RESEARCH PAPER

Legal Challenges of Generative AI in India: Scope and Limitations of the IT Act, 2000

Arpita Mishra[a*], Dr. Monica Yadav[b], Dr. Pooja Batra Nagpal[c]

[1*] *Research Scholar at IILM University, Gurugram, Email: arpitamish09@gmail.com*
[2] *Professor of Law at IILM University, Gurugram, Email: monica.yadav@iilm.edu*
[3] *Associate Professor at IILM University, Gurugram, Email: poojanagpal@iilm.edu*

Abstract
The large language models, image and audio portent creators and generative Artificial Intelligence (gen-AI) introduce fresh legal, ethical and regulatory issues. The Information Technology Act, 2000 (IT Act) is the main instrument of cyber-law in India, and it was created long before the appearance of gen-AI and, as such, has no provisions specifically aimed at the regulation of the algorithmic generation, synthetic content, or mass-scale model training. The current gen-AI risks, such as in the data protection, intermediary liability, deepfakes, misinformation, are critically discussed in this paper in their interaction with the current cyber-legal framework in India, which is the IT Act and associated rules. It considers the conformity of the statutory text to technological realities at the time, surveys concomitant legal development especially the Digital Personal Data Protection Act, 2023 as well as examines recent policy initiatives of the NITI Aayog strategy and MeitY AI governance guidance. There are specific legislative and regulatory reforms, the amendments of the intermediary rules, AI-specific duties of care, the mandated transparency and audit requirements, sectoral sandboxes, and enhanced data governance that are provided in the paper to adjust the IT Act era framework to the needs of the gen-AI and not to undermine innovation and digital inclusion.

Keywords: *Generative AI, Information Technology Act, Intermediary Liability, Data Protection, India, MeitY, NITI Aayog*

How to cite this article: Mishra A, Yadav M, Nagpal PB. Legal Challenges of Generative AI in India: Scope and Limitations of the IT Act, 2000. Int J Drug Deliv Technol. 2026;16(10s): 331-339; DOI: 10.25258/ijddt.16.10s.45

1. Introduction

Gen-AI systems (hereafter, gen-AI) have the ability to produce scaleable human-like text, realistic images, audio, and other artefacts. They increase the potential to innovate in law, medicine, education and services but increase the threat of automated misinformation, futile reputational damage brought about by deepfakes, abuse of copyright-protected works, breach of privacy brought about by the use of training datasets, and anonymous decision-making, which undermines accountability.[1] These trends challenge the traditional legal typologies as in who to blame when a model comes up with a defamatory text? Who is it, the model builder, the uploader, or the intermediary when a harmful synthetic video is posted on a platform?[2]The most important law in India concerning cyber activities and the intermediary liability is the Information Technology Act, 2000 (IT Act) that provides an exemption of the liability to the intermediaries provided that they comply with the procedural and content-removal liability requirements.[3]

Meanwhile, India has been working on complementary schemes to regulate information of the Digital Personal Data Protection Act, 2023 and AI in addition to policy and direction of NITI Aayog and MeitY, which are directly connected to gen-AI governance. The question posed in this paper concerns the extent to which the IT Act and corresponding Indian cyber-law architecture is sufficient to regulate generative AI and to what extent do reforms to curb the downsides of gen-AI and encourage positive innovation? The paper continues as follows where under part 2 gives a brief legal and policy context, intermediary regime of the IT Act, recent data privacy legislation, and national AI strategy and guidance. Part 3 aligns gen - AI technical issues with legal issues like data, IP, intermediaries, criminal abuse, platform regulation, algorithmic harms. Part 4 examines the doctrinal fit and lapses of the IT Act and the related instruments. Part 5 provides reforms plans including the legislative amendments, regulatory forms, procedural

[1] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin's Press, 2018).

[2] Shreya Singhal v. Union of India, (2015) 5 SCC 1; Information Technology Act, 2000, § 79 (India); Ministry of Electronics and Information Technology, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*; United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (2021).

[3] Information Technology Act, 2000, §§ 2(w), 79 (India); Shreya Singhal v. Union of India, (2015) 5 SCC 1.

*Author for Correspondence: aarpitamish09@gmail.com

protection and the enforcement forms and ends with effective directions and research priorities.

International law has no way to separate the normative architecture of generative artificial intelligence governance.[4] Many years before the emergence of algorithmic systems, there were international conventions with formulations of general principles that tried to restrain power whether in the form of states, markets, or technology and to maintain the pre-eminence of human dignity.[5] Generative AI is the era where these conventions are gaining a new meaning, as they serve as moral and legal grounding in a more automated world. There is currently not a binding and encompassing international convention on artificial intelligence, but a network of human rights traditions, data protection and other data protection tools, labour standards, and ethical codes jointly makes up an international jurisprudence of AI humanisation.[6]Tasks of these instruments are not to control AI; they are to control human implications of the technological power, thus defining the contours of the legitimate AI governance.

