

(JOINT JURIST)

[NATIONAL-LEVEL | PEER-REVIEWED | OPEN-ACCESS LEGAL JOURNAL]

| VOLUME 1 | ISSUE 1 | MAY 2026

ABOUT THE JOURNAL

The **Joint Jurist** is a strictly law-focused national publication designed to bridge the gap between academic research and litigation expertise. We operate on a **Double-Blind PeerReview** model, ensuring that every published work meets the highest standards of original scholarship and academic integrity. Our platform is dedicated to providing an openaccess environment for legal professionals, scholars, and students to contribute to the evolving legal discourse.

EDITORIAL & ADVISORY BOARD

The Joint Jurist Journal is guided by a distinguished panel of legal luminaries and academicians committed to fostering excellence in legal scholarship.

- **Advocate Suraj Shandil**
- **Dr. Seema Gupta**
- **Dr. Mohd Rafiq**
- **Dr. Harshita Thalwal**
- **Ms. Sabrina Bath**
- **Ms. Soumya Sharma**

NAME	DESIGNATION	INSTITUTION/AFFILIATION	SPECIALIZATION & IMPACT
Advocate Suraj Shandil	Founder, CEO & Editor-in-Chief	High Court of Himachal Pradesh	IPR Specialist, Courtroom Strategy & Legal Research.

Prof. (Dr.) Seema Gupta	Editorial Board Member	Associate Professor / Chandigarh University (CU)	Constitutional Law, IPR, & Supreme Court Certified Mediator/ Interdisciplinary Legal Studies.
Prof. (Dr.) Mohd. Rafiq Dar	Editorial Board Member	Associate Professor/Lovely Professional University (LPU)	Consumer Law, Criminal Law, Law on Consumer Protection/Interdisciplinary Legal Studies.
Dr. Harshita Thalwal	Editorial Board Member	Associate Professor & HOD, Chandigarh University(CU)	Academic Leadership & Interdisciplinary Legal Studies.
Asst. Prof. Ms. Somya Sharma	Editorial Board Member	Professor of law & Ph.D. Scholar/ Shoolini University	Banking Laws, Corporate Laws, & Human Rights /Interdisciplinary Legal Studies..
Asst. Prof. Ms. Sabrina Bath	Editorial Board Member	Assistant Professor & Ph.D. Scholar/Chandigarh University (CU)	Legal Framework Analysis & Academic Rigour/ Interdisciplinary Legal Studies.

**“ REGULATING SYNTHETIC MEDIA: A CONSTITUTIONAL
CRITIQUE OF INDIA’S 2026 INTERMEDIARY RULES ”****AUTHOR:- Sneha Awasthi**

Abstract

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, are India’s first targeted attempt at grappling with the rise of synthetic digital media.¹ Synthetic videos, audio, and other forms of media are now produced and distributed with unprecedented speed and volume.² The Amendment proposes labelling, metadata, and faster response times for takedowns.³

This article suggests that, while the 2026 Rules may tackle the symptoms of misinformation, they fail to grapple with the root challenges of artificial intelligence. The approach appears to favour speed over process, and control over content over systemic responsibility. In doing so, it may not meet the Supreme Court’s test for proportionality. The debate in this Part provides an overview of the regulatory environment, describes the salient features of the Amendment, and places the debate in the context of India’s constitutional history.

I. Introduction: Context and Emergence of Synthetic Media

India is on the cusp of a future where artificial intelligence (AI) is becoming a part of daily life. AI-powered systems are increasingly influencing how we communicate, make decisions, and even shape our opinions.⁴ The advent of synthetic media has given this a new twist.⁵ A video

¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120€ (Feb. 10, 2026).

² Ministry of Electronics & Info. Tech., FAQs on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, at 2-4 (Feb. 10, 2026).

³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(2)(d), 3(3)(a)(ii), as amended by G.S.R. 120€ (Feb. 10, 2026).

⁴ *Id.* At 2-4.

⁵ *Id.*

may be faked, yet look entirely authentic. An audio clip may not be produced by a human voice at all.

