

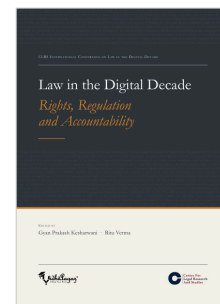
CHAPTER 6

Governance by Design, Accountability by Default? India's Techno-Legal Turn in AI Regulation and the Problem of Contestability

Gautami Seth and Surabhi Kumari

in *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma (VidhiAagaz 2026), pp. 61–71

DOI <https://doi.org/10.63108/VAB.LDD.1.6>



CITATIONS

BLUEBOOK (21ST ED.)

Gautami Seth & Surabhi Kumari, *Governance by Design, Accountability by Default? India's Techno-Legal Turn in AI Regulation and the Problem of Contestability*, in *LAW IN THE DIGITAL DECADE: RIGHTS, REGULATION AND ACCOUNTABILITY* 61 (Gyan Prakash Kesharwani & Ritu Verma eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Gautami Seth and Surabhi Kumari, 'Governance by Design, Accountability by Default? India's Techno-Legal Turn in AI Regulation and the Problem of Contestability' in Gyan Prakash Kesharwani and Ritu Verma (eds), *Law in the Digital Decade: Rights, Regulation and Accountability* (VidhiAagaz 2026) 61.

CHICAGO (17TH ED.)

Seth, Gautami, and Surabhi Kumari. "Governance by Design, Accountability by Default? India's Techno-Legal Turn in AI Regulation and the Problem of Contestability." In *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma, 61–71. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.1.6>.

APA (7TH ED.)

Seth, G., & Kumari, S. (2026). Governance by design, accountability by default? India's techno-legal turn in AI regulation and the problem of contestability. In G. P. Kesharwani & R. Verma (Eds.), *Law in the digital decade: Rights, regulation and accountability* (pp. 61–71). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.1.6>

SOURCE

<https://doi.org/10.63108/VAB.LDD.1.6>

LICENCE

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

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

CHAPTER 6

Governance by Design, Accountability by Default? India's Techno-Legal Turn in AI Regulation and the Problem of Contestability

GAUTAMI SETH* AND SURABHI KUMARI**

India's AI Governance Guidelines (2025) take a light-touch, principle-based path. Instead of a dedicated statute on the model of the EU's Artificial Intelligence Act, they rely on existing law, chiefly the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, and on a "techno-legal" approach that builds legal and policy requirements into the technical architecture of AI systems by design. This chapter argues that the approach is presented as a technical choice but carries constitutional consequences. By moving rule-making from legislatures and courts to code and to the compliance functions of AI developers, it reallocates governing authority, and its reliance on voluntary frameworks shaped by dominant providers risks leaving legal requirements symbolic.

Through a doctrinal and comparative reading of the Guidelines, the IT Amendment Rules 2026, the DPDP Act and the RBI's FREE-AI report against the EU AI Act and Article 22 of the GDPR, the chapter shows that a person affected by an automated decision in India must assemble a remedy from instruments not designed for the purpose: the DPDP Act offers grievance redressal, but no right to contest an automated decision or to receive reasons for it. The chapter concludes that India's principles need clear, legally enforceable rules behind them, with contestability and remedy as a baseline, and that the techno-legal framework, as presently designed, falls short of it.

Keywords: AI governance; techno-legal regulation; governance by design; algorithmic accountability; contestability; due process; self-regulation; India

1 INTRODUCTION

1.1 Overview of the AI Regulation Landscape

Manuel Castells wrote, 'We know that technology does not determine society: it is society'.¹ Increasingly, privately owned web-based platforms control our access to public services, security, education, the public sphere, health services and our very relationship with the countries we live in. As society is 'datafied', public services are delivered through public-private partnerships.² AI's potential has grown rapidly, and governance struggles to keep pace. As a result, AI's rapid evolution continues to create new legal and policy challenges. The growing use of AI also requires processing large volumes of personal and sensitive information, including healthcare data, medical records, and financial records. This raises major concerns

* Manager, New Initiatives & Research at India Legal Research Foundation, Noida, Uttar Pradesh, India.