2. International Conventions and the Humanisation of AI Governance

The normative baseline against which the AI systems should be considered is rights to privacy, freedom of expression, equality before the law, and protection against arbitrary interference. These rights are directly implicated by generative AI systems, which can generate speech, images and stories. Automated content generation has the potential to sway the opinion of the population, control behaviour, and construct identity in a manner that endangers autonomy and freedom of thought.[7] In the global human rights view, outsourcing the expressive and decision-making processes to obscure algorithms is a threat to the weakening of individual agency, and consequently, the existence of democratic society itself. The international human rights jurisprudence, therefore, requires that AI systems must be subordinate to human judgment, which, in turn, supports the idea that machines may be helpful, but they should never substitute the human moral judgement.[8]

Privacy has been established as a fundamental pillar of personal dignity in the European Convention on Human Rights (Article 8) and in the case law of the European Court of Human Rights.[9] This knowledge has also been put into practical use by the General Data Protection Regulation (GDPR) that has become a de facto international standard in data management. Within the framework of generative AI, such principles highlight the principle of informational self-determination, which is to state that people should have the right to control the collection, use, and manipulation of their personal information. It is this principle that AI training practices founded on blind data scraping dispute, especially in the situation when personal data is repurposed, in an irrevocably opaque and globally distributed way. International data protection guidelines therefore support the importance of transparency, consent, limit of purpose and accountability of AI systems not as a neutral input, but as a mirror of lived human experience.[10]

The Convention on the Elimination of Racial Discrimination of All Forms (1965) and the Convention on the Elimination of Discrimination against Women (1979) are international conventions, which have positive commitments to states to ensure that they are not involved in systemic discrimination. These apply to digital systems that recreate or magnify historical injustices. Generative AI models that have been trained on biased data are prone to reinforce exclusion on a scale as well as perpetuate stereotypes. Algorithms bias is a type of structural discrimination, according to the jurisprudence of international equality, despite the deficiency of bad motives.[11] Humanised AI governance as such involves active steps to identify, address and correct bias, so that technological regimes may serve to promote substantive equality, but not formal neutrality.

Rights to work, education and fair conditions of employment have been acknowledged by the International Covenant on Economic, Social and Cultural Rights (1966) and conventions of the

---

[4] United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021); United Nations General Assembly, *Report of the Secretary-General: Roadmap for Digital Cooperation* (UN Doc. A/74/821, 2020); NITI Aayog, *National Strategy for Artificial Intelligence: #AIforAll* (Government of India, 2018).

[5] Universal Declaration of Human Rights, 1948; International Covenant on Civil and Political Rights, 1966; International Covenant on Economic, Social and Cultural Rights, 1966.

[6] United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021); United Nations General Assembly, *Roadmap for Digital Cooperation* (UN Doc. A/74/821, 2020); International Labour Organization, *Work for a Brighter Future – Global Commission on the Future of Work* (ILO, 2019); General Data Protection Regulation (EU) 2016/679.

[7] United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).

[8] United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021); International Covenant on Civil and Political Rights, 1966, arts. 18–19.

[9] European Convention on Human Rights, 1950, art. 8; *S. and Marper v. United Kingdom*, App. Nos. 30562/04 & 30566/04 (Eur. Ct. H.R., 2008).

[10] Organisation for Economic Co-operation and Development (OECD), *OECD Principles on Artificial Intelligence* (OECD, 2019); General Data Protection Regulation (EU) 2016/679, arts. 5, 6 & 22.

International Labour Organization (ILO). By automating cognitive and creative labour, generative AI brings up some significant questions concerning displacement, deskilling and the future of human work. The international labour standards affirm that technological advancements should promote human good and not alienate employees. This principle extends to a responsibility of states to carefully control AI implementation in a manner that facilitates reskilling, fair access, and social safeguards, especially in the developing economies where digital inequalities are still significant.[12]

The most explicit statement of human-centred AI governance on the international level is the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021). The Recommendation adopted by UNESCO member states in 2013 is a unanimous decision that combines the human rights law and the development ethics as well as the democratic governance in a unified normative framework.[13] It stipulates that AI systems must uphold human dignity, be transparent and explainable and be open to human control. Most importantly, it cautions against the loss of human agency to automation stating that the outcomes of AI can always be traced to natural or legal entities.

