

Autonomy, Accountability And Algorithms: India's Cyber Law At A Crossroad

Arpita Mishra^{a*}, Dr. Monica Yadav^b, Dr. Pooja Batra Nagpal^c

^{a*} Research Scholar at IILM University, Gurugram

^b Professor of Law at IILM University, Gurugram

^c Associate Professor at IILM University, Gurugram

Abstract

Generative artificial intelligence has completely changed the connections between technology, law, and society. In contrast to previous digital technologies, generative AI systems automatically generate content, imitate human expression, and affect the decision-making process on a large scale. Such abilities question the core premises of Indian cyber law that is stuck in a human-oriented, reactive, and intermediary based regulatory paradigm. This paper critically analyses the cyber legal framework of India using the overlapping autonomous, accountable and algorithmic governance perspectives. It states that although Indian law has continued to acknowledge personal autonomy and informational dignity, it is yet to advance to hold algorithmic systems and their creators accountable in the same proportion. Through the examination of constitutional jurisprudence, statutory provisions, policy tools, and the international trend, the paper shows that the Indian cyber law is at a very crucial crossroads. It ends with a recommendation of a moderate, rights-based, and risk-focused governance process that can strike a balance in the innovation and democratic responsibility.

Keywords: Generative AI, Cyber Law, Autonomy, Accountability, Algorithmic Governance, India

1. Introduction

The emergence of generative AI in a short period of time is a paradigm shift of the digital ecosystem, as it is no longer a platform that accepts and distributes human expression but a system that creates, filters, and amplifies at scale. In contrast to the previous digital technologies, generative AI systems engage in the process of speech, image, decision-support, and behavioural nudge creation, and as a result, they make a difference in the discourse of the population, impact the formation of personal preferences, and alter the way institutions decide on the matter. Such functions pose deep legal, ethical and governance concerns that put in question the assumptions upon which modern cyber-law regimes are based. This technological change has developed in the context of a cyber-law regime that was designed in a previous stage of the internet - infrastructural to identifiable human authorship, traceable will, and post hoc allocation of responsibility. These regulatory instruments (the Information Technology Act, 2000 and the separate regulations) were formulated to conduct intermediaries as a passive medium of third- party content, with a liberal approach of minimal intervention on the basis of safeguarding free speech and encouraging innovation. Generative AI challenges this logic of regulation, by erasing the distinction between the host of the content and the creator of the content, and (in consequence) revealing the inefficiency of legal principles that are based on human agency. Meanwhile, constitutional jurisprudence in India has been experiencing a significant development.

The establishment of privacy, dignity and decisional autonomy by the courts has expanded normative horizon of digital rights underscoring the individual as an autonomous subject and not a data point. This rights turn, nevertheless, is in conflict with regulatory strategies that still consider algorithmic systems as a neutral technology tool but not normative actors with the capacity to cause systemic harm. This disconnection is also especially clear within the context of generative AI, whose result can be printed without legally identifiable author; but produce practical effects on the real world as false information, reputational damage, discriminatory results, consumer loss, and distortion of democracy. This paper will argue that the Indian cyber law is at a crossroad. Regulators and courts face the selection of whether or not to regulate generative AI, but it is how to carry out these regulations in a way that balances technological innovation with

constitutional values and democratic accountability. The threat of failure to adapt entails the risk that a regulatory model of platforms and technological efficiency over individual rights, public trust and institutional legitimacy is entrenched. On the other hand, excessive control can drive innovation out of the market and reduce the hopes of India in the digital economy.

It is on this basis that the paper proceeds to develop one main idea: to govern generative AI well, it is necessary to conceptually redefine Indian cyber law and go beyond a reactive, intermediary-focused approach, to one that anticipates autonomy, accountability and responsibility of algorithms. Through a constitutional legal analysis of law, statutory frameworks, policy efforts and international comparative law and policy, this paper explores the question of whether the current legal system is capable of having a significant response to the specific problems associated with generative AI. The paper is organised around three themes that are interconnected, including autonomy, accountability, and algorithms, which combined offer an evaluation of the strengths, weaknesses, and opportunities of the algorithmic era of the Indian cyber-law system.