** Legal Research and Content Associate at India Legal Research Foundation, Noida, Uttar Pradesh, India.

¹ *The Network Society: From Knowledge to Policy*, in *The Network Society: From Knowledge to Policy* 2 (Manuel Castells & Gustavo Cardoso eds., 2006).

² Chinmayi Arun, *AI and the Global South: Designing for Other Worlds*, in *The Oxford Handbook of Ethics of AI* 749 (Markus D. Dubber, Frank Pasquale & Sunit Das eds., 2020).

pertaining to privacy, data security, unauthorised access, and accountability. AI could affect rights to freedom of expression, privacy, social security, and protection against discrimination. It may also violate States' obligation to guarantee these rights without discrimination.³

1.1.1 *Importance of the Topic in the Context of India and Global Trends*

AI regulation has developed into a prominent legal and policy issue, given the prospective impact of AI systems on privacy, equality, human autonomy, employment, healthcare, and other fundamental rights. The European Union's Artificial Intelligence Act⁴ is a legally binding, risk-based regulatory framework, while India's AI Governance Guidelines⁵ adopt a more flexible, principles-based approach that promotes responsible AI development while boosting technological development and innovation. Using the EU's AI Act as a reference, the Guidelines set out a "light-touch," principle-based framework structured around seven guiding "sutras" that relies on existing laws. The "techno-legal" approach intentionally integrates legal instruments and policy regulations directly into the technical architecture of artificial intelligence (AI) systems. This "governance by design" methodology, within a "LAW PLUS" paradigm, is significantly different from the traditional broad legislative regimes. This research analyses the viability of a 'techno-legal' approach, which is 'soft' in nature and appears to be a technical arrangement that significantly reallocates governing authority.

1.1.2 *Purpose of the Paper: Critiquing India's Techno-Legal Approach to AI Governance*

The paper argues that India's shift toward a techno-legal framework is presented as a technical choice, but it raises questions about the legitimacy of state decision-making. By moving rule-making from courts and legislatures to code and AI developers' compliance functions, it risks impairing essential procedural guarantees. A measured regulatory approach is therefore essential to foster technological innovation while protecting individual privacy and the security of sensitive personal information. Such an approach is fundamental to defending the integrity of democratic rights in an increasingly technological domain.

2 RESEARCH QUESTIONS

1. What is the "techno-legal" model of AI governance in India, and how does its "governance by design" approach differ from traditional command-and-control regulation and the EU's risk-tiered model?
2. How are the legal arguments associated with the technical architecture, and where can remedies for automated decisions be found?

3 DEFINING THE TECHNO-LEGAL MODEL

The techno-legal approach to AI governance can be defined as the amalgamation of legal instruments, rule-based conditioning, regulatory monitoring, and technical enforcement processes embedded in the

³ Id. Pg. 12

⁴ 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 O.J. (L 1689) 1.

⁵ Ministry of Electronics and Information Technology [MeitY], *India AI Governance Guidelines* (Nov. 5, 2025)

<https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf> (last accessed 17 July 2026)

technical architecture by design. In this research article, the authors analyse the intertwined AI governance models, which vary in scope and application as well as the presupposition of the structure of compliance. Some reflect a “governance by audit” paradigm, emphasising post-deployment documentation and oversight. In contrast, others adopt a “governance by design” approach, embedding legal and ethical obligations into the development lifecycle itself.

This paper also distinguishes India’s AI Governance Guidelines from the EU’s risk-tiered model. Although the Indian guidelines recognise the importance of risk assessment, they do not establish a detailed statutory risk-classification system like the EU AI Act. The EU AI risk assessment law distinguishes AI on the basis of risk creation. Chapter II, Article 5 deals with prohibited AI practices, while Chapter III, Article 6 identifies high-risk AI systems. High-risk systems are then subject to stricter legal requirements. The main problem with India’s present AI governance approach is not that it lacks principles of responsible and safe AI. The issue is that clear, legally enforceable rules do not support these principles.

India’s present principles-based approach does not provide a complete answer to every such situation. It recommends a graded liability system based on the function performed, the level of risk, and whether proper care was taken. It also recommends clearer responsibilities for different actors in the AI value chain. This paper explores the complications of AI governance and regulatory systems in India, highlighting that ambiguous accountability may give rise to considerable data threats in the country.