This principle is controversial to generative AI because it emphasizes the disposition to view algorithmic outputs as autonomous or value-neutral. The disruptive nature of AI technologies is becoming an acknowledged part of the international humanitarian environment and the new discourse of security. Deepfakes, psychological operations and information warfare are some of the ways in which generative AI can be weaponised, harming democratic institutions and public trust. Although the current conventions like Geneva Conventions do not specifically mention AI, such principles as distinction, proportionality, and accountability are still applicable. The humanised AI governance implies that states must be cautious and accountable as such that the technological innovation does not weaken democratic resilience and international stability.

In the perspective of the international conventions, the Indian effort to regulate the generative AI via the Information Technology Act should be interpreted within the wider legal tradition of human rights.[14] But policy purpose is not enough to be aligned to international norms, it involves internalising human-focused principles to enforceable legal norms. International values, including dignity, equality, accountability, and transparency, embedded in domestic AI regulation would see to it that India has not just a system of digital governance that responds to the technological change, but also a system that would collaboratively work with the rest of the world project of humanising artificial intelligence.[15] International conventions teach us that law is not finally devoted to innovation as such, but rather to the safeguard of human values against the concentration of power. When it comes to regulating generative AI, states have the difficult task not only to regulate machines, but to confirm the central position of human beings in the law.

3. Law and Policy History: A Jurisprudential Approach

3.1 IT Act and the Jurisprudence of Intermediary Liability

Information Technology Act, 2000 is the initial statute in India which is a legislative response to the issue of digital communication and governance of cyberspace. The IT Act is jurisprudentially based on a instrumentalist conception of the internet in which intermediaries are perceived as neutral facilitators, as opposed to normative actors.[16] This is in line with classical legal positivism whereby liability is based on human agency and intentional acts and not on automated-algorithms. Section 79 of the IT Act realises this philosophy by means of the theory of conditional immunity, which gives intermediaries a safe harbour against liability relating to third-party content, assuming that they meet the requirements of statutory due-diligence.[17] The provision is a compromise between two conflicting jurisprudential issues: (i) the necessity to maintain freedom of speech and creativity in the online world, and (ii) the need to avoid the harm resulting due to illegal content online. This statutory system has been gradually

[12] International Labour Organization, *Work for a Brighter Future: Global Commission on the Future of Work* (ILO, 2019); International Covenant on Economic, Social and Cultural Rights, 1966, arts. 6–7; United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021).

[13] United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021).

[14] Universal Declaration of Human Rights, 1948; International Covenant on Civil and Political Rights, 1966; United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021); Information Technology Act, 2000 (India).

[15] Universal Declaration of Human Rights, 1948; International Covenant on Civil and Political Rights, 1966; United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021); Organisation for Economic Co-operation and Development, *OECD Principles on Artificial Intelligence* (OECD, 2019).

[16] Information Technology Act, 2000, §§ 2(w), 79 (India); *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

[17] Information Technology Act, 2000, § 79 (India); Information Technology (Intermediary Guidelines) Rules, 2011.

subject to judicial interpretation in the introduction of constitutional values. Courts have stressed that the intermediary immunity is not absolute and has to be construed with reference to the Article 19(1)(a) and the reasonable restrictions.

As a result, the intermediary has been redefined as a rather controlled gatekeeper with restricted responsibilities of being vigilant and responsive. This is the basic jurisprudential pillar that Generative AI is destabilizing. AI-based platforms are not passive carriers or distributors of content; they produce expressive outputs in an autonomous way, which endangers the anthropocentric presumption of the Section 79.[18] Conventional teachings of fault, knowledge, and intent are conceptually fragile when the product of the content is the result of probabilistic models as opposed to human cognition. This begs a deeper jurisprudential question, one that, in turn, is deemed to have been addressed by this case: Is it possible to use the liability regimes, which were created to regulate human speech, to control machine-generated expression?[19]

3.2 Data Protection, Informational Autonomy and the DPDP Act, 2023

The introduction of the Digital Personal Data Protection Act, 2023 is an important change in the Indian legal thinking in terms of the acknowledgment of informational autonomy as a part of individual dignity. The DPDP Act is jurisprudentially based on the rights-based definition of privacy of action by the Supreme Court, personal data is not only an economic asset, but an extension of the personality of the individual. The Act proposes a fiduciary model of data management, which puts responsibilities of care, purpose limitation, and security on the data fiduciaries. This model is a variant of trust-based regulatory approach, according to which the entity that handles personal data is supposed to act in the best interests of the data principals.[20]