2. *Global Views of Autonomy, Accountability and Algorithmic Governance*

The dilemmas of artificial intelligence generative is not unique to India. In different jurisdictions, law systems are struggling to come up with a way of balancing the introduction of technology with the need to safeguard autonomy, accountability, and democracy. The global experience can be an insight into the ways various models of governance are trying to counter the risks posed by autonomous algorithm systems and still maintain the freedom of individuals and the economic development. At the international level, it increasingly comes to understand that generative AI has an impact on the basic human interests. Although it did not exist at the time of the development of the artificial intelligence, the international human rights law provides a normative framework that could be applied in the regulation of the AI systems. Human dignity, equality, privacy, and freedom of expression were once of the ideas embedded in such instruments as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, and they remain the guide in the modern debate on the regulation of AI. These tools reinstate the fact that technological progress should be kept in second place to human well-being and democratic responsibility. This, in the context of generative AI, is converted to the notion that algorithms are supposed to aid, not erode or disempower, human judgment and agency. The European Union has taken the most extensive approach to the governance of AI among modern regulatory models. Artificial Intelligence Act by European Union embodies a preventive and risk-based approach to regulation. The EU framework will not react to malevolence once it has taken place but classifies AI systems regarding their degree of risk to the individuals and the society. Strict obligations pertaining to transparency, data control, human regulation, and accountability apply to high-risk systems, e.g. work, credit, medical care, and civil services. It has its basis in the robust constitutional tradition of fundamental rights protection inherent in the EU and how autonomy can be preserved using structural regulation, as opposed to using individual consent. The United States, on the contrary, has adhered to a sectoral and market-based approach to AI regulation. Instead of having an inclusive AI law, the U.S. uses the already established law, including consumer protection law, discrimination law, tort liability, and regulation by specialised regulatory agencies. Most recent executive instructions and policy at the agency level promote responsible development of AI but does not go as far as to establish binding and consistent requirements. This model is more innovative and flexible, but has been criticised as leaving serious accountability gaps, especially in the case of systemic risks, like misinformation, algorithms bias, and concentration of the market. International bodies have been also involved in influencing the norms of AI governance. The Recommendation on the Ethics of Artificial Intelligence by UNESCO focuses on the human-centred perspective and requests the transparency, fairness, responsibility, and respect of human rights within AI systems. Such tools are not legally binding, but they help to create a common global consensus that AI governance should be based on ethical and democratic principles. On the same note, the OECD AI principles emphasise inclusive growth, human oversight and responsible innovation and supporting the notion that autonomy and accountability are not contrary, but complementary, goals. The trends in these countries indicate a slow transformation of the perception of AI as an objective technological assistant to the understanding of the fact that it is a power system that can influence social and political processes. Particularly, generative AI gives

cause to the concern of manipulation, misinformation, and the loss of individual agency on a scale. International governance systems are increasingly recognising that autonomy protection is more than privacy protection necessitating consideration of the effects of the algorithmic systems on behaviour, shape decisions and democratic involvement. To India, these foreign viewpoints provide wisdom and advice.

Current policies of AI governance in India have been policy-based and have mostly been based on ethical principles, regulatory sandboxes, and sectoral programs instead of full-scale legislation. Such flexibility should facilitate innovation and be aligned with the developmental priorities of India, however, it can lead to the issue of regulatory fragmentation and uneven enforcement. Lack of binding obligations of high-impact AI systems can expose people insufficiently to systemic harms. Meanwhile, India cannot afford to imitate the foreign regulatory models. The European model represents the institutional abilities and socio-economic situations that are not comparable with the Indian reality, whereas the American scheme might not be adequate to deal with structural inequalities and democratic weaknesses in Indian setting. The trick here is to develop a system of governance that considers the international best practices and at the same time is not insensitive to the domestic constitutional values and social lives. After all, its foreign experience teaches a common lesson, which is that autonomy, accountability, and algorithmic governance are inseparable.

An efficient regulation of AI should safeguard personal freedom, and at the same time, the creators and implementers of powerful algorithmic systems should be responsible regarding their social outcome. Since India is on the brink of its cyber-law evolution, it can consider following the global trends and comparative examples to establish a balanced and, crucially, human-centred approach to generative AI that would encourage innovation, without violating dignity and democratic integrity or causing people to lose confidence in the state.

3. Indian Law: Autonomy, Accountability, and Algorithms

The legal reaction to the issues of generative artificial intelligence in India consists of the legal frameworks of cyber and data protection and the constitutional provisions as the main factors instead of AI-specific laws. Currently, there is no specific law governing artificial intelligence in India. Rather, the regulation of AI systems is in effect via a mixture of constitutional guideline, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and government-level direction. This piecemeal treatment is indicative of the flexibility as well as the constraints of Indian cyber law in a moment when algorithmic systems are becoming more and more a part of social, economic, and democratic existence.

On the constitutional level, Indian law offers a solid normative basis to establish rules in generative AI. The new meaning given by the Supreme Court to Article 21 has broadened the right to life and personal liberty to incorporate dignity, privacy, decisional autonomy, and informational self-determination. Such principles become especially applicable to the realm of AI where algorithms are used to process personal data and make judgments about the behavioural patterns and impact the person decisions. This is what constitutional jurisprudence defines as the fact that the development of technologies should be attentive to human dignity and autonomy even in cases where the technological systems are used by the non-state actors. Nonetheless, although the constitutional values provide some guidance, the translation of the constitutional values into tangible regulatory obligations of AI systems is still not developed. The Information Technology Act, 2000 still forms the foundation of the cyber-law regime in India. This Act was passed at a time when the internet was mainly a communication and information sharing platform and as such, it follows a more humanistic and responsive approach to regulating it.