4 METHODOLOGY

The proposed research adopts a doctrinal and comparative approach, using normative analysis while deliberately excluding empirical fieldwork. Through a comprehensive and technical analysis of India’s primary policy and regulatory framework, i.e. the India AI Governance Guidelines, Office of the Principal Scientific Adviser white papers, the IT Amendment Rules 2026, the DPDP Act 2023 and the RBI FREE-AI report (2025), it aims to understand whether the ‘governance by design’ framework delivers ample security and does not risk the breakdown of essential procedural guarantees. The research article compares it with the European Union’s AI Act and the provisions on automated decision-making in the General Data Protection Regulation (GDPR). This analysis showcases the necessary components of a contestability-protective alternative within the context of emerging AI governance.

5 REALLOCATION OF RESPONSIBILITY IN AI GOVERNANCE – ANALYSING EU AND INDIAN AI REGULATION

5.1 EU AI Act – Binding Legislation

The EU AI Act is detailed legislation to monitor and control the detrimental effects of Artificial Intelligence. The EU AI Act prohibits certain uses of artificial intelligence (AI). Some AI systems are prohibited if they have been created to manipulate an individual’s decision-making, creativity and/or exploit vulnerabilities of individuals classified by their social behaviour and characteristics. Furthermore, the Act forbids the processing of facial recognition data and categorisation of individuals through biometric information, except when utilised for legitimate law enforcement objectives, such as locating missing persons or preventing acts of terrorism.⁶ Chapter III, Article 6 outlines the classification of high-risk AI systems used

⁶ Artificial Intelligence Act, art. 5, 2024 O.J. (L 1689)

as a product safety feature or as products themselves (Annex I). An Annex III system is exempt from high-risk classification only when it does not pose a significant risk to health, safety, or fundamental rights and meets the required criteria. The EU Commission is responsible for issuing guidelines and examples of high-risk and non-high-risk AI systems and further protecting the fundamental rights.⁷ Therefore, under Article 27, public bodies and private organisations engaged with public services must disclose how the system could impact people's fundamental rights by outlining risks associated with the system, and the further steps to be implemented in a high-risk situation. This assessment must be done for the first use of the system, but can be updated if necessary. Unless exempt, they must report their findings to the market surveillance authority using the template provided by the AI Office.⁸ The transparency of the high-risk AI system has been considered vital and must include clear information and instructions, identifying the system's capabilities and limitations, and any potential risks. The record-keeping of such data is important for the working mechanism of such systems.⁹ Article 50 states that companies must inform users when they interact with an AI system or use AI for emotion recognition or biometric categorisation, or create or alter content; the company must disclose this, unless it's for legal purposes or the content is artistic or satirical. The EU AI Act provides India and other such nations with a useful example of how broad principles such as safety, transparency, accountability and equity can be converted into specific legal obligations.¹⁰

5.2 India's AI Governance Guidelines (2025) – 'Light-Touch' and 'Seven Sutras'

In November 2025, the Ministry of Electronics and Information Technology (MeitY) unveiled guidelines for AI governance in India.¹¹ The guidelines are based on seven voluntary principles adapted from the RBI's FREE-AI Committee report¹² and apply across all sectors: Trust; People First; Innovation over Restraint; Fairness & Equity; Accountability; Understandable by Design; and Safety, Resilience & Sustainability. India's future leadership depends on the ability to set an example in governing AI with technical foresight, which guarantees safety and inclusivity. India's Guidelines describe themselves as a technology-agnostic, techno-legal framework built on voluntary measures, as set out in the Preface and reinforced by the "Innovation over Restraint" sutra.¹³ They further provide wider principles for responsible and safe AI, emphasising transparency and clarity. These principles are mere guidelines rather than strict sanctions like the EU's AI Act. They depend on existing legal mechanisms, which lack penalties and a compliance system.