This kind of approach is especially applicable when it comes to generative AI, which is based on big-data aggregation and inferential analytics. On the jurisprudential perspective, the use of generative AI makes it difficult to use the traditional paradigm of data protection which focuses on consent. Training datasets can be indirect or historical data or scraped data, and it is questionable whether meaningful consent is a realistic possibility to achieve. Also, the reuse of personal information to train models undermines the principle of purpose limitation, since the downstream applications of AI-generated outputs can be unexpected and unforeseen. The dynamic regulatory framework stipulated under the DPDP Act is, therefore, in a liminal position between protection of rights and pragmatism in technology. It may lay down critical principles but its usefulness in addressing AI-specific evils will rely upon interpretive direction, subordinate law and executive regulator readiness to modify data protection jurisprudence to the realities of machine-learning systems.[21]

3.3 National AI Strategy, MeitY Guidance and Jurisprudence of Risk Governance

The regulation of AI in India can be perceived in terms of risk governance jurisprudence, and not as a command-and-control regulation approach. The National Strategy on Artificial Intelligence by NITI Aayog is based on the vision of AI to All with the principles of distributive justice, social inclusion, and developmental equity. This is a sign of a welfarist and utilitarian legal philosophy, in which a technological progress is attributed to the social good of the whole.[22] Simultaneously, the focus on the responsible AI is accompanied by normative limitations based on the constitutional morale, equity, and responsibility. Indian AI policy does not involve the codification of strict legal taboos, but instead takes the form of principles-based approach, which prefers ethical principles, voluntary adherence and capacity building of institutions. This is in line with the contemporary regulatory theory, which promotes responsive regulation, where the norms can change with technology. This jurisprudential orientation is operationalised in new guidelines by MeitY as part of IndiaAI Mission in which it proposes risk classification, transparency requirements and redress grievances. Such actions implicitly acknowledge that not every AI system is equally dangerous and should be regulated in accordance with the possible harm. The ability to shape the discourse of people, their personal choices, and the functioning of democracy makes generative AI an area to be regarded with a closer emphasis as a high-impact technology that needs more attention.[23] Nonetheless, the use of soft law creates a jurisprudential issue of legitimacy, enforceability and accountability. Without a legal obligation, ethics are at the risk of remaining a dream. Lack of legal implications of non-deployment can make

[18] Information Technology Act, 2000, § 79 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

[19] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637; Information Technology Act, 2000, § 79 (India).

[21] Digital Personal Data Protection Act, 2023 (India); Ministry of Electronics and Information Technology, *Explanatory Note on the Digital Personal Data Protection Bill, 2023*; Justice B.N. Srikrishna Committee, *Report of the Committee of Experts on a Data Protection Framework for India* (Government of India, 2018).

[22] Jeremy Bentham, *An Introduction to the Principles of Morals and Legislation* (Oxford University Press, 1789); NITI Aayog, *National Strategy for Artificial Intelligence: #AIforAll* (Government of India, 2018).

[23] United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021); European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM(2021) 206 final.

the normative power of Responsible AI frameworks more watered down, especially in high-risk deployments.

All these points together represent a jurisprudence of transition, neither overly optimistic of technology nor overly protective of regulation over the generative AI sector, in India. The IT Act represents an early liberal understanding of the digital freedom; the DPDP Act indicates a rights-based shift to informational dignity and AI policy tools include a risk-disposed governance philosophy.[24] However, generative AI reveals the conflict between these models. In autonomous content production challenges the human-centred liability frameworks, deep learning challenges the consent-led privacy principles, and soft law challenges the boundaries of regulatory legitimacy. Such tensions lead to the necessity of a consistent jurisprudential reconsideration of digital regulation something that redefines responsibility, agency, and accountability in the age in which machines are gaining growing involvement in spaces of normativity once played by humans. The next section will cover the topic of arbitrary dimensionless currency ratios. The following section will discuss the issue of arbitrary dimensionless currency ratios. The conceptual flaws of the current legal systems are especially clear once analyzing the practical damage and regulation issues created by generative AI, which is why the deficiencies in the doctrines and their enforcement in the modern Indian cyber legislation should be discussed in greater detail.[25]