If technology can produce such a convincing hoax, how does the law deal with it?⁶

The Central Government has tried to provide an answer to this in the 2026 Amendment Rules under the Information Technology Act, 2000.⁷ These Rules broaden the concept of “information” on the internet to also cover synthetic content. They also place new responsibilities on intermediaries. Intermediaries must clearly identify such content, include metadata to enable tracing, and act within short time-frames (as short as three hours) on complaints.⁸

The Court has previously interpreted this to mean that restrictions should not be excessive or unclear.⁹ It appears that the 2026 Rules are operating in this space. They seek to regulate harmful content, but do so in a way that shifts a lot of responsibility to private companies. This presents an immediate problem. When intermediaries are required to make quick decisions about what should and shouldn't be on the internet, are they simply providing services or performing a private regulatory function?¹⁰

This is not censorship by the State, but privatised censorship.¹¹

This is not a new problem. In *Shreya Singhal v Union of India*¹², the Supreme Court held Section 66A of the IT Act unconstitutional for being vague and open to abuse. Specifically, the Court was worried about the chilling effect on speech.¹³ If people do not know what they can or cannot say, they might not say anything. It seems to be an issue again, but in a different context.

⁶ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended by G.S.R. 120€ (Feb. 10, 2026); Ministry of Electronics & Info. Tech., FAQs on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, at 3-4 (Feb. 10, 2026).

⁷ Information Technology Act, No. 21 of 2000, § 79, India Code (2000), as amended by G.S.R. 120€ (Feb. 10, 2026).

⁸ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(2)(d), 3(3)(a)(ii), as amended by G.S.R. 120€ (Feb. 10, 2026).

⁹ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India); *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

¹⁰ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

¹¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(1B), 7, as amended by G.S.R. 120€ (Feb. 10, 2026).

¹² *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

¹³ *Id.* ¶¶ 84, 90.

A new aspect has emerged recently. There is now a risk of misuse of AI in courtrooms. In *Gummadi Usha Rani v. Sure Mallikarjuna Rao* (2026), a trial court cited non-existent cases.¹⁴ These “precedents” were created by AI.¹⁵ The Supreme Court considered this to be a grave error and stepped in.¹⁶ The case is still under way, but it demonstrates that the issue is not just confined to social media. It can affect the justice system itself.

This raises a broader concern. If even institutional actors may not recognise synthetic content, can it really be left to the intermediaries to manage it in a matter of hours? Or is it a more complex issue?

II. The 2026 Amendment: Structure, Design, and Regulatory Scope

The 2026 Amendment builds on the intermediary framework provided in Section 79 of the IT Act.¹⁷ Limited liability remains, but it is now linked to the fulfilment of particular obligations. Intermediaries are required to exercise due diligence in taking down infringing content, and also in labelling synthetic content.

There are three important features of this design.

First, the need for labelling. Content deemed to be artificial must be labelled accordingly.¹⁸ This will assist the viewer in differentiating between authentic and synthetic content. It is based on the idea that disclosure may lessen the impact. If the user knows that the video is fake, they may be less likely to be deceived.

Second, provenance metadata. Companies are required to keep information on content provenance.¹⁹ This is meant to enhance transparency. Theoretically, it makes it easier to trace the origin of offensive content.

¹⁴ *Gummadi Usha Rani v. Sure Mallikarjuna Rao*, C.R.P. No. 2487 of 2025, at 1-2 (A.P. H.C. Sept. 26, 2025).

¹⁵ *Gummadi Usha Rani & Anr. V. Sure Mallikarjuna Rao & Anr.*, S.L.P. © No. 7575 of 2026 (S. Ct. India Feb. 27, 2026) (order on admission).

¹⁶ *Gummadi Usha Rani v. Sure Mallikarjuna Rao*, C.R.P. No. 2487 of 2025, at 1-2 (A.P. H.C. Sept. 26, 2025); *Gummadi Usha Rani & Anr. V. Sure Mallikarjuna Rao & Anr.*, S.L.P. © No. 7575 of 2026 (S. Ct. India Feb. 27, 2026).

¹⁷ Information Technology Act, No. 21 of 2000, § 79, India Code (2000), as amended by G.S.R. 120€ (Feb. 10, 2026).

¹⁸ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(3)(a)(ii), 4(1A), as amended by G.S.R. 120€ (Feb. 10, 2026).