5.3 Existing Legal Framework and Instruments in India

5.3.1 *Analysing DPDP Act and EU AI Act*

The EU AI Act regulates the development and deployment of artificial intelligence systems, emphasising risk-based classifications that dictate how AI is designed, tested, and utilised. The Act prioritises AI

⁷ Artificial Intelligence Act, art. 6, 2024 O.J. (L 1689)

⁸ Artificial Intelligence Act, art. 27, 2024 O.J. (L 1689)

⁹ Artificial Intelligence Act, art. 13, 2024 O.J. (L 1689)

¹⁰ Artificial Intelligence Act, art. 50, 2024 O.J. (L 1689)

¹¹ India AI Governance Guidelines, *supra* note 5.

¹² Reserve Bank of India, Committee on Framework for Responsible and Ethical Enablement of Artificial Intelligence, *Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI)* (13 August 2025), <https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=1306>. (last accessed 16 July 2026)

¹³ India AI Governance Guidelines, *supra* note 5, at pg. 12.

systems and their technical management rather than designing a product-safety framework on personal data involvement. The Act, compliance with which is overseen by the European AI Office and national authorities, applies to any AI system affecting the EU market, regardless of where it is developed. However, India's DPDP Act seems similar to GDPR¹⁴ when it is concerned with the collection, storage and processing of personal data focused on privacy, but limited to digital personal data. DPDP essentially focuses on personal rights and consent, mandating regulation over personal data through consent, access, and grievance redressal. The Data Protection Board of India (DPBI)¹⁵ enforces it, with appeals to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), and it applies to data processing outside India that targets individuals within the country. DPDP Act is based on consensual processing of lawful data and its violations invite the imposition of penalties; however, the EU AI Act lacks a consent regime and instead imposes notice and disclosure obligations for transparency. Its penalties follow a percentage-of-revenue model with minimum thresholds, tiered by severity of its violations. And it raises the question whether such frameworks focus on personal data protection or on transparent risk-management regulation.

5.3.2 *Analysing the IT Act, 2000 and the EU AI Act*

The IT Act, 2000¹⁶ was adopted to monitor digital governance, e-commerce and cybercrime. India has deviated from the global phenomenon of creating a separate AI Act – instead, it has chosen to adapt existing laws through reinterpretation and targeted amendments. Section 79 of the IT Act, which is the core provision, grants conditional immunity to intermediaries by exempting them from liability for third-party content, contingent on their passive role in data transmission. The IT Act's major drawback is the definition of 'intermediary' in Section 2(w)¹⁷, which might not sufficiently encompass AI systems that generate or modify content autonomously. The protections under the section are limited when applied to AI systems, raising doubts about liability for AI-generated outputs. The fines and punishments similar to the criminal law system under the Act are also restricted. The EU AI Act offers a multi-layered, approach-driven mechanism for AI regulation, with a risk-assessment model and strict enforcement obligations. The Indian IT Act functions within a wider digital governance framework that has yet to decisively address the complications caused by AI technologies.

5.3.3 *Analysing the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*

The clearest instantiation of the techno-legal method is found not in the Guidelines themselves but in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified on 10 February 2026 and brought into force on 20 February 2026.¹⁸ The Amendment introduces a statutory category of 'synthetically generated information' (SGI) — content that appears reasonably authentic but is algorithmically created, modified, or altered — and folds it into the

¹⁴ 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 O.J. (L 119) 1.

¹⁵ Digital Personal Data Protection Act, No. 22 of 2023, § 18 (India).

¹⁶ Information Technology Act, No. 21 of 2000, India Code (2000).

¹⁷ Information Technology Act, 2000, § 2(1)(w).

¹⁸ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Gazette of India, G.S.R. 120(E) (Feb. 10, 2026), amending the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

existing intermediary due-diligence regime.¹⁹ Intermediaries must ensure that such content is conspicuously labelled, that provenance metadata is embedded and preserved, and that users declare synthetic material at the point of upload; larger intermediaries that themselves enable the creation of synthetic content bear the heavier obligation of deploying automated detection.²⁰ Crucially, compliance is enforced through the conditionality of safe harbour under Section 79 of the IT Act rather than through any independent adjudicatory route: an intermediary that fails to meet these design obligations risks forfeiting the very immunity on which its operation depends. The Amendment is therefore a typical example of governance by design in which a legal obligation is translated into ‘the labelling, watermarking, and filtering’ layers of the platform, rather than into an adjudicable duty owed to an affected person. Yet it is here that the reallocation of authority this paper identifies becomes visible. The obligation runs between the State and the intermediary, and its currency is takedown speed — roughly three hours for unlawful content acted upon under a court order or government notification, and two hours for non-consensual intimate imagery.²¹ The individual whose likeness, voice, or data is processed is the object of protection but not a participant in it: she acquires no right to notice of an automated determination, no reasons, and no forum in which to contest either the classification of her content or the decision to act, or not act, upon it. What the technical architecture delivers efficiently — detection, labelling, removal — it delivers in place of, not alongside, the procedural guarantees that contestability requires.