4. Critical Analysis: Generative AI Regulation in India Jurisprudential Fault Lines

The general issue of regulatory challenges of generative artificial intelligence reveals fundamental jurisprudential weaknesses in the Indian system of cyber-law, especially the Information Technology Act, 2000.[26] On a fundamental level, the IT Act is based on a reactive model of liability that is human-centric and assumes that such aspects as content creation, intent, and harm can be attributed to distinguishable human agents.[27] Generative AI subverts this premise by creating autonomous and probabilistic systems that can generate expressive, advisory and decision-influencing outputs without active human authorship. This transformation makes the doctrines of fault, knowledge and causation more and more inadequate, and a structural imbalance is uncovered that exists between legal categories designed around human agency and technological systems that are characterised by a sense of non-transparency and scope. Under jurisprudential perspective, the intermediary safe-harbour in Section 79, is a liberal adherence to free-speech and innovation, which is based on a philosophy of minimal-intervention.[28] Nevertheless, this doctrine presupposes the intermediaries as passive pipelines, which fails when the platforms passionately design, train, deploy, and monetise generative AI systems.[29] The insistence of the law on reactive takedown mechanisms to the detriment of the victims lays the load of harm mitigation on the victims thus favoring the longuit of the invention over the longuit of dignity and safety. Practically speaking, the safe-harbour doctrine, when interpreted without reflection as applied to generative AI, stands to become a defence of structural irresponsibility instead of taking on the role of supporting digital freedom. This crisis of legal coherence is further enhanced by the problem of attribution. The concept of authorship has been used to explain the connection between harm and accountability in jurisprudence and Artificial intelligence disconnects this bridge.

Outputs do not have a legally recognisable author, but they have real-life impacts- defamation, fraud, discrimination and harm to consumers.[30] The lack of mandatory provenance systems, like model logging or watermarking, indicates a laissez-faire attitude on the part of regulations on imposing ex ante burdens on the developers of technologies. This exclusion comes at the expense of the rule of law per se because enforcing it without being traceable turns into a mere symbolic gesture instead of a substantive one. Another normative tension is depicted by data governance. The DPDP Act, 2023 is a rights-based twist in Indian jurisprudence, in which informational privacy is an element of dignity and autonomy.

---

[24] Information Technology Act, 2000 (India); Digital Personal Data Protection Act, 2023 (India); NITI Aayog, *National Strategy for Artificial Intelligence: #AIforAll* (Government of India, 2018); Ministry of Electronics and Information Technology, *IndiaAI Mission – Responsible AI Framework* (Government of India)

[25] Information Technology Act, 2000 (India); *Shreya Singhal v. Union of India*, (2015) 5 SCC 1; Ministry of Electronics and Information Technology, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*; NITI Aayog, *National Strategy for Artificial Intelligence: #AIforAll* (Government of India, 2018).

[26] Information Technology Act, 2000 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Justice B.N. Srikrishna Committee, *Report of the Committee of Experts on a Data Protection Framework for India* (Government of India, 2018).

[27] *Avnish Bajaj v. State (NCT of Delhi)*, (2008) 150 DLT 769 (Del. HC); Information Technology Act, 2000 (India), §§ 2(w), 79.

[28] *MySpace Inc. v. Super Cassettes Industries Ltd.*, (2017) 236 DLT 478 (Del. HC); Information Technology Act, 2000 (India), § 79.

[29] *Christian Louboutin SAS v. Nakul Bajaj*, (2018) 253 DLT 728 (Del. HC); Information Technology Act, 2000 (India), § 79; Ministry of Electronics and Information Technology, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*.

[30] United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021).

However, the acceptance-driven framework of data protection law is put into question by the training of generative AI practice. Individual consent as a meaningful protection in algorithmic ecosystems is revealed to be constrained by large-scale data ingestion, typically through the scraped or repurposed personal data. The absence of the law regarding the harms of inferential and model-generated personal data generates a void in the regulations whereby the protection of privacy is not proactive and structural but retrospective and fragmented. The same case with the intellectual property law by indicating doctrinal indeterminacy. The undecided position of AI training under fair dealing principles is a symptom of a more fundamental jurisprudential quandary, to which is whether creativity and originality are in the digital age solely human qualities. The Indian copyright legislation is based on human authorship and it finds it difficult to comply with machine-generated products which imitate, reorganize, or fuse protected work. As much as this ambiguity is death to innovation, it is also a destabilising force to the moral underpinnings of copyright traditionally, which strike a balance between incentive, labour and public interest. The end result of these loopholes is a regulatory ecosystem that regulates the outcomes rather than the causes. Indian law regulates AI wrongs only when they come to fruition, and it is based on post hoc actions in criminal law, consumer protection laws, or constitutional litigation.[31]

On a constitutional plane, Article 19(1) a) provides the freedom of speech and expression, which has traditionally been interpreted as a continuation of the human agency and autonomy. This freedom was designed by the intermediary safe-harbour of the IT Act Section 79, which does not allow too much censorship, but rather free digital discussion. But this protection is normatively problematic when it is put in the context of generative AI systems. Speech generated by machines has not been produced by human conscience or through democratic discussion, but it could affect the opinion of people, control the discourse of elections, and corrupt the truth at scale. Applying human protections on speech to autonomous systems would be tantamount to drain the democratic justification of Article 19 itself.

