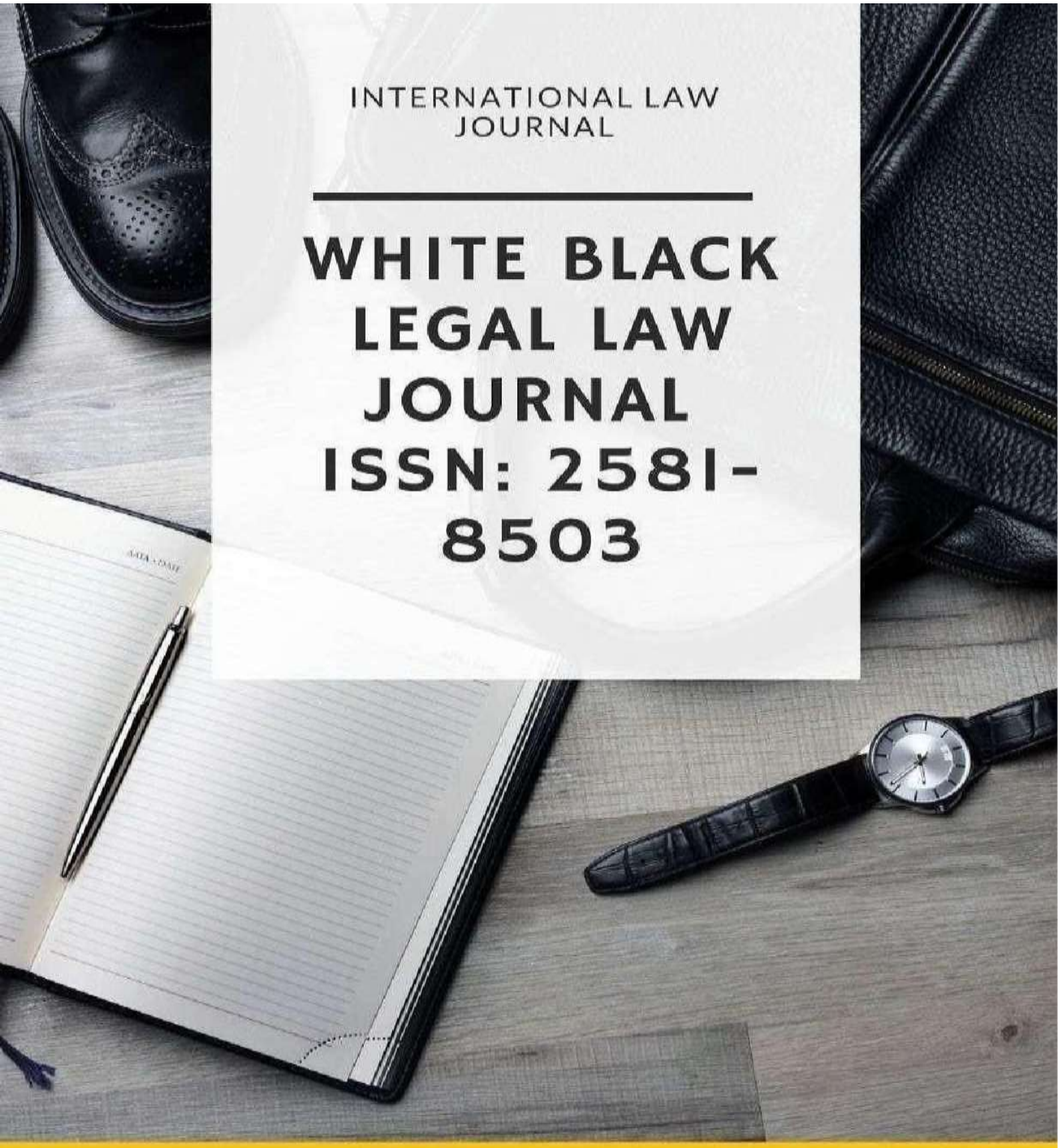

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

LESSONS FROM THE EUROPEAN AI ACT FOR INDIA: AI PLATFORMS AND LIMITS OF SAFE HARBOUR.

AUTHORED BY - RAJDEEP DUTTA

Introduction.