5.4 India’s Law Plus Model

The Reserve Bank of India (RBI) FREE-AI Committee²² undertook the assessment of AI adoption in financial institutions and identified challenges to innovation and integration. The Committee asserted that there is a rise in AI’s transformative potential and associated risks, and it is important to review global governance approaches in financial services. The Committee recommended establishing a progressive framework that promotes ethical AI adoption in India’s financial sector. The Office of the Principal Scientific Adviser²³ paper endorses a techno-legal model that ensures AI technologies comply with national technical, legal, and ethical standards. This governance approach emphasises transparency, explainability, provability, and enabling conditions aligned with India’s constitutional values.

According to the India AI Governance Guidelines,²⁴ the goal is to encourage voluntary compliance rather than impose strict regulations. This balanced model unites mandatory legal baselines with voluntary guidelines to promote innovation—known as LAW PLUS.²⁵ By embedding legal obligations into the design and development phases of AI systems, this proactive approach ensures ongoing compliance. Therefore, clarity in AI development can increase investment, create new startups, and strengthen global leadership. The “Responsible AI by Design” principle will support large-scale adoption and encourage confidence in AI technologies.

But achieving enhanced inclusive AI requires systematised change across the full AI life cycle, including remedying structural imbalances in who develops, defines, owns, and governs AI systems. It also

¹⁹ IT Amendment Rules, r. 2(1)(wa)

²⁰ Id. at pt. II, sec. 3(2).

²¹ Id. pt. II, sec. 2(b).

²² Free AI Report, *supra* note 12.

²³ Office of the Principal Scientific Adviser (OPSA), *Strengthening AI Governance Through Techno-Legal Framework* (Gov’t of India, White Paper No. 2, Jan. 23, 2026)

²⁴ India AI Governance Guidelines, *supra* note 5.

²⁵ Id.

requires investments in AI capacity, infrastructure, and skills across countries and regions, as well as more representative data and benchmarks.²⁶

6 CRITICAL REVIEW OF INDIA'S SHIFT TOWARDS TECHNO-LEGAL AI GOVERNANCE

6.1 Assessment of the Effectiveness of the Techno-Legal Framework

Technologists design the basic infrastructure features that create and implement information policy defaults.²⁷ What Reidenberg highlighted three decades ago is still relevant in today's modern era – “technological developments outpace the rate of legal evolution. Consequently, today's regulations may easily pertain to yesterday's technologies. Second, today's technology may limit the ability of government to regulate.”²⁸ Koops and Leenes, when discussing data governance, reiterate that ‘hard privacy by design’ is challenging for determining legal regulations of data. Although simple and very specific rules may be suitable for hardcoding in IT systems, one cannot rely on building in legal requirements in the design of data-processing systems in such a way that compliance with ‘the’ data protection requirements and ‘the protection of the rights of the data subject’ is ensured.²⁹ As Scharf notes, ‘privacy by design orientated policy combined with privacy by design impeding legislation embodies a serious policy dilemma that makes it unrealistic to assume that privacy by design can be developed to its intended potential.’³⁰ How can one effectively regulate the governance of AI? The techno-legal framework has its own challenges. A recurring and important theme in scholarly and policy discussions focuses on the need to secure ‘algorithmic accountability’. But to understand what securing meaningful algorithmic accountability might require, it becomes important to gain a deeper understanding of algorithmic power.³¹ Thus, the most important question arises: How should accountability then be accomplished? Regulations could be derived from what Citron and Pasquale have referred to as “technological due process”—procedures ensuring that predictive algorithms live up to some standard of review and revision to ensure their fairness and accuracy.³²