Its intermediary liability model specifically the 79 section assumes that the platform is a neutral conduit through which third-party content is transmitted. The intermediaries will enjoy conditional immunity against liability, but must satisfy due diligence and content takedown conditions. Although this framework has played a crucial role in enhancing digital development and freedom of expression, it is increasingly being challenged in the generative AI sector where platforms are conducting design, deploy, and monetisation of autonomously generated content systems. Generative AI introduces a challenge to the basic assumptions of the IT Act because it does not provide a clear differentiation between content creator and content host. When dangerous or

misleading AI-generated material spreads over the internet, the issues of accountability get complicated. The current legal system is aimed at remedy of damage after the fact, through takedowns, criminal law or civil rights. This type of post-hoc solution is not a proper fit to combat such systemic risks as deepfakes, automated misinformation, and algorithmic discrimination, which can propagate at a lightning speed with little to no human interference. This leads to the creation of accountability loopholes where affected persons have few and slow solutions.

Digital Personal Data Protection Act, 2023 is a new law in India that has a beneficial impact on the sphere of digital governance. The Act identifies personal data protection as a continuation of individual dignity and autonomy and puts responsibilities on those who process digital personal data. These are legal processing requirements, data security requirements and transparency requirements. Theoretically, DPDP Act should be applicable to the datasets utilized in training the AI models of generative types, which creates a valuable degree of accountability. Nevertheless, the Act is mostly consent-based and does not capture the issues of AI systems fully, which are based on the aggregation of mass data, de-identification, and inferential data. Consequently, although the DPDP Act reinforces the rights of individuals, it does not offer full protection against the manipulation of algorithms and system damage yet. In addition to the statutory law, the policy efforts and soft-law tools have influenced how India regulates AI. The National Strategy on Artificial Intelligence, and its successor, National Strategy on responsible AI by NITI Aayog focus on ethics development, inclusiveness, and welfare of the population. Later in the India AI Mission and guidance issued by the Ministry of Electronics and Information Technology, there is an attempt to shift towards risk-based governance, transparency and redressing of grievances. These efforts are an indication of the realization of the special issues presented by generative AI, yet their informal character prevents any imposition, especially in the case of strong commercial forces.

Combined, the national legal system of India demonstrates a transitional stage of cyber governance. The constitutional values are highly acclaimed to the principles of autonomy and dignity, whereas there are few statutory tools to hold the accountable algorithmic systems. The IT Act puts more emphasis on innovation and free speech, yet it has a hard time controlling proactive harm of AI. The DPDP Act reinforces the protection of the data, yet it fails to address the challenges of generative AI entirely in terms of behaviour and structure. The guidance of policies fosters ethical AI but is not binding. Such combination of strengths and weaknesses puts Indian cyber law at a crossroad. It is not so much about controlling technology, but it is about re-aligning past rules of law to accommodate the power of algorithms without compromising the innovation. A future-responsive attitude would involve identifying generative AI creators and implementers as responsible subjects, implementing features to block high-risk systems, and harmonizing cyber-governance with constitutional promises of autonomy, equality, and democratic wholeness. This way, India can be on its way to a consistent national structure where there is an alignment of algorithms with human values and not the redefining of the same with impunity.

4. Accountability Gaps in the Algorithmic Ecosystem

Responsibility is the fundamental element of the effective legal system, as it is the means, according to which power is limited and damage is compensated. The Indian traditional approach to cyber law is founded on the well-conceptualized legal principles of knowledge, intent, control and causation-principles that assume the identification of human actors that may be held responsible of engaging in criminal acts. Liability under this system is normally attributed in situations where an individual willfully inflict, enable or fail to avoid harm. Although the model has worked quite well in the process of regulating human behaviour in the digital space, it is ever becoming destabilized by the advent of generative artificial intelligence. Generative AI systems work based on probabilistic and self-educational mechanisms and generate not personally written, revised, and approved outputs of a single human decision-maker. Such systems produce content according to patterns acquired by huge amounts of data rather than premeditated human intervention. Consequently, negative consequences, including misinformation, deep fakes, discriminatory inferences or misdirected advice, do not always have a distinct human authorship or intent. This spreading of responsibility makes it difficult to apply the traditional liability doctrine which is not well suited to address the effects of autonomous and opaque algorithmic processes. This gap in accountability is further enhanced by the intermediary liability regime under the Indian cyber law.