¹⁹ *Id.* R. 3(3)(a)(ii).

Third, the speedy takedowns. This is probably the most controversial. The timeframe may be just hours after the content is identified. In some cases, such as impersonation and intimate images, it could be even less.²⁰

All of these measures make sense on their own. But together they have practical and constitutional implications. Hurrying up the process leads to quicker decisions. Inaccurate decisions may result. In uncertain situations, a platform might opt to take down a piece of content to avoid liability.²¹

This is not censorship by the State, but privatised censorship.

The State must demonstrate that the restriction serves a legitimate purpose, is necessary, and not disproportionate.²² These questions remain open. The Rules offer some guidance, but not a comprehensive approach to decision-making and review.²³ Nor do they address the underlying questions of how content is generated by AI systems.

III. Limits of the 2026 Amendment as an AI Governance Framework

Upon closer inspection, we see that the Amendment focuses primarily on the level of platforms. It controls the presentation, labelling, and deletion of content. It does not regulate, at least in detail,²⁴ the design and operation of the AI systems that produce such content.

The Rules tackle the symptoms of the problem through content moderation. This strategy might work in the short run, particularly in crises. But it creates a gap in governance.

The European Union has done something different with the AI Act, which classifies AI systems based on risk.²⁵ These are subject to more stringent measures, such as audits and human oversight.²⁶ India's 2026 Rules do not yet take this step. Rather, they uniformly rely on an intermediary model.

²⁰ Id. R. 3(2)(d).

²¹ Id. Rr. 3(1B), 7.

²² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India); Modern Dental College & Research Ctr. V. State of M.P., (2016) 7 S.C.C. 353 (India).

²³ Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India); Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).

²⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(3)(a)(ii), 3(1B), as amended by G.S.R. 120€ (Feb. 10, 2026).

²⁵ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 2024/1689).

²⁶ Regulation (EU) 2024/1689, arts. 9, 14, 16, 50, 2024 O.J. (L 2024/1689).

This does not necessarily mean that the Indian model is wrong. It is a product of a desire for agility. It might also be driven by the desire to foster innovation while regulating. But the lack of a framework in place raises a question. Will a content-driven approach be sufficient to uphold constitutional values in an AI world?

This question is not clear. It depends on how the law develops over the next few years. But what we can say at this point is that the 2026 Amendment is a first step in the right direction. It recognises the issue but doesn't resolve it entirely.

IV. Outsourced Censorship and Its Chilling Effect on Speech

A closer examination of the 2026 Amendment Rules reveals that the key constitutional issue is not just the content of the prohibitions, but the manner in which they work. The regime places a significant emphasis on the intermediaries to make speedy determinations about the legality and propriety of content. This move from public law to private platform judgment is worth considering.

Regulation of speech is not prohibited by the Constitution. It allows it in certain circumstances. But it has also insisted that regulation be imposed by clear law and subject to some form of review. When private companies are put in a position where they must determine what speech is allowed to remain online, the distinction between regulation and delegation is blurred.

The three-hour takedown period is a case in point. It's supposed to curb harm rapidly. It might also lead to defensive censorship. In doubt, a platform will err on the side of censorship and then test for legality. This is not because it is told to over-censor by law, but because the stakes are high.

It might be indirectly discouraged.

The Supreme Court tackled a similar problem in *Shreya Singhal v. Union of India*. The Court concluded that vague and overbroad restrictions on free speech can result in arbitrary censorship. It noted that intermediaries shouldn't be "forced to act as judges in a statutory vacuum". The 2026 Rules do not repeat Section 66A, but they raise a similar issue. They establish a regime where platforms must work fast with general and sometimes vague criteria like "constitutional compliance."

And how to appeal the decision. This presents a silent question. If the Constitution demands due process and accountability from the State, should it also demand it from private persons acting on behalf of the State?

V. Proportionality and Constitutional Constraints

Proportionality is a key doctrine in the Indian Constitution, particularly since *K.S. Puttaswamy v. Union of India*. The Court adopted a four-part test. A restriction on a fundamental right must meet four criteria.²⁷ It must be for a legitimate purpose, rationally connected to that purpose, necessary (in the sense that there is no less restrictive alternative) and proportionate (in the sense of balancing the right and the restriction).