In a discussion paper released in June 2018, NITI Aayog states the overarching goal for a national AI strategy as one which will “leverage AI for economic growth, social development and inclusive growth, and finally as a ‘Garage’ for emerging and developing economies.” NITI Aayog’s role goes beyond recommending a policy approach; it also includes implementation and deployment.³³ The techno-legal framework under India’s AI governance³⁴ is devoid of tangible compliance infrastructures, wherein legal requirements risk becoming symbolic, reinforcing inequality rather than accountability.³⁵ Voluntary AI frameworks shaped by dominant providers shift obligations and, instead of assuming ethical maturity,

²⁶ Independent International Scientific Panel on Artificial Intelligence, *Preliminary Report: Scientific Assessment of the Capabilities, Opportunities, and Risks of Artificial Intelligence* (2026), <https://www.un.org/independent-international-scientific-panel-ai/en/preliminary-report> (last accessed on 18 July 2026)

²⁷ Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 Tex. L. Rev. 553 (1997-1998) Pg. 20.

²⁸ Id. Pg. 35.

²⁹ Bert-Jaap Koops & Ronald Leenes, *Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the ‘Privacy by Design’ Provision in Data-Protection Law*, 28 Int. Rev. Law Comput. & Tech. 159 (2014).

³⁰ Id.

³¹ Karen Yeung, *Algorithmic Regulation: A Critical Interrogation*, 12 Reg. & Gov’t 505 (2018). Pg. 29.

³² Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).

³³ NITI Aayog, Nat’l Inst. for Transforming India, *National Strategy for Artificial Intelligence: #AIforAll* (2018)

³⁴ India AI Governance Guidelines, *supra* note 5.

³⁵ W. Holmes Finch & Marya Butt, *Gaps in AI-Compliant Complementary Governance Frameworks’ Suitability (for Low-Capacity Actors), and Structural Asymmetries in the Compliance Ecosystem—A Systematic Review*, 5 Journal of Cybersecurity and Privacy 101 (2025).

prioritise regulatory capture by those providers. For an AI governance structure to be effective, the framework thus must be grounded in legal obligations.

6.2 Identification of Gaps in Contestability and Remedy

The Organisation for Economic Co-operation and Development (OECD), an intergovernmental economic organisation focused on stimulating world trade, includes a right to contest in its recommendations on AI.³⁶ The right to contest decisions is central to due process. Indeed, other familiar due process protections—for example, transparency, notice, and the right to an impartial arbiter—serve to strengthen contestation rights.³⁷ A utilitarian argument for a right to contest AI decisions can take three forms:³⁸

1. May lead to increased acceptance of AI systems among individuals.
2. In major cases, for example, welfare benefits or child custody, process protections and contestations could prevent serious harm.
3. Even utilitarians might support individual process rights if AI decisions encroach on personal privacy.

In an ideal scenario, an impartial entity would be responsible for adjudicating disputes arising from AI decisions. This may be possible only in certain scenarios; for example, in the criminal justice system, defendants should have the opportunity to contest AI-driven decisions meaningfully before a judge. The GDPR incorporates both systemic governance measures and various individual rights for data subjects: transparency, notice, access, a right to object to processing, and, for those subject to automated decision-making, the right to contest certain decisions.³⁹ Furthermore, when AI is utilised in regulatory environments, constitutional due process may necessitate adjudication by a neutral party.⁴⁰ The increasing use of machine learning systems to make crucial decisions raises concerns about whether models can be fair and non-discriminatory. This seems intuitive and straightforward as a goal, but a number of complications arise in the context of fairness in AI systems.⁴¹ In other words, the contestability of AI recommendations increases the need for a check mechanism. The primary purpose of the EU AI Act and the GDPR is to protect fundamental rights, but they originate from different sources — regulation of product safety versus privacy protection. This difference leads to inconsistencies in implementation, particularly in lawful data processing, consent, and impact assessments. Key differences are: firstly, the AI Act's requirement for human oversight in high-risk AI systems (Article 14) versus the GDPR's restrictions on automated decision-making (Article 22). Secondly, GDPR's principles of data minimisation and purpose limitation may conflict with the data needs of AI models. And finally, the AI Act's vague definitions of fairness and non-discrimination further complicate its alignment with GDPR's more detailed individual rights.⁴² Scholars have often argued that instead of depending exclusively on static, audit-based mechanisms, these models should advocate for viewing compliance as an ongoing process—a dynamic system that adapts to technological advancements and the evolving capacities of organisations. It is apparent that

³⁶ Margot E. Kaminski & Jennifer M. Urban, *The Right to Contest AI*, 121 Colum. L. Rev. 1957 (2021). Pg. 1963.