This form of regime was conceived at an earlier stage within the internet, and it has a philosophy of minimal intervention, where the intermediaries are given conditional immunity against liability since they carry third-party content to protect freedom of speech and innovation. Platforms are viewed as passive channels, where they are supposed to only respond when they are informed on illegal content. Nevertheless, this conceptualisation is increasingly untenable when platforms actively design, train, deploy and monetise their generative AI systems, which are autonomous content generators. When this occurs, platforms cease serving the role of a neutral facilitator and become influential actors with vast influence on the architecture, capabilities, and societal influence of the algorithmic systems. Irrespective of this change, Indian cyber law is still largely based on reactive measures including the notice-and-takedown methods and the post-hoc enforcement. These processes put a lot of responsibility on the responsibility of affected individuals who have to locate the harmful content, define its illegality and move on to claim redress when the damage has already been done. This is especially poor in the case of generative AI. Malicious information can be produced and propagated at a large scale, copied immediately, and altered to avoid detection. The victims of deepfakes, automated misinformation, or algorithmic discrimination usually have little to no chance to repair their reputation, psychological, or economic damages, which are usually irreversible before the legal action can be taken.

The responsibility deficit that is produced by this reactionary model is not the responsibility gap of procedure; it is the gap of jurisprudence. A legal framework that only acts once harm is committed is ineffective in terms of mitigating predictable and structural risks that are involved in the generative AI technologies. In contrast to individual cases of illegal speech, AI-based harms are usually systematic and repetitive, inbuilt in the design of systems, training data, and optimisation objectives. Examples such as deepfakes are not some kind of accidental by-products but reasonable applications of generative models that are trained to copy human appearance and voice. Likewise, discriminant outputs are often a replica of biases in training data as opposed to the deliberate misbehavior of individual users.

This is also worsened by the lack of ex ante obligations. Indian cyber law does not at the moment imperate AI creators or implementers to carry out algorithm impact analysis, analyze any likely risks or execute safeguards prior to the usage of high-impact systems. No legal requirements exist with regard to the transparency of model design, outputs auditability, or decision-making process traceability. In the absence of these kinds of preventative measures, regulatory control is scattered and inefficient and the damage spreads and responsibility is hard to find. This failure to exercise proactive governance also poses questions as to the issue of power asymmetry as well as democratic accountability.

Generative AI systems put much power into the hands of the private agents who determine data, infrastructure, and deployment decisions. By considering these actors as tools of the system instead of being liable system designers, law protects them at the expense of putting people and society in a skewed level of risk. The consequence of this is a regulatory asymmetry where platforms enjoy the protection of innovation-friendly regulation, and individuals take the social costs of algorithm failure. Finally, the unchecked vulnerability of the algorithmic ecosystem in India demonstrates the inadequacy of human-based and reactive-oriented assumptions of a cyber-law framework. Generative AI is proposing law to stop relying on the limited notions of intent and authorship but rather a wider concept of responsibility, based on risk, control, and social influence. Unless accountability mechanisms are recalibrated to the reality of algorithmic power, Indian cyber law will become even more detached of the very technologies it is intended to regulate.

5. Freedom and the Constitutional Turn of Digital Governance

The autonomy is the emerging concept of Indian constitutional law as the cornerstone of human dignity, which is a good indicator of a pivotal change in the perception of individual rights protection in the digital era. The judicial acknowledgement of privacy, choice and bodily integrity indicates a shift in the conventional concept of liberty as freedom of governmental intrusion to a more abundant, rights-based concept of people as self-determining agents who can construct their own lives. The constitutional twist of this is immense regarding the digital regulation, specifically as far as generative artificial intelligence is concerned, which functions by conducting massive extraction, aggregation, and interpretation of data created by human behaviour, expression, preferences, and identity.

The development of AI systems, in general, and generative AI, in particular, is completely dissimilar to the previous data-driven technologies. They do not simply archive or process the information provided by users, but learn through large volumes of data consisting of human experience and then revisits, simulates and creates speech, pictures, stories, and decision-supports in the manner of human innovativeness and thought. By so doing, these systems confuse the line between human expression and machine generated content. Using personal information in such systems without significant transparency, choice or control makes individuals not subjects but raw materials in the algorithmic optimisation. In these conditions, autonomy stands the risk of being degraded to a data abstraction, as fragmented, decontextualised and reused in ways that people have not anticipated and may not even comprehend. Informational privacy has been identified by the Indian constitutional jurisprudence as part and parcel of the concept of dignity, with the argument that individual control over personal information is a prerequisite to autonomy, which is meaningful.