Artificial Intelligence is being used by everyone, everywhere. From making content to copying intellectual properties to a near-exact level, AI is doing everything. The rapid rise of AI has led many countries to enact laws regulating its uses and misuses, with the European Union among the first to create dedicated, well-structured laws for AI-related crimes. India also has the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, in place to somewhat counter the threat AI poses.

Section 79[1] of the Information Technology Act, 2000, provides a conditional safe harbour to intermediaries, that is, AI systems. Now, these generative AI systems generate synthetic content based on the prompt the user provides. The synthetic content produced by these generative AI models can often be incriminating, detrimental, or simply harmful to the privacy of individuals or groups. Unlike traditional internet platforms that primarily host and transmit third-party content, generative AI systems produce outputs at the user's command using large, well-trained models on extensive datasets. The provision was designed and installed in an earlier phase of the internet, where platforms performed as neutral stations facilitating communication. The judiciary has shed light on this section, notably in Shreya Singhal v. Union of India.[2]and has reinforced that intermediaries cannot be held liable or asked to remove content unless directed by the judiciary itself. As generative AI becomes increasingly integrated into digital infrastructures, the continued application of intermediary safe- harbour protections to such systems raises significant concerns about accountability, misinformation, intellectual property infringement, and algorithmic harm.

These concerns, however, have been well addressed and prompted by the EU AI Act. The EU AI Act governs artificial intelligence through a risk-based model. The Act mandates transparency and implies an ex ante compliance obligation to meet government standards for

[1] Information Technology Act, § 79, No. 21 of 2000, India.
[2] Shreya Singhal v. UOI, AIR 2015 SC 1523.

data output, which can be flagged as high-risk. This removes the concept of neutrality granted to the intermediaries and treats them as technological products that require regulatory oversight. India, by contrast, has not yet adopted a comprehensive legislative framework specifically governing artificial intelligence. AI governance remains fragmented across existing digital laws, policy advisories, and sector-specific regulations.

This paper compares India's intermediary liability framework with the European Union's risk-based regulatory approach to artificial intelligence. It argues that generative AI systems fundamentally challenge the conceptual foundations of safe harbour regimes designed for passive hosting platforms. While the European Union has moved toward preventive, risk-oriented governance of AI systems, India continues to rely on a reactive intermediary liability model developed for an earlier technological context.

Intermediary Liability and the Doctrine of Safe Harbour.

Safe harbour provisions were introduced to ensure that online intermediaries are not treated as publishers of third-party speech. Similar doctrines can be found in Section 230 of the Communications Act of 1934[3], of the United States of America, which provides conditional and limited immunity to artificial intelligence providers. Section 230(c)(1) understood that the service providers are not owners of the content produced through their product, nor do they hold the power to publish or are liable for when a user publishes their product.

Section 79 of the Information Technology Act, 2000[4]It holds the doctrine of safe harbour. Introduced through amendments in 2008, the provision grants conditional safe-harbour protection to intermediaries for third-party information hosted on their platforms. Under the Act, an intermediary includes entities such as social media platforms, internet service providers, online marketplaces, and other digital platforms that facilitate the transmission or hosting of user-generated content. The section states that intermediaries shall not be held liable for any third-party information or data produced or hosted on their platforms, subject to a few conditions. These conditions should satisfy that the provider itself does not initiate the production of the output, nor does it select the receiver at the other end. Additionally, it is recommended that these intermediaries perform the necessary "due diligence" before disbursing output.

[3] Communications Act, § 230, 47 of 1934, U.S.A.
[4] Information Technology Act, § 79, No. 21 of 2000, India.

The constitutional interpretation of Section 79 was significantly clarified by the Supreme Court of India in Shreya Singhal v. Union of India.[5]. The case is widely regarded as a landmark decision in Indian internet law, not only because the Court struck down Section 66A of the Information Technology Act for violating freedom of speech under Article 19(1)(a) of the Constitution, but also because it provided authoritative clarification regarding the scope of intermediary liability. The Court held that intermediaries must remove or disable access to unlawful content only when they receive a valid order from a competent court or a notification from the appropriate government authority. Private complaints alone are insufficient to trigger a mandatory takedown obligation. By adopting this interpretation, the Court sought to prevent arbitrary censorship and to ensure that determinations of illegality are made through legally accountable processes rather than through private platforms' discretion.