³⁷ Id. Pg. 1974.

³⁸ Id.

³⁹ Id.

⁴⁰ Id. Pg. 2039.

⁴¹ Vidushi Marda, *Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making*, 376 Phil. Trans. R. Soc. A 20180087 (2018) Pg. 09

⁴² Emmanuel Kwasi Abrokwa, *Does the GDPR Impede AI Progress? A Critical Analysis* (May 29, 2026). Available at SSRN: <https://ssrn.com/abstract=7119642> (last accessed on 20 July 2026)

effective AI governance for regulation may necessitate compliance infrastructures that develop alongside institutional capabilities, rather than requiring immediate and comprehensive implementation.

We need to create a meaningful right to contest AI, but it must be carefully designed to succeed. There is no single approach; legislators can start with different archetypes and refine them to avoid pitfalls. Contestation is influenced by various factors such as notice, reasoning, substantive law, and incentive structures. A successful contestation mechanism must consider not only the algorithm but the entire decision-making system—human, machine, and organisational—along with the legal framework.

A remedy for an automated decision within the Indian framework requires assembling one from instruments not designed for the purpose, and the exercise exposes the gap the paper diagnoses. The Digital Personal Data Protection Act, 2023 confers a right of grievance redressal against a data fiduciary and channels unresolved complaints to the Data Protection Board of India, with an appeal to the Telecom Disputes Settlement and Appellate Tribunal.⁴³ But the Act contains no analogue to Article 22 of the GDPR: it creates neither a right against solely automated decision-making nor a right to an explanation of one, so the data principal may complain about how her data was handled but cannot demand reasons for, or contest the logic of, the decision that data produced.⁴⁴ The intermediary route is narrower still. Section 79 of the IT Act immunises the intermediary rather than empowering the affected person, and its safe harbour presupposes a passive conduit — an uneasy fit for systems that generate or determine outcomes autonomously.⁴⁵ The residual avenues are general and ill-suited: grievance redressal under the Consumer Protection Act, 2019 treats the harm as a defect in a service rather than as a contested exercise of decisional power, and the constitutional writ jurisdiction under Articles 32 and 226 reaches state action but not, ordinarily, the private developers and deployers to whom the techno-legal model delegates the operative choices.⁴⁶ Set against the contestability baseline of notice, reasons, and adjudication before a neutral arbiter,⁴⁷ India's architecture offers redress for data and for content while leaving the automated decision itself substantially unreviewable. The EU's pairing of a human-oversight obligation for high-risk systems (Article 14 of the AI Act) with an individual right in respect of automated decisions (Article 22 of the GDPR) is not advanced here as a template to be copied; it simply marks the distance between a framework that anticipates contestation and one that, by embedding governance in design and leaving remedy to pre-existing and general law, does not.

6.3 How Can India Remedy the Issues under Its AI Governance?

AI has increased large-scale production of targeted content, which is often misleading and undermines the integrity of information and weakens public trust, social cohesion, and democratic discourse. Cyber-criminals use AI for cyberattacks, disproportionately impacting vulnerable groups. The growing gap between advancing AI capabilities and effective risk management could lead to serious consequences. In Article 22, the GDPR dictates that for certain automated decisions, affected individuals must be provided “at least the right to obtain human intervention . . . to express his or her point of view and to contest the

⁴³ Digital Personal Data Protection Act, No. 22 of 2023, §§ 13, 18, 29 (India).

⁴⁴ Regulation (EU) 2016/679, art. 22, Digital Personal Data Protection Act, No. 22 of 2023 (India) (containing no equivalent right against automated decision-making). See also Kaminski & Urban, *supra* note 36.

⁴⁵ Information Technology Act, No. 21 of 2000, §§ 2(w), 79 (India).