Generative AI does reveal, however, the weakness of a legal system largely focused on discrete, identifiable breaches of privacy. The negative effects of generative AI tend not to occur as a result of one illegal action or violation, but rather through systematic and aggregate algorithmic effects that condition behaviour and impact perception, as well as affect decision-making in a manner that is subtle and over time. Profiling, behavioural nudging, predictive personalisation, and automated inference are all executed to ensure continuous and invisibility, and as such it is challenging to determine when people have been affected against their autonomy and possible to find an effective solution to the problem. This move towards personal injury to structural power poses a big challenge to constitutional governing.

The conventional rights enforcement frameworks are ill-suited to deal with the harms that are diffuse, probabilistic, as well as embedded in technological design. Formally, generative AI systems can be legal and comply with the current legal regulations, but in reality can weaken autonomy through manipulation of attention, reinforcing biases, or restricting the perceived options. Consequently, the safeguarding of autonomy in the era of AI cannot be reduced to ex post facto adjudication or personal consent procedures. The enactment of the data protection law in India is a significant change in norms, which introduces an understanding that people are not the passive objects of data manipulations but the rights holders that have the right to know, to be fair, and accountable. This change in legislation is consistent with the constitutional values, recognizing the informational self-determination as the element of dignity.

However, autonomy as a concept in the framework of generative AI cannot be satisfied by the consent-based compliance. Can-Consent, especially in complex algorithmic ecosystems tends to be formal, but not substantive. People are regularly exposed to long and unclear privacy policies, uneven bargaining strength, and unclear knowledge of the mechanisms of the AI systems, as well as the way their data will be utilized in the future. Under such circumstances, consent can justify data processing and do not necessarily enable people to gain effective control over their digital personalities. An autonomy that is constitutionally significant must have structural guarantees that go beyond the choice of the individual at the moment of data gathering. Such protections should address the design, training and deployment of generative AI systems per se.

Transparency requirements to be considered should not only cover data use, but also the reason, logic and possible effect of algorithmic systems. We have to put restrictions on manipulative architectures, which take advantage of cognitive weaknesses or manipulate user behaviour. Where AI systems impact important life decisions, civic discourse, or democracy, human monitoring systems are required. Otherwise, autonomy can be viewed as being safeguarded on paper but undermined in practice. Furthermore, the constitution constitutional shift toward autonomy calls on the wider reconsideration of power in digital governance. Generative AI places a lot of power into the hands of the designer and operators of algorithm systems which are frequently private actors outside of the conventional frameworks of accountability. By considering these systems as tools of neutrality instead of the places of normative power within law, the lack of attention to the asymmetry between the individual user and the developers of AI occurs.

To safeguard autonomy, in this regard, it is important to remember that freedom is not endangered only by direct forms of coercion but also by indirect coercion in the form of technological controls that determine preferences, opportunities, and self-image. Making decisions that are independent of democratic self-determination is, in this respect, unimaginable in the era of generating AI. It is the freedom of thought, ability to make opinions and be involved in the life of the people in a

meaningful way that relies on digital environments that value human agency instead of using it. The constitutional governance is thus required to go beyond a small-scale emphasis on privacy infringements to an all-encompassing one, which meets how the algorithmic systems organize choice and shape the communal existence. Finally, the Indian constitutional turn in digital governance requires a redefinition of legal imagination. Generative AI has a retaliatory role in defending autonomy as a personal right and a structural state of dignity, freedom of thought and democratic agency. Unless these values are integrated into the rules of governance of the algorithmic systems, the prospect of constitutional sovereignty is likely to be overwhelmed by the technological structures that redefine human experience without uttering a single word about it.

6. Comparative and Policy Perspectives

The comparative legal developments offer a good sense of insights into the various jurisdictions that are trying to regulate the risks and opportunities brought about by generative artificial intelligence. Regulators are becoming more and more aware around the world that the time-honored, reactive legal frameworks are no longer adequate to capture the magnitude, pace or systemic effects of algorithmic systems. The difference in regulatory styles may be seen as the constitutional traditions, capacity of the institutions, socio-economic priorities, which contain valuable lessons to India, as it attempts to work out its own way of regulation. The European Union has become a leader in the overall AI regulation with the adoption of the Artificial Intelligence Act. EU model is based on the *ex ante* risk-based regulatory philosophy, which categorizes AI systems as prohibited, high-risk, limited-risk, or minimal-risk systems in accordance with the potential effects on basic rights, safety, and democratic processes. There are also stringent obligations of high-risk systems, which are in areas of employment, credit scoring, biometric identification, and access to public services. This is an EU framework of high constitutional adherence to the standards of dignity, equality and proportionality, which is elaborated by its Charter of Fundamental Rights and jurisprudence of the Court of Justice of the European Union.