The court held that intermediaries should only remove content when they receive a valid order from a competent court or a notice from the Government. However, the rise of generative artificial intelligence introduces significant doctrinal tension with this framework. Unlike traditional platforms that merely host or transmit user-generated speech, generative AI systems actively produce outputs shaped by training data and algorithmic design. This development raises important questions regarding whether the conceptual foundations of intermediary immunity articulated in the previously mentioned case can continue to apply to technologies that generate content rather than merely facilitate its transmission.

The Emerging Indian Approach to AI Governance Framework.

At present, the principal legal framework governing digital platforms and online intermediaries in India remains the Information Technology Act, 2000. The Act regulates cyber offences, intermediary liability, and digital communication networks, but it was enacted long before the development of modern machine learning systems and generative artificial intelligence. Consequently, the statute does not directly address legal issues relating to automated decision-making, algorithmic accountability, or AI-generated content. As a result, questions concerning liability and regulatory oversight for AI systems must currently be interpreted through legal provisions that were designed for an earlier phase of the internet economy.

India’s policy engagement with artificial intelligence gained significant momentum with the

[5] Shreya Singhal v. UOI, AIR 2015 SC 1523.

release of NITI Aayog's National Strategy for Artificial Intelligence in 2018[6]. NITI Aayog aims to implement AI across multiple sectors to improve public service.

Another important dimension of India's digital governance architecture is data protection regulation. The enactment of the Digital Personal Data Protection Act, 2023, represents a significant step in regulating the collection, processing, and use of personal data within the digital economy. Although the Act is not specifically designed as an AI regulation statute, it has substantial implications for the development of artificial intelligence systems, particularly those trained on large datasets containing personal information. AI models often rely on extensive data processing during training, which raises questions about consent, data minimisation, and lawful processing under data protection law. Consequently, data governance frameworks are likely to play a central role in shaping the regulatory environment for AI technologies in India.

India is in a transitional phase of AI governance, with the creation of a legal framework that is adequate and addresses all issues that arise. This stands in sharp contrast to the European Union, whose Artificial Intelligence Act is based on a risk-based model.

The EU AI Act.

The European Union has taken a significantly more structured and preventive approach to regulating artificial intelligence through the adoption of the EU AI Act.[7]. Unlike jurisdictions that rely primarily on existing digital governance frameworks, the EU has introduced a comprehensive legislative regime specifically designed to regulate the development, deployment, and use of AI systems. The Act represents the first large-scale attempt by a major jurisdiction to create a harmonised legal framework governing artificial intelligence across multiple sectors. Its core objective is to ensure that AI technologies are developed and deployed in ways that protect fundamental rights, consumer safety, and democratic values while still encouraging technological innovation within the European digital market.

The regulatory architecture of the EU AI Act is built around a risk-based classification model that regulates AI systems based on the level of risk they pose to individuals and society. This

[6] NITI AAYOG, https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf (11th March, 2026).
[7] Congress.gov, https://www.congress.gov/ (12th March, 2026).

framework reflects the EU's broader approach to technology governance, which often treats emerging technologies through the lens of product safety and the protection of fundamental rights. The Act therefore categorises AI systems into four distinct levels of regulatory risk: unacceptable, high, limited, and minimal. Each category is subject to different regulatory obligations and compliance requirements. The regulatory architecture of the EU AI Act is built around a risk-based classification model, which regulates AI systems according to the level of risk they pose to individuals and society. This framework reflects the EU's broader approach to technology governance, which often treats emerging technologies through the lens of product safety and the protection of fundamental rights. The Act therefore categorises AI systems into four distinct levels of regulatory risk: unacceptable, high, limited, and minimal. Each category is subject to different regulatory obligations and compliance requirements.

The second category, high-risk AI **systems**, is the core focus of the EU AI Act's regulatory framework. These systems are permitted but are subject to extensive compliance obligations because they can affect fundamental rights, safety, or important social outcomes. High-risk systems include AI used in areas such as biometric identification, employment decision-making, credit scoring, law enforcement, and critical infrastructure. Providers of high-risk AI systems must comply with several governance requirements before deploying their systems in the European market. These obligations include conducting risk assessments, ensuring high-quality training datasets, maintaining technical documentation, establishing human oversight mechanisms, and implementing transparency obligations. The Act also requires conformity assessments to verify that these systems comply with regulatory standards before they can be placed on the market.[8]

The EU AI Act also introduces regulatory obligations for general-purpose AI systems and generative AI models, recognising the growing influence of foundation models in digital ecosystems. Providers of such models must disclose summaries of the data used for training, comply with European copyright law, and ensure that AI-generated content can be identified as synthetic when necessary. These transparency measures aim to mitigate risks associated with misinformation, intellectual property violations, and the misuse of generative technologies.