⁴⁶ Consumer Protection Act, No. 35 of 2019 (India); India Const. arts. 32, 226.

⁴⁷ Kaminski & Urban, *supra* note 36, at pg. 1974.

decision.”⁴⁸ The right to contest goes beyond rectifying incorrect data that concludes a decision. The right to contest must be held to higher standards of not just correction, but regulation of personal rights. The HEW Report⁴⁹ published over 50 years ago contemplated the conception of ‘data privacy’ and data disclosure and concluded that affected individuals should have some agency in deciding “the nature and extent of such disclosure.” These findings are still relevant today, in the context of AI – individual rights and the right to contestability will lead to better governance of modern information systems. As the Independent International Scientific Panel on AI report⁵⁰ highlights, growing disorder in global governance is observed, with some countries having introduced AI-specific legislation with fundamentally contradictory rules and compliance costs. Jurisdictions exhibit divergent regulatory philosophies, with no unified risk-management mechanism, no comparable evaluation standards, and limited cross-jurisdictional coordination, risking a fragmented regulatory landscape.⁵¹ Hence, the inadequate, highly autonomous AI systems have necessitated the evolution of reliable methods for retaining control. Decisions that affect people’s lives implicate dignity. Categorising individuals arguably objectifies them; affording a right to contest that categorisation restores at least some form of dignity.⁵² An example of such contestation could look like – “An individual shall have a right to contest, as under the due process clause.” Lawmakers should ensure that the implementation anticipates and closes foreseeable loopholes. To achieve comprehensive and inclusive AI governance, India must incorporate systemic changes not only to tackle structural imbalances (related to developers, rulemakers, and owners) but also to build capacity, invest in AI, and share infrastructure and knowledge across regions.

7 CONCLUSION

Pasquale correctly identifies that transparency alone does not always produce either redress or public trust in the face of institutionalised power or money.⁵³ After analysing multiple sources, the authors conclude that AI compliance exists along a non-linear range rather than a binary one. It has to exist on a spectrum from stringent legal effectiveness to aspirational ethics-based governance. India is yet to adopt a comprehensive legal framework for AI governance; the ‘techno-legal’ approach is highly ambiguous and requires essential reviews and checks. Amendments to the existing legislation could bridge the gap and foster innovation; however, a ‘whole-of-government approach’ could create a better resolution to the current shortcomings. Regulators must implement robust model governance mechanisms covering the entire AI model lifecycle, including model design, development, deployment, and decommissioning. Regulators must also invest in training and institutional capacity-building initiatives to ensure that they possess an adequate understanding of AI technologies and to ensure that the regulatory and supervisory frameworks match the evolving landscape of AI, including associated risks and ethical considerations. As discussed in detail, the right to contest AI should apply to high-risk sectors, and it must not be limited to decisions made solely by AI but also to human decisions that rely on AI. Many find AI systems opaque and worry that autonomous decisions made by these systems will be inexplicable and have unintended

⁴⁸ Regulation (EU) 2016/679, art. 22.

⁴⁹ Secretary’s Advisory Committee on Automated Personal Data Systems, U.S. Dep’t of Health, Education & Welfare, Pub. No. (OS) 73-94, Records, Computers and the Rights of Citizens (1973).

⁵⁰ Independent International Scientific Panel Report, *supra* note 26.

⁵¹ *Id.*

⁵² Christopher McCrudden, *Human Dignity and Judicial Interpretation of Human Rights*, 19 Eur. J. Int’l L. 655 (2008).

⁵³ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 8, 16 (2015).

consequences. They are concerned about the unethical sourcing of data and that these systems could be used for harmful activities. Therefore, there is an impending need for immutable audit trails and transparency in automated systems, which allow individuals to understand and challenge inaccuracies, and individuals under the ‘due process clause’ become entitled to reasonably calculated notice when governmental systems make adverse decisions. Fostering trust by maintaining transparency and safety could be achieved solely via ethical AI adoption that respects rights and upholds fairness. A technology, no matter how powerful, will only be adopted if people trust it. Overall, AI regulations need to be flexible, coordinated, and constantly updated to advance innovation while protecting human rights, consumer protection, and ethical values.

* * *