The EU aims at deterring the harm before its occurrence instead of having post-hoc remedies by introducing the element of accountability at the design and deployment phases. By contrast, the US has followed a highly sectoral and market-focused approach to the governance of AI. The U.S. is not implementing a single, broad-based AI statute, instead depending on the current legal measures, including consumer protection, tort liability, anti-discrimination, and the supervision of specialised regulatory bodies, including the Federal Trade Commission. In the recent executive directions and policy frameworks, responsible and trustworthy AI development are prioritised although these steps are mostly unenforceable. This style is more innovation-oriented, flexible, and competitive in the market, which is the constitutional tradition of the United States of limited regulation and high protection of free speech. Critics, however, note that where there are no consistent, enforceable commitments, there exist large gaps of accountability, especially concerning systemic risks like misinformation, algorithmic bias, and concentration of technological power.

The regulatory model used by India lies halfway between these models. Instead of a broad-based legislation, India has thus far depended on a combination of the current legislation on cyber alongside data protection and policy based guidance. The foundation of the cyber-law is established by the Information Technology Act, 2000, and rights-based requirements connected with personal data processing in the Digital Personal Data Protection Act, 2023. Parallel to that, the government in India has undertaken policy initiatives like NITI Aayog National Strategy on Artificial Intelligence and IndiaAI Mission which focus on ethical AI development, inclusivity, and populace well-being. Regulatory sandboxes and regulator advisory frameworks have been advanced as the means to promote innovation, but at the same time enable regulators to gain experience of what is actually practiced. There are obvious benefits of this incremental and flexible method. It allows experimentation, domestic innovation, and it does not prematurely lock the regulatory system to a rapidly changing and rapidly developing technological domain.

Nevertheless, it provokes serious concerns on enforceability and democratic legitimacy. The soft-law instruments, moral rules, and advices are not binding and usually rely on self-compliance. This restriction is especially sharp, when it comes to dealing with high-impact generative AI systems that are designed, deployed, and monetised by powerful private actors. In the absence of statutory requirements, ethical undertakings may be only aspirational as opposed to operational, which will

result in disproportional compliance and regulatory arbitrage. Indian court rulings also provide an example of the conflict between the innovation-oriented regulation and the accountability requirement. The traditional interpretation of intermediary liability provisions by courts has been in line with the values of free expression and immunization against involvement of the court as seen in the landmark cases that have stressed on the use of platforms as facilitators rather than publishers. On the one hand, this jurisprudence has played a vital role in protecting speech and innovations, to the extent that it has strengthened a reactive regulatory stance in which the mitigation of harm is imposed on the individual. Within the framework of the generative AI, this kind of approach might be too small to handle systemic and predictable harms caused by the algorithmic design decision instead of end-user mischief. New policy measures are an indication of increased appreciation of such issues. The governmental directions are making more and more accent on openness, auditability, redressal of grievances, assessment of impact on the public of the AI systems. These trends imply a fledgling move to procedural accountability, where developers and deployers are to explain design decisions and determine their impacts on society. But unless there is some statutory anchoring, these measures are easily subject to dilution, selective enforcement, and lack of effectiveness. Comparative experience thereby points to an important lesson of India, namely that a delicate balance between flexibility and enforceability is needed in an effective governance of AI.

Excessive regulation may result in restraining of innovation, whereas excessive use of soft law may lead to normative degradation and mistrust. An approach that is tailored to the extent of 400,000 with references to the preventative safeguards of the EU, the U.S. focus on innovations, and the Indian constitutional values might be a way to resolve this. This would include an incorporation of fundamental responsibility requirements of the high-risk AI systems into the law, and policy instruments and sandboxes through adaptive governance. In conclusion, the comparative and policy-oriented approaches enable us to understand that the framework of cyber-law in India is on the crossroads. The decisions taken today will define whether India can come up with a comprehensive, rights-affirming AI governance model or remain with incoherent regulation that is barely able to keep up with technological transformation. The deployment of national policy efforts to comply with binding law standards is necessary to realize the national policy initiatives based on the constitutional values of dignity, equality, and democratic accountability to make sure that generative AI can promote the societal interests instead of harming it.

7. *Next Horizons: Reinventing Cyber Law in the Age of Algorithms*

Indian cyber law needs to experience a transformative change, which should be principled and visionary and orient it toward integrating legal doctrine with the reality of algorithmic power. To begin with, the law should specifically acknowledge generative AI developers, deployers and platform operators as separate regulatory actors, not to be absorbed in the conventional intermediary categories. Such actors have extensive influence on system design, training data, deployment situations, and commercial incentive and thus they should be liable to result oriented responsibilities of care. These responsibilities must not be solely directed at the adherence to formal guidelines, but they must also aim at avoiding the avoidable harms that might occur due to the application of the high-impact generative AI systems. Second, Indian cyber governance needs to change to a more reactive style to preventive and risk-based regulation.

