 bind mainly the State. The DPDP Act protects data rather than decisions, and its exemptions favour the actors most likely to deploy AI at scale. The IT Rules regulate intermediaries and audio-visual content, not AI systems. Consumer, tort, criminal and copyright law stall on who is responsible, and sectoral guidance stays within sectoral lines. Six gaps result: no definition, no allocation of responsibility, no right to explanation or review, weak limits on State use, no model-level duties, and no institution with statutory powers. As the trader in the opening example shows, ordinary people and small developers bear the cost.

The EU Act shows what a comprehensive law can offer, and also the limits of its product-safety design, its reliance on self-assessment and its need for institutions India lacks. The delay to its high-risk deadlines shows how hard that machinery is to build. India should borrow the structure and leave the machinery. A short, principle-led statute, as Section 7 proposes, would give developers clarity about what is expected and individuals clarity about

[86] *RBI, FREE-AI Committee Report (n 36); SEBI, Consultation Paper (n 38); ICMR, Ethical Guidelines (n 39).*
[87] *Puttaswamy (n 14).*
[88] DPDP Act (n 21) s 17(2)(a).
[89] DPDP Act (n 21) ss 11–14; GDPR (n 23) art 22; AI Act (n 1) art 86.
[90] Guidelines (n 2).

what they can demand. That is a condition for sustaining India's AI ambitions, not a restraint on them.