The liability regime is the reactive takedown based on the IT Act, which means that the liability is imposed upon the victims after damage has been done, as opposed to the proportionality requirement of the constitution. Jurisprudence on proportionality requires restrictions to be found necessary, effective and least intrusive. A purely reactive regime, which is unable to stop predictable AI-based harms, including deepfakes or automated misinformation, fails this test, which makes constitutional protections unequal, i.e., strong in favor of platforms and weak in favor of individuals.[32] The difficulty is compounded by Article 21, which enshrines the right to life and personal liberty and which is interpreted by the Indian courts to mean dignity, privacy and informational self-determination. Generative AI models that learn on large and frequently obscure datasets are causing significant questions of dignity blunting. AI systems may represent, recreate, or simulate individuals without their consent or knowledge and degrade human identity to a data abstraction.[33] Although the Digital Personal Data Protection Act, 2023 is a rights-affirming change, its consent-based model fails to address the issue of inferential harms and presents a second use of secondary data as an inseparable part of AI training. The outcome is that a type of structural invisibility is created in which individuals are influenced by AI systems but are not legally acknowledged as rights-bearing subjects in those systems. In the context of Article 14 which ensures equality before the law, generative AI brings in algorithmic discrimination, diffuse, systemic and usually unintentional. Conventional jurisprudence of equality is used to deal with the outcome of discriminatory results based on post hoc adjudication, whereas generative AI is inherently biased during the design and training phases.[34]

The IT Act has provided no tool of algorithmic audit, bias testing or pre-deployment impact assessments. Such regulatory silence permits discriminatory results to exist under the appearance of technological neutrality and dilute substantive equality and enhance socio-economic status quos. This regulatory failure is jurisprudentially indicative of adherence to legal positivism, in which the law responds to recognizable breaches instead of predicting the risk to the system.[35] Generative AI requires the transition to preventive and purposive jurisprudence, consistent with the internal morality of law proposed by Fuller, the focus on coherence, clarity, and concordance between rule-making and social reality. Only when they come into reality, a legal regime which regulates AI is harmful because it is neglecting this internal morality by allowing predictable harm by regulatory permissiveness. The uncertainty of the intellectual property also brings out normative tensions.[36]

---

[32] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637; *Shreya Singhal v. Union of India*, (2015) 5 SCC 1; Information Technology Act, 2000 (India), § 79.

[33] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1; Digital Personal Data Protection Act, 2023 (India); United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021).

[34] *D.H. and Others v. Czech Republic*, App. No. 57325/00 (Eur. Ct. H.R., 2007); United Nations Committee on the Elimination of Racial Discrimination, *General Recommendation No. 14: Definition of Racial Discrimination* (1993); United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021).

[35] H.L.A. Hart, *The Concept of Law* (2nd edn., Oxford University Press, 1994); Information Technology Act, 2000 (India).

[36] Lon L. Fuller, *The Morality of Law* (Rev. edn., Yale University Press, 1969); Information Technology Act,

The copyright law, which is rooted in the human creativity and labour theory, is inadequately prepared to manage machine-generated products that seem to be between originality and reproduction. The lack of transparency in fair dealing in AI training does not only frighten innovation, but also the very foundations of the moral rationalisation of copyright itself are upset. Once machines have offered a scale of imitation of creative labour, the law has to address whether protection is available to incentivize human creativity, promote its distribution or simply maintain market power. The sum total of this lack of doctrines is a system of governing where economic innovation is more important than constitutional loyalty. Soft-law components, policy advisories and voluntary ethical guidelines, though normatively attractive, are not enforceable or democratically acceptable.

They endanger to turn constitutional rights into idealistic ideals instead of making them a fetter on the power of technology. In this regard, what is happening in India can be described as a kind of colonisation of the lifeworld by systems by Habermas in which technical rationality has replaced normative reasoning. To balance the ideas of innovation and constitutionalism, India needs to shift to a more human-focused, proactive regulatory approach, which would incorporate the constitutional values in the structure of generative AI regulation. It would mean reinventing the notion of intermediary liability and giving affirmative responsibilities to AI creators, enforcing transparency and auditability, and acknowledging algorithmic harm as a separate form of legal injury. Otherwise, the law will be a silent onlooker in an automated society instead of being a vigilante that upholds human dignity, equality, and democratic integrity.