It demands the introduction of ex ante requirements like compulsory algorithmic risk evaluation, transparency, and explainability, and traceability solutions of AI-created content. Systems that are at risk of harming the population, individuals, access to services, or democracy should be highly scrutinized and monitored. The proactive governance would minimize the use of post-hoc solutions that are usually received late enough to prevent or reduce damage and enhance the confidence of people in digital systems. Third, there needs to be institutional coordination in the regulation sectors in effective AI governance. Lacking a unified control over the data protection and sectoral regulators, as well as over cyber governance organizations, may create a lack of uniformity in standards and loopholes in enforcement. Harvesting of information, alignment of compliance needs and better accountability pathways would be facilitated by a well-coordinated framework, where the harms of AI are managed holistically and not solely. More importantly, these reforms should be in touch with constitutional principles of dignity, equality and democratic accountability. It is not that regulation negatively impacts innovation, but rather should steer it in a direction that

would produce socially beneficial and rights-respecting consequences. It is through instating constitutional values in the management of algorithmic systems that the Indian cyber law will come out of crisis-driven regulation and produce a well-established framework that is future-oriented and able to regulate generative AI in a way that enhances technological advancement and human well-being.

8. Conclusion

Generative artificial intelligence has indicated the conceptual and structural weaknesses of current cyber-law in India. Although constitutional jurisprudence has gradually enhanced the rights of autonomy, dignity, and privacy, the regulations have been slower to create significant accountability of an algorithmic system, which is becoming more and more influential in shaping social, economic, and democratic life. This incongruence plunges Indian cyber law in a critical dilemma that lies between adaptive governance that can address the algorithmic power and normative erosion between reactive and fragmented regulation. When this gap is not addressed, it will worsen the situation where constitutional safeguards may be strong in theory and weak in practice, skewed towards technological platforms and against people and societal good. It is not just a legal or technical challenge, but a constitutional one, in need of redefining roles of law in the algorithmic era as regards understanding responsibility, harm, and power. The future of cyber regulation is neither between innovativeness and regulation, but in a process of balancing freedom and responsibility by the means of principled, risk-conscious regulation. India can overcome reactive regulation by reforming its cyber-law system to include proactive protective mechanisms, institutional alignment, and result-focused responsibilities of care. By so doing, it can play a role in a way of the world model of democratic, human-friendly AI governance in which technological advancement can keep abreast with constitutional principles and social trust.

References

1. 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.
2. Information Technology Act, 2000 (India); Shreya Singhal v. Union of India, (2015) 5 SCC 1.
3. Christian Louboutin SAS v. Nakul Bajaj, (2018) 253 DLT 728 (Del. HC); Information Technology Act, 2000 (India), § 79; World Intellectual Property Organization (WIPO), Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence (WIPO, 2020)
4. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
5. Information Technology Act, 2000 (India), § 79; Shreya Singhal v. Union of India, (2015) 5 SCC 1; 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).
6. European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act); White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (Executive Order No. 14110, 2023); United Nations Educational, Scientific and Cultural Organization (UNESCO), Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021).
7. United Nations Educational, Scientific and Cultural Organization (UNESCO), Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021); European Union, Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).
8. 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 Artificial Intelligence (FTC Guidance, 2021); Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 U.C. Davis L. Rev. 399 (2017).
9. United Nations Educational, Scientific and Cultural Organization (UNESCO), Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021).
10. 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), OECD Principles on Artificial Intelligence (OECD, 2019); European Union,

- Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).
11. Ministry of Electronics and Information Technology, Government of India, National Strategy on Artificial Intelligence – Towards Responsible AI (Discussion Paper, 2021); NITI Aayog, Operationalising Principles for Responsible AI (Government of India, 2023).
 12. Ran Hirschl, *Comparative Matters: The Renaissance of Comparative Constitutional Law* (Oxford University Press 2014).
 13. Upendra Baxi, *Constitutionalism in India* (Oxford University Press 2008); Ran Hirschl, *Comparative Matters: The Renaissance of Comparative Constitutional Law* (Oxford University Press 2014); Sujit Choudhry (ed), *The Migration of Constitutional Ideas* (Cambridge University Press 2006).
 14. Information Technology Act, 2000; Digital Personal Data Protection Act, 2023; Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; Ministry of Electronics and Information Technology, National Strategy for Artificial Intelligence (NITI Aayog, 2018).
 15. Information Technology Act, 2000; Digital Personal Data Protection Act, 2023; Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; NITI Aayog, National Strategy for Artificial Intelligence (2018); Ministry of Electronics and Information Technology, Advisory on Responsible Artificial Intelligence (2024).
 16. Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; Information Technology Act, 2000; Digital Personal Data Protection Act, 2023; NITI Aayog, National Strategy for Artificial Intelligence (2018); Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).
 17. Information Technology Act, 2000; Pavan Duggal, *Cyber Law: The Indian Perspective* (Saakshar Law Publications 2004); S. Krishnamurthy, 'Law and the Internet in India: A Regulatory Overview' (2001) 43 *Journal of the Indian Law Institute* 327.
 18. Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018); Digital Personal Data Protection Act, 2023; Arghya Sengupta and Vidushi Marda, 'India's Data Protection Framework and Digital Governance' (2024) *Economic & Political Weekly*; OECD, *Data Governance and Privacy* (2020).
 19. Digital Personal Data Protection Act, 2023; Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018); Arghya Sengupta, 'Consent Fatigue and the Limits of Data Protection in India' (2023) *Economic & Political Weekly*; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR' (2017) 7 *International Data Privacy Law* 76.
 20. NITI Aayog, National Strategy for Artificial Intelligence (2018); NITI Aayog, *Responsible AI for All* (2021); OECD, *Recommendation of the Council on Artificial Intelligence* (2019).
 21. Digital Personal Data Protection Act, 2023; Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; NITI Aayog, *Responsible AI for All* (2021); Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI' (2021) 41 *Computer Law & Security Review* 105567.
 22. Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; Anuj Garg v Hotel Association of India (2008) 3 SCC 1; NITI Aayog, *Responsible AI for All* (2021); OECD, *Recommendation of the Council on Artificial Intelligence* (2019); Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).
 23. OECD, *Artificial Intelligence: An Overview* (2021); Nils J. Nilsson, *The Quest for Artificial Intelligence* (Cambridge University Press 2010); Frank Pasquale, *New Laws of Robotics: Defending Human Expertise in the Age of AI* (Harvard University Press 2020); Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep Learning* (MIT Press 2016).
 24. Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019); Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015); Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018); OECD, *Platform Governance* (2021).
 25. Shreya Singhal v Union of India (2015) 5 SCC 1; MySpace Inc v Super Cassettes Industries Ltd (2017) 236 DLT 478; Google India Pvt Ltd v Visaka Industries Ltd (2020) 4 SCC 162; Information Technology Act, 2000, s 79.
 26. NITI Aayog, *Responsible AI for All* (2021); OECD, *Recommendation of the Council on Artificial Intelligence* (2019).

27. European Union, Artificial Intelligence Act (Regulation (EU) 2024/1689); White House Office of Science and Technology Policy, Blueprint for an AI Bill of Rights (2022); Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; NITI Aayog, Responsible AI for All (2021); Ran Hirschl, Comparative Matters: The Renaissance of Comparative Constitutional Law (Oxford University Press 2014).
28. European Union, Artificial Intelligence Act (Regulation (EU) 2024/1689); OECD, Recommendation of the Council on Artificial Intelligence (2019); NITI Aayog, Responsible AI for All (2021); Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR' (2017) 7 International Data Privacy Law 76.
29. Information Technology Act, 2000 (India), §§ 66C, 66D, 67; Consumer Protection Act, 2019 (India); Shreya Singhal v. Union of India, (2015) 5 SCC 1; United Nations Educational, Scientific and Cultural Organization (UNESCO), Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021). Information Technology Act, 2000, No. 21 of 2000 (India).
30. Digital Personal Data Protection Act, 2023, (11 Aug. 2023).
31. Justice K.S. Puttaswamy (Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.), (2017) 10 SCC 1.
32. Shreya Singhal (Shreya Singhal v. Union of India), (2015) 5 SCC 1.
33. NITI Aayog, National Strategy for Artificial Intelligence (2018).
34. NITI Aayog, Responsible AI for All (RAI papers / AI for All series, 2021–2022).
35. Ministry of Electronics and Information Technology (MeitY), Advisory on Safe, Trusted and Responsible Artificial Intelligence (2024) and related MeitY reports on platforms/AI.
36. European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act) (Official Journal of the European Union, July 2024).
37. OECD, Recommendation of the Council on Artificial Intelligence (2019) and related OECD AI policy guidance.
38. White House Office of Science and Technology Policy, Blueprint for an AI Bill of Rights (2022).
39. B. N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Report of the Committee of Experts on Data Protection, 2018).
40. Sandra Wachter, Brent Mittelstadt & Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR' (2017) 7 International Data Privacy Law 76.
41. Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015). Frank Pasquale.
42. Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs 2019). Shoshana Zuboff.
43. Ian Goodfellow, Yoshua Bengio & Aaron Courville, Deep Learning (MIT Press 2016) — for technical grounding on probabilistic/self-learning AI systems. Ian Goodfellow.