Scholars examining the EU AI Act have observed that the regulation reflects a broader shift

[8] European Parliament, European Parliament, (11th March, 2026)

toward preventive technology governance, where regulatory obligations are imposed before technologies are widely deployed rather than after harms occur. Michael Veale and Frederik Zuiderveen Borgesius[9] argue that the risk-based framework seeks to reconcile technological innovation with fundamental rights protections by imposing proportionate obligations based on the potential societal impact of AI systems.

These regulatory features demonstrate that the European Union conceptualises artificial intelligence as a technology requiring ex ante governance mechanisms rather than reactive liability frameworks. By imposing structured compliance obligations on developers and deployers of AI systems, the EU AI Act seeks to prevent harmful outcomes before they occur. This preventive regulatory architecture stands in contrast to jurisdictions such as India, where the governance of digital technologies continues to rely heavily on intermediary liability doctrines developed for earlier generations of internet platforms.

Intermediary Neutrality and its Cons.

The emergence of generative artificial intelligence presents a significant doctrinal challenge to intermediary liability regimes that were originally designed for passive digital platforms. Traditional safe harbour frameworks, including those embedded in Section 79 of the Information Technology Act, 2000, are premised on the assumption that intermediaries function as neutral conduits that merely host or transmit third-party content. Generative AI systems, however, fundamentally disrupt this conceptual foundation by actively producing outputs through algorithmic processes shaped by training data, model architecture, and deployment decisions. This transformation raises critical questions regarding the continued applicability of intermediary neutrality doctrines to technologies that generate content rather than facilitate its dissemination.

Legal commentary increasingly recognises that the governance challenges posed by generative AI extend beyond traditional content moderation concerns. In the Indian context, practitioners have noted that existing intermediary liability doctrines were formulated for user-generated content rather than algorithmically generated outputs. As one legal analysis observes, the question of intermediary liability in relation to deepfakes and AI-generated content is now a

[9] Michael Veale & Frederik Zuiderveen Borgesius, Demystifying the Draft EU Artificial Intelligence Act, SSRN, (12th March, 2026, 8:00 PM).

"hot topic" reflecting divergent approaches to platform responsibility across jurisdictions.[10]

Regulatory discourse in India has increasingly focused on developing specific governance frameworks for synthetic media. Recent policy discussions surrounding amendments to the Intermediary Guidelines emphasise the need for enhanced due diligence obligations for platforms that facilitate AI-generated content. These proposals aim to introduce transparency requirements and accountability mechanisms without imposing blanket censorship obligations, thereby balancing innovation with harm prevention. At a broader governance level, comparative analyses suggest that jurisdictions worldwide are experimenting with regulatory responses to synthetic media. For instance, recent legal reforms and policy debates have proposed explicit prohibitions on the malicious use of deepfake technologies for impersonation and misinformation[11]. Such developments indicate an evolving understanding of cybersecurity and digital law frameworks in response to emerging AI-driven risks.

From a doctrinal perspective, generative AI therefore destabilises the intermediary–publisher distinction that has historically structured internet liability law. The output of generative systems cannot be characterised solely as user speech, nor can responsibility be attributed entirely to autonomous technological processes. Instead, accountability is distributed across developers, deployers, and platform operators. This diffusion of responsibility challenges the conceptual foundations of safe harbour regimes and suggests the need for regulatory models that impose proportionate obligations based on technological risk and control.

Comparative Analysis: Risk Governance vs Indian Safe Harbour.