What was glaringly missing is a preventive jurisprudence, that is, a requirement of safety-by-design, algorithmic responsibility and proportionate risk evaluation at the time of technological manufacture. The system of soft-law guidance and policy advisories, though being flexible, implies questions of democratic legitimacy and enforceability especially in the high-risk AI deployment.

Finally, the generative AI regulation in the form of the IT Act indicates a jurisprudential change in progress, yet unfinished. The Indian cyber law is at a junction of instrumental governance based on economic growth and innovation and normative constitutionalism based on foresight of dignity, equality and accountability. Unless the legal doctrine is recalibrated to acknowledge machines as disruptive normative forces, instead of neutral mechanisms, the law risks falling behind the technology in a manner that undermines public trust, support of rights and disperses the regulatory imperative. What is being proposed as a jurisprudential reimagining, based on human-centred values and anticipatory regulation, is not only desirable but also necessary to regulate generative AI within a constitutional democracy.

5. Policy and Comparative Approach: Towards a Contextualised Model of AI Governance

The policies of the world on artificial intelligence along with government of India is very much oriented towards the ways of policy-based, adaptive regulation instead of strict, prescriptive statutory regulation. This inclination fits into the overall regulatory philosophy of India in new technologies where innovation, scalability and inclusion takes precedence with incremental legal regulation. Instead of passing an explicit AI law, India has incorporated AI regulation into the current regulatory system, most prominently the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023 and an expanding number of executive policy tools published by MeitY and NITI Aayog.[37] This mixed system will aim at resolving the clash between the needs in economic development and the requirements of ethics and law. Relative to each other, the global regulatory models expose different courses of action based on institutional capability, constitutional culture, and economic priorities. The Artificial Intelligence Act of the European Union is an exemplary instance of a risk-based, ex ante regulation regime, which divides AI systems into prohibited category, high-risk category, limited-risk category, and minimal-risk category.[38] The method is indicative of the rights-based legal tradition of the EU, in which the precaution, proportionality, and protection of fundamental rights are preempted. In comparison, the United States has been largely sectoral and market-driven, with the repercussions of government regulation of AI implementation resting on the already existing agencies, tort law, and executive guidance.[39] The US model is based on innovation and competition and it is comfortable with regulatory disintegration as the trade-off to technological

2000 (India); Copyright Act, 1957 (India); World Intellectual Property Organization (WIPO), *Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence* (WIPO, 2020).

[37] Ministry of Electronics and Information Technology (MeitY), *Advisory on Safe and Trusted Artificial Intelligence* (Government of India, 2024); Ministry of Electronics and Information Technology, *IndiaAI Mission: Responsible AI Framework and Implementation Strategy* (Government of India).

[38] European Union, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM(2021) 206 final; Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (EU Artificial Intelligence Act).

[39] White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (Executive Order No. 14110, 2023); Federal Trade Commission, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI* (FTC Guidance, 2021); Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. Davis L. Rev. 399 (2017).

leadership. The new structure in India is positioned in the middle between these frameworks.

It does not accept the total statutory control of the EU and the laissez-faire of the US. Rather, India has resorted to soft law, regulatory sandboxes, and guidance by principles which is a practical approach to institutional constraints and developmental priorities. In specific cases, such as regulatory sandboxes, a jurisprudence of trial includes regulators to identify the effects of technology in the controlled setting and then implement normative rules. This strategy corresponds to the modern regulatory theory that proposes responsive and reflexive governance in which the law is updated in a series of steps with technology. The MeitY guidance of recent and the IndiaAI Mission documents are examples of a gradual transition of abstract ethical commitments to operational governance tools.[40] The focus on risk classification, systems of auditable AI, grievance redress, and human control is an indicator of the realization that generative AI presents differentiated risks that cannot be solved by using a one-size-fits-all regulation. The increase in attention to transparency reporting, model documentation and assessing the impact of the public interest is an indication of a nascent shift towards procedural accountability, which requires AI developers to justify design choices that can impact rights and safety and democratic processes.[41] This policy course implies the implicit adoption of proportionality and subsidiarity as a principle of justice in a jurisprudential view. Indian policy instruments do not ban technologies, but are aimed at grading the risk based on the potential harm by setting up graduated obligations.

This is in line with the constitutional values preserving the space of innovation and placing greater responsibilities of care on high-impact applications like generative AI systems that may change the discourse of the masses, or modify financial choices or access to vital services. Nonetheless, the use of policy guidance also brings up the issues of legal certitude, democratic validity and enforceability. The soft-law tools do not have the binding power of the statutes and can lead to disproportionate adherence, especially when it comes to high-profile actors in the private sector. Lack of clear legal implications of non-compliance will lead to it becoming a voluntary ethics issue instead of a binding responsibility with regards to AI.