The picture for the 2026 Rules is mixed.

The first criterion, legitimacy, is not problematic. The prevention of misinformation, harm to individuals, and public order are legitimate state interests. Everyone would agree that there should be some regulation of synthetic media.

The second requirement, reasoned connection, also seems to be met. Notifying users of synthetic content and facilitating quick takedowns may help prevent the use of synthetic media. These steps are rationally connected to the objectives.

The problem arises at the necessity stage. It is unclear whether such short time frames and broad duties are the least intrusive. Could independent oversight minimise the risk of arbitrary removal? These options appear to have been overlooked.

The last step, balancing, needs more consideration. The Rules place substantial compliance costs on intermediaries, particularly smaller sites that do not have sophisticated moderation technologies. They also impact users' freedom of expression. The need for speedy action has to be assessed against the risk of over-censorship.

The Court's observations in *Modern Dental College and Research Centre v. State of Madhya Pradesh* are pertinent.²⁸ It noted that even if the State has a legitimate objective, it cannot use excessive means. Even if effective, a measure that is too harsh might not pass constitutional muster.

²⁷ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 325-26, 436-44 (India); *Modern Dental College & Research Ctr. V. State of M.P.*, (2016) 7 S.C.C. 353 (India).

²⁸ *Modern Dental College & Research Ctr. V. State of M.P.*, (2016) 7 S.C.C. 353 (India).

In this context, the 2026 Amendment appears to be somewhat in between. It deals with a problem, but its structure may be too much in favour of control at the expense of subtlety. Lacking specific safeguards, it is hard to say that the balance has been meticulously preserved.

VI. Courts in the Time of AI: Emerging Judicial Concerns

Recent court cases offer insight into how courts might deal with AI. A case in point is *Gummadi Usha Rani v. Sure Mallikarjuna Rao*.

The trial court In this case cited non-existent judgments. The cases were cited by an AI tool and seemed to make sense. The Supreme Court stepped in, highlighting the seriousness of the mistake and its impact on the justice system. The case was put on hold and further investigated.²⁹

The case doesn't set out a broad legal framework on AI. It is more a case of institutional caution. It demonstrates that even legal professionals may have trouble telling the difference between the real and the fake. If this is true for the judiciary, then the problem is even more serious for intermediaries.

Here, one might pause for thought. If the detection of synthetic content involves verification, is this possible within three hours? Or is the law, in requiring acceleration, likely to lead to shallowness?

VII. Structural Gaps in the Indian Regulatory Framework

The 2026 Rules are a targeted intervention, but they don't address the complexity of the harms associated with AI. A more comprehensive response may involve a breakdown of risks.

Such content may be taken down quickly, since the harm is immediate.

Another category includes synthetic content that is not unlawful, but potentially deceptive. Transparency and labelling may be all that is needed in this context. The aim is not banning the content but educating the consumer.

A third, more sophisticated, category is high-risk applications. This involves uses in elections, policing, finance and courts. These risks are systemic. They stem from the design and use of the systems, not only from the content.

²⁹ *Gummadi Usha Rani & Anr. V. Sure Mallikarjuna Rao & Anr.*, S.L.P. © No. 7575 of 2026 (S. Ct. India Feb. 27, 2026); *Gummadi Usha Rani v. Sure Mallikarjuna Rao*, C.R.P. No. 2487 of 2025, at 1-2 (A.P. H.C. Sept. 26, 2025).

The existing framework does not clearly distinguish these. It uses a largely one-size-fits-all approach that focuses on intermediaries. This makes enforcement easier, but it also means the system is less able to deal with underlying problems like algorithmic bias, explainability and discrimination.

India's approach, on the other hand, is still stuck in content regulation. It relies on the belief that control of output is enough to control harm. This may be true in some instances, but not all.

VIII. Emerging Constitutional Questions

As the debate unfolds, some questions emerge. They are not easy to answer, but they serve to focus the question.

Will a system of quick takedown preserve the balance between safety and free speech?

Should intermediaries be the primary decision-makers on matters of fundamental rights?

Should we focus on AI outputs or should we also focus on its operations?