The EU AI Act represents a significant shift toward ex ante governance, imposing compliance obligations on AI developers and deployers before technologies are introduced into the market. This approach aligns with the European Union's broader regulatory tradition of treating emerging technologies as products that must meet safety and rights-based standards.[12]. In contrast, India's digital governance framework remains reactive and liability-oriented, relying primarily on safe-harbour provisions that limit intermediaries' liability for third-party content. This model assumes that platforms function as neutral conduits and that regulatory intervention should occur primarily after harmful content has been identified. Legal commentators have

[10] Bar and Bench, www.barandbench.com, (11th March, 2026).
[11] DNP Vietnam Law Firm, www.dnp-law.com , (12th March, 2026).
[12] European Commission, European Commission, official website - European Commission, (10th March, 2026).

observed that such an approach may be increasingly inadequate for addressing the systemic risks posed by generative AI, particularly in areas such as misinformation, synthetic media, and algorithmic bias. deployment. As policy analyses note, the Act seeks to create a harmonised legal framework that both fosters innovation and ensures that AI systems respect fundamental rights, safety norms, and democratic values.

India's regulatory position, however, reflects a broader developmental strategy that prioritises technological growth and digital innovation. Government policy documents and legal analyses indicate that Indian regulators have been cautious about introducing comprehensive AI legislation, citing concerns that overregulation could hinder the country's emerging digital economy. At the same time, this innovation-first approach has resulted in a regulatory environment characterised by policy guidance, sectoral rules, and executive advisories rather than binding statutory obligations.[13]. The implications of this divergence are particularly significant for accountability for AI-generated harms. Under the EU AI Act, developers of high-risk AI systems must implement governance mechanisms, including conformity assessments, transparency obligations, and human oversight protocols, before deploying their technologies. These requirements reflect an understanding that AI systems can generate systemic risks that must be mitigated through structured regulatory intervention.

In India, by contrast, accountability mechanisms remain largely reliant on post hoc enforcement through intermediary liability rules or sector-specific regulatory actions. This reliance on reactive governance may create legal uncertainty when generative AI systems produce harmful or unlawful content. As commentators have noted, the absence of a dedicated AI regulatory statute complicates the attribution of responsibility among developers, deployers, and platform operators, thereby exposing gaps in the existing legal framework.[14]

Ultimately, the comparative analysis demonstrates that the EU and India are adopting fundamentally different regulatory paradigms in response to the rise of artificial intelligence. The EU's preventive, risk-based governance model seeks to impose structured obligations on AI providers to mitigate harms before they occur. In contrast, India's reliance on intermediary safe-harbour doctrines reflects a more reactive, innovation-oriented regulatory philosophy. As

[13] Mondaq Legal500, www.mondaq.com, (12th March,2026)
[14] Lexology, www.lexology.com ,(12th March,2026).

generative AI technologies continue to evolve, the tension between these approaches raises critical questions about the future trajectory of digital governance and the adequacy of existing liability frameworks in addressing the risks associated with algorithmically generated content.

Conclusion

The rise of generative artificial intelligence represents a profound shift in the technological and regulatory landscape of digital governance. Traditional intermediary liability regimes, including those embedded in Section 79 of the Information Technology Act, 2000, were designed for an earlier phase of the internet, when platforms functioned primarily as passive facilitators of user-generated communication. Generative AI systems, by contrast, actively produce synthetic content shaped by complex algorithmic processes and extensive training datasets. This transformation challenges the conceptual foundations of intermediary neutrality and raises urgent questions regarding accountability, liability, and regulatory oversight in the contemporary digital ecosystem.

The comparative analysis undertaken in this paper demonstrates that jurisdictions are responding differently to these challenges. The European Union's adoption of the EU AI Act reflects a preventive, risk-based approach that imposes structured compliance obligations on AI developers and deployers. By conceptualising AI systems as technological products capable of generating systemic risks, the EU has sought to establish ex ante governance mechanisms to safeguard fundamental rights, consumer protection, and democratic integrity. India, in contrast, continues to rely on a reactive intermediary liability framework supplemented by policy guidance and sectoral regulatory initiatives. While this innovation-oriented approach has supported technological growth, it also exposes gaps in accountability when applied to generative AI systems that do not fit neatly within traditional intermediary categories.

Ultimately, the governance of generative artificial intelligence will require a reimagining of legal frameworks that balance innovation with accountability. As AI technologies become increasingly embedded in social, economic, and political processes, regulatory systems must evolve to address the distributed and systemic nature of algorithmic risk. The future of digital governance in India will depend on its ability to move beyond platform-era liability doctrines toward more adaptive and forward-looking regulatory paradigms.