The experience of the EU indicates that the application of ethical principles, not based on enforceable commitments, is often not a good way to eliminate systemic harms. In the case of India, the point of comparison is not wholesale exportation of foreign models of regulation, but the localisation of international best practices under local constitutional and institutional circumstances. A pragmatic solution a mix of statutory minimum standards as per the IT Act and the DPDP Act with sector-specific rules, sandboxes and developing guidance could provide an opportunity. The legitimacy could be increased by embedding binding procedural requirements, including obligatory risk assessment of high-risk generative AI and the existence of legally binding grievance mechanisms, without affecting the flexibility. In a nutshell, the comparative advantage of India indicates a philosophy of governance which is focused on adaptive regulation and is constitutional. The difficulty in this progress will be to turn policy dreams into legal norms that are long-lasting and responsive to the magnitude, obscurity, and social implication of generative AI. By striking this balance, it will be possible to make sure that the AI governance framework in India can become an example of inclusive and responsible innovation or persist as a system susceptible to disintegration and normative watering down.[42] These relative lessons explain why India must go beyond policy experimentation to structured legal integration, whereby generative AI governance is innovation-friendly and constitutionally entrenched.

6. Suggestions and Conclusion

Generative artificial intelligence is a characteristic technological change that has the potential to alter the economic, administrative, and social environment in India. Meanwhile, it also presents complicated legal risks that cross over the set doctrinal lines privacy, intellectual property, criminal liability, consumer protection, and administrative accountability. This study has shown that even though India has a foundational framework of cyber-law in the form of Information Technology Act, 2000, its intermediary-based and reactive framework is not apt to handle the autonomous, scalable, and opaque nature of generative AI systems. The article indicates that generative AI undermines the principles of legal regimes that are based on the notion

[40] Ministry of Electronics and Information Technology (MeitY), *Advisory on Safe and Trusted Artificial Intelligence* (Government of India, 2024); Ministry of Electronics and Information Technology, *IndiaAI Mission: Responsible AI Framework and Implementation Strategy* (Government of India).

[41] European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM(2021) 206 final; United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021); Ministry of Electronics and Information Technology, *IndiaAI Mission – Responsible AI Framework* (Government of India).

[42] NITI Aayog, *National Strategy for Artificial Intelligence: #AIforAll* (Government of India, 2018); United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (UNESCO, 2021); European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM(2021) 206 final.

of human authorship, identifiable intent, and post-hoc liability. The failure to legally acknowledge AI model providers, the absence of preventive requirements including risk assessment and auditing, and the takedown as a remedy to this kind of harm all undermine the ability of the law to avert harm before it strikes. Even though recent events, in particular, the Digital Personal Data Protection Act, 2023, and policy actions as part of the IndiaAI Mission, are indicative of a positive trend of rights-based and risk-conscious governance, these efforts are still fragmented and mostly advisory in nature.

On the global level, the paper places the governance of AI in India in a wider normative context that is informed by the human rights conventions, data protection guidelines, labour regulations, and ethical tools like the Recommendation on the Ethics of Artificial Intelligence developed by UNESCO. These global postulates highlight human dignity, autonomy, equality, and responsibility and strengthen the notion of AI governance as a technical and moral and legal duty. The fact that there is no binding world AI treaty does not weaken these obligations; it only puts a larger burden on the states to internalise global norms through domestic legal systems. Using some comparison lessons and constitutional jurisprudence, the paper will support a careful, human-friendly, and risk-oriented reform agenda.

eavor of humanising artificial intelligence.

To start with, the IT Act needs to be revised in order to explicitly classify generative AI model providers as new regulatory participants, who are liable to duty of care based on outcomes. Second, AI systems that pose a significant risk should have their mandatory risk and impact assessment, especially when these systems touch upon essential rights or benefit of the people at large. Third, transparency and auditability should be entrenched by documentation that is legally binding, logs, and redress systems. Fourth, the regulatory cooperation between MeitY, data protection agencies, sectoral regulators and consumer protection agencies must be institutionalised to prevent piecemeal regulation.

Finally, above all, the AI regulation system in India should be based on the premise that technology is created to serve human good, rather than to substitute human reason or human decency. The law should not only respond to technological maleficence but also to influence the design of technology itself. The integration of domesticity regulation with core values of humanism and international principles of human rights can help India to develop the governance model that upholds innovation and protects democratic integrity, social justice, and the rule of law. By doing that, not only will India be able to regulate generative AI, but it will also have its part to play in the global end