The Dialogue®
INFORM ENGAGE IDEATE

POLICY BRIEF

EVOLVING CONTOURS OF PLATFORM GOVERNANCE IN INDIA:

Reading the 254th Report of the Parliamentary Standing Committee on Home Affairs

SEPTEMBER, 2025

POLICY BRIEF

EVOLVING CONTOURS OF PLATFORM GOVERNANCE IN INDIA: READING THE 254TH REPORT OF THE PARLIAMENTARY STANDING COMMITTEE ON HOME AFFAIRS

Author: Garima Saxena, Senior Research Associate, The Dialogue
Editor: Sachin Dhawan, Deputy Director, The Dialogue

(C) 2025 The Dialogue®. All rights reserved.

The Dialogue® is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue® has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

For more information
www.thedialogue.co

Suggested Citation
Saxena, G. (September, 2025). Policy Brief: Evolving Contours of Platform Governance in India. The Dialogue.®.

Catalogue No
TD/PR/PB/0925/08

Publication Date
September 26, 2025

Disclaimer
The facts and information in this report may be reproduced only after giving due attribution to the author and The Dialogue®.

Contents

Executive Summary

India's cybergovernance posture is moving from a largely conduct-based regime to a more accountability-centric model. Read alongside recent advisories, enforcement actions, and court interventions, the 254th Report of the Parliamentary Standing Committee on Home Affairs, tabled on 20 August 2025, is best understood as a directional marker. It aggregates concerns across ministries and regulators and foreshadows where statutory change, institutional capacity, and enforcement practices may converge.

At a high level, the Report signals momentum toward recalibrating intermediary immunity and cooperation duties, clearer treatment of AI-generated content through provenance and labelling, faster, lawful access to cross-border data, and early-stage evidence preservation, as well as capacity upgrades in investigation, forensics, and threat intelligence. It also references sectoral touchpoints, OTT and digital media, telecom anti-spam and fraud rails, advertising verification, app-store governance, and financial-influencer conduct.

It will be crucial to observe how this conversation unfolds in the upcoming parliamentary session and subsequent inter-ministerial processes, as the drafting choices, institutional coordination, and resource allocation will ultimately determine how the strands identified in the Report are sequenced and implemented.

I. Introduction and Background of the Committee

This brief provides a focused analysis and commentary on the 254th Report of the Department-related Parliamentary Standing Committee on Home Affairs, titled *"Cyber Crime–Ramifications, Protection and Prevention"*, which was presented to the Rajya Sabha on 20 August 2025.[1] The Committee initiated its inquiry on 16 October 2024 and, over the course of seven subsequent meetings, heard from a broad cross-section of institutions and stakeholders. Written and oral inputs were received from ministries and regulators, including Ministry of Home Affairs (MHA), Indian Cyber Crime Coordination Centre (I4C), Ministry of Electronics and Information Technology (MeitY), Department of Telecommunication (DoT), Central Bureau of Investigation (CBI), National Investigation Agency (NIA), Financial Intelligence Unit-India (FIU-IND), Reserve Bank of India (RBI), and other bodies such as Indian Computer Emergency Response Team (CERT-In), and Centre for Development of Advanced Computing, India (C-DAC), alongside leading banks, education departments, securities regulators and critical-infrastructure entities. The objective of the Committee's inquiry was multifaceted: to address the growing national security implications of cybercrime; to enhance the protection of individuals, institutions, and infrastructure from digital threats; and to support the development of preventive strategies that foster long-term resilience in India's digital ecosystem.

The brief maps the Committee's observations and selected recommendations, focusing on (i) platform safety and digital accountability, and (ii) institutional responses to cybercrime, and assesses how these proposals could set the direction of India's forthcoming governance regime, situating them within concurrent parliamentary and legislative, regulatory, and judicial developments. In doing so, it evaluates implications for legal design, coordination mechanisms, and rights safeguards across some of the Report's most consequential themes:

- Intermediary Liability and Safe Harbour
- Cybercrime: Legal and & Institutional Framework
- OTT and Digital Media, Advertising and App Store Ecosystem
- Telecom
- Financial Influencers

[1]Parliamentary Standing Committee on Home Affairs. (2025, August 25). "Cyber Crime – Ramifications, Protection and Prevention". Report no.254 <https://sansad.in/getFile/rsnew/Committee_site/Committee_File/ReportFile/15/197/254_2025_8_12.pdf?source=rajyasabha>

II. Relevance of the Report: Landscape and Context

Over the last five years, particularly following the COVID-19 pandemic and emergence of generative AI, India's discourse on cyber governance has expanded to encompass national security, consumer protection, financial integrity, competition, and fundamental rights. Policy movement has accelerated across multiple tracks, including intermediary norms, privacy and data governance, telecom and cybersecurity, media and advertising oversight, among others, often with overlapping mandates and evolving judicial guidance.

Against this backdrop, the Committee's report consolidates concerns that span multiple ministries and regulators, and its recommendations suggest where the next round of reforms may be directed. Read in context, the value of the report lies in clarifying what is already in motion, what will require fresh authority or capacity, and how to sequence changes so that enforcement is coherent, rights-respecting, and workable in practice. Concurrently, the Report frames cybercrime and adjacent online safety harms as more than a law-and-order issue, describing them as a national security challenge with cross-border dimensions. While a security-first emphasis may be necessary to drive coordination and resourcing, it is equally important that, as these proposals take shape, enforcement remains rights-preserving, with precise legal thresholds, due-process safeguards, and protections for privacy, speech, and innovation. Beyond the Home Affairs Committee, parliamentary deliberations are also converging on information integrity, spanning fake news, misinformation, and editorial accountability. Most recently, the Parliamentary Standing Committee on Communications and Information Technology (IT) is reported to have adopted a draft recommending a comprehensive framework to address fake news, spanning platform liability, editorial duties across print, electronic, and digital media, and the treatment of AI-generated misinformation.[2] The draft reportedly proposes the establishment of mandatory fact-checking units and internal ombudsmen within media outlets, as well as coordination between ministries and platforms, and amendments to penal provisions to clarify accountability for editors, publishers, and platform operators. In parallel, MPs across party lines continue to raise these concerns through debates and questions, seeking clarifications from the government on the evolving dimensions of information integrity[3], online safety[4], AI[5], and OTT governance[6], among others.

---

[2] Rahi, A.(2025, September 5). New AI rules in India may force creators to label their content as AI-generated. *Hindustan Times.* <*https://www.hindustantimes.com/technology/new-ai-rules-in-india-may-force-creators-to-label-their-content-as-aigenerated-101757917113816.html*>

[3] Rajya Sabha Unstarred Question no. 3937.(2025,4th April)
< https://sansad.in/getFile/annex/267/AU3937_P45eRL.pdf?source=pqars>

[4] Lok Sabha Unstarred Question no.2952. (2025, 6th August
< https://sansad.in/getFile/loksabhaquestions/annex/185/AU2952_foNm40.pdf?source=pqals>

[5] Lok Sabha Unstarred Question no.3090. (2025, 19th March)
< https://sansad.in/getFile/loksabhaquestions/annex/184/AU3090_sDZA9w.pdf?source=pqals>

[6] Rajya Sabha Unstarred Question no. 2965. (2024, 20th Dec)
< https://sansad.in/getFile/annex/266/AU2965_KjJWgH.pdf?source=pqars >

Alongside parliamentary interventions, regulatory actions have also become more muscular. Over the years, MeitY has issued deepfake and misinformation advisories to social-media intermediaries (November 2023) and a further compliance advisory (December 2023) reiterating Rule 3(1)(b) duties.[7] Amidst concerns about electoral integrity and the spread of deepfakes, MeitY issued two advisories in March 2024 that encouraged tighter controls on AI outputs and provenance. Alongside, in November 2024, CERT-In also issued a deepfake threats and counter-measures advisory.[8]

On the content side, the Ministry of Information and Broadcasting (MIB) issued (i) an NDPS (Narcotic Drugs and Psychotropic Substances Act, 1985)-focused advisory cautioning OTT services against glamorising or promoting narcotic drugs and psychotropic substances and calling for disclaimers and due diligence (26 Nov 2024);[9] (ii) an "obscenity" advisory reminding OTT and social media publishers of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021(IT Rules 2021) Code of Ethics and applicable penal statutes (19 February 2025);[10] (iii) an advisory to align OTT releases with disability-rights and IT-Rules obligations following a Delhi High Court order (22 April 2025)[11] and (iv) an advisory to all media to refrain from live coverage of defence operations and troop movements in the interest of national security (26 April 2025).[12] Direct enforcement has run in parallel: after initial blocks in March 2024[13], authorities ordered Internet Service Providers (ISPs) to block over 20 OTT platforms for obscene/indecent content in July 2025, signalling willingness to use hard levers where advisories fail.[14]

Courts have played an essential role in clarifying interim boundaries while Parliament and the Executive consider broader changes to India's cyber governance framework. Expressing serious concern over objectionable and obscene content online, the Supreme Court, in a PIL filed in *Uday Mahurkar vs Union of India*[15], issued notice to the Union and major OTT/social platforms and sought detailed replies. The Court remarked that some form of regulation appears necessary and noted that it is for the Executive and the Legislature to introduce appropriate measures. Appearing for the Centre, the Solicitor General stated that regulations already exist and further measures

---

[7] MeitY, (2024, December 26) *Advisory* <https://www.meity.gov.in/static/uploads/2024/02/c9f89809b63d22656be38a166ef14949.pdf >
[8] MeitY (2025, April 4) *Press Release* < https://www.pib.gov.in/PressReleasePage.aspx?PRID=2119050 >
[9] I&B Ministry cautions OTT platforms against glorifying drug use. *The Indian Express.* <https://www.newindianexpress.com/nation/2024/Dec/17/ib-ministry-cautions-ott-platforms-against-glorifying-drug-use>
[10] MIB., (2025, February 19). *Advisory.* <https://mib.gov.in/sites/default/files/2025-02/advisory-dated-19.02.2025_0.pdf>
[11] MIB (2025, April 22). *Advisory* <https://mib.gov.in/sites/default/files/2025-04/advisory-dated-22.04.2025-1.pdf>
[12] MIB (2025, April 26), *Advisory.* <https://mib.gov.in/sites/default/files/2025-04/advisory-to-all-media-channels-dated-26.04.2025-1.pdf>
[13] PIB (2024, March 14). *Press Release.* < https://www.pib.gov.in/PressReleasePage.aspx?PRID=2014477>
[14] Pandey, D. (2025, July 25). ALTT, ULLU among over 20 OTT apps banned for obscene conten. *The Hindu.* <https://www.thehindu.com/news/national/altt-ullu-among-over-20-ott-apps-banned-for-indecent-representation-of-women/article69854104.ece>
[15] *Uday Mahurkar vs Union Of India* (2025) [W.P.(C) No. 313/2025]

are under consideration, flagging that some content is so perverse that age warnings are inadequate. The petition highlights the unrestricted availability of pornographic and sexually explicit material, including content involving minors and non-consensual contexts, across OTT catalogues and social-media pages. It warns of harms to children and youth, the risk of fostering deviant behaviour, and broader impacts on public morals, mental health, and safety. Counsel for the petitioner emphasised that the plea is not adversarial but seeks judicial intervention where prior representations have not yielded effective action.

In the Ranveer Allahbadia proceedings (arising from remarks made on India's Got Latent), the Supreme Court sharply criticised the language used and granted Allahbadia interim protection, initially restraining further shows and later permitting him to resume subject to decency/morality conditions and without prejudicing the case.[16] In addressing the related Cure SMA petition, a Bench of Justices Surya Kant and Joymalya Bagchi distinguished constitutionally protected expression from monetised "commercial speech" by influencers, making clear that when creators commercialise content, they bear heightened responsibilities, particularly where vulnerable groups may be harmed. The Court also directed the comendians to tender unconditional apologies on their social media platforms.[17] The Court also emphasised the need to frame broad-based guidelines for digital platforms and stand-up comedy, stressing the need to anticipate future challenges rather than respond to isolated controversies. It directed the Attorney General of India to assist in preparing such guidelines and tasked the MIB with drafting comprehensive rules in consultation with the News Broadcasters and Digital Association (NBDA) and other stakeholders.[18]

However, last year, the Court had also clarified that vulgarity is not a synonym for obscenity. In *Apoorva Arora v. State (NCT of Delhi)*[19], arising from the College Romance web series, the Court quashed proceedings under Sections 67 and 67A of the IT Act, 2000 emphasising that profanities and coarse banter, viewed in context and as part of a work taken as a whole, do not by themselves satisfy the statutory thresholds of lascivious or sexually explicit material. The ruling restrains overbroad policing of online language and re-centres the legal test: obscenity turns on prurience, sexual explicitness, and a tendency to deprave or corrupt, not on whether someone is personally offended.

In *Just Right for Children Alliance v. S Harish*[20], the Supreme Court set aside a Madras High Court decision that had held downloading and viewing child abuse material in

---

[16] Shah, M.(2025, Feb 18). Supreme Court slams YouTuber Ranveer Allahbadia for 'obscene' remarks, grants interim protection. *Supreme Court Observer.* <https://www.scobserver.in/journal/supreme-court-slams-youtuber-ranveer-allahbadia-for-obscene-remarks-grants-interim-protection/>

[17] (2025, August 26). SC: No free speech immunity for content by influencers. *Times of India.* <https://timesofindia.indiatimes.com/india/sc-no-free-speech-immunity-for-content-by-influencers/articleshow/123512489.cms>

[18] (2025, August 26). Consult NBDA, frame guidelines for influencers: Supreme Court to Centre. *India Today*. <https://www.indiatoday.in/india/law-news/story/not-free-but-commercial-speech-top-courts-tough-remarks-on-influencers-language-2777080-2025-08-26>

[19] *Apoorva Arora v. State (Govt. of NCT of Delhi)* [2024 INSC 223]

[20] *Just Right for Children Alliance & Anr v. S Harish & Ors* [2024 INSC 716]

private was not an offence under the Protection of Children from Sexual Offences Act (POCSO)/IT laws. The Court held that mere storage or viewing, where intent or knowledge is established, can amount to an offence under Section 15 of POCSO. The Court also made a notable terminological intervention, directing that the expression "child pornography" should no longer be used in judicial or administrative discourses. Instead, the term "Child Sexual Exploitation and Abuse Material (CSEAM)", which more accurately reflects the gravity of the offence, should be adopted. The Court reasoned that "pornography" carries connotations of adult consent and commodification of sex, which risks trivialising or mischaracterising the abuse of minors. The Court also went beyond punitive framing, stressing that law enforcement alone cannot address the systemic challenges of CSEAM and highlighted the urgent need for comprehensive sex education and sensitisation, both to prevent abuse and to reduce the demand that drives the circulation of exploitative material. This marks an important shift: rather than viewing CSEAM solely through a law-and-order lens, the Court situated it within a public health, education, and rights-based framework.

III. Critical Analysis: Opportunities and Gaps

3.1 Intermediary Liability