These questions indicate the problem is not technical. It is constitutional in nature. It has to do with the relationship between the State, private parties and individual rights in the digital sphere.

The 2026 Amendment is a milestone in recognising this issue. But it also shows the limitations of a model that is primarily concerned with content. It does little to resolve the underlying problems of accountability, transparency and justice.

IX. Comparative Lessons and the Search for a Regulatory Model

One way to see the shortcomings of the current model is to compare it with other regulatory models that have started to emerge. The European Union's Artificial Intelligence Act classifies systems by risk. Generative AI, such as deepfakes, is positioned within a transparency framework, with disclosure as a key element.

The Indian 2026 Amendment, on the other hand, remains within an intermediary-focused framework. It focuses on platforms as the main regulatory site and leaves it to platforms to deal with the effects of AI content. Should we regulate the creation, design and deployment of AI systems, or the moment at which material is put into the public sphere?

It is not an easy question to answer. A platform-based approach can be implemented rapidly. However, this ease also comes at a price. It may fail to address the root causes of the problem. If a factory consistently produces flawed products, checking the goods at the time of sale may minimise damage in the short to medium term. But it doesn't fix the root of the problem. Eventually the focus may need to be on the manufacturing process itself. This appears to be the case with AI.

X. Reconsidering the Constitutional Balance in the Digital Era

The Indian Constitution has always involved a balance between State and individual rights. This balance is more challenging in the digital era. The 2026 Rules place an emphasis on speed. Harms need to be remedied swiftly, often within hours. This makes sense, particularly in cases of privacy infringements or public nuisance. But speed has never been the only constitutional concern. It has demanded fairness, transparency and accountability too.

The lack of fine-grained procedural protections in the current system is problematic. When a user's content is removed, there is no need for an explanation at the time. In the digital environment, timing is important. If a message is unavailable for a few hours at a critical time, it could be lost.

Here we come back to the concept of proportionality. The Court's reasoning in cases like *Anuradha Bhasin v. Union of India* provides guidance. It stressed the importance of periodic review and transparency in imposing internet access restrictions.³⁰ Although the case is different, the same principle applies. Restrictions should not operate in isolation. They should be subject to review and justifiable.

In the context of the 2026 Amendment, the absence of a review process for platform decisions may detract from this. It relies heavily on intermediaries without providing sufficient oversight.

XI. Towards a More Coherent Regulatory Framework

If the current approach is only a partial solution, the question becomes what a more comprehensive approach might look like. One option is to enact a law governing AI. This law would not only regulate content, but also the lifecycle of AI systems. It could mandate risk

³⁰ *Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637, ¶¶ 151-54 (India).

assessment prior to deployment, documentation of system design, and the ability to override the system in critical situations.

Transparency would still be crucial, but it would not be confined to content labelling. It could also involve the description of how systems work and make decisions. This could be important in applications such as credit scoring or predictive policing, where decisions have direct consequences for human rights.

Institutional design also matters. An independent regulatory agency, with technical expertise and quasi-judicial powers, may be better suited to regulate compliance than a platform-only approach.³¹ It could provide guidance, audits, and offer dispute resolution.

Another consideration is the harmonisation of laws. The Digital Personal Data Protection Act covers data collection and processing, but not the results of AI processing. An integrated approach could address this, bringing together data protection and algorithmic accountability.³²

XII. Concluding Reflections

The 2026 Amendment Rules signify a turning point. They demonstrate a recognition that the law is failing to keep up with technological change. They also show the challenges of developing an effective and constitutionally compliant response.

The framework is more focused on control at the level of content. It attempts to control the effects of AI rather than the processes. This may be understandable as a short-term response, but it does not address all of the challenges posed by artificial intelligence.

The constitutional tradition may not supply answers, but it can offer some guidance. It tells us that regulation needs to be proportionate, transparent, and accountable. It warns us not to put all of our eggs in any one basket, public or private. And it reminds us that rights do not wither in the light of technological advance. They evolve, but they remain.

³¹ Regulation (EU) 2024/1689, arts. 14, 53, 54, 2024 O.J. (L 2024/1689); Information Technology Act, No. 21 of 2000, § 79, India Code (2000).

³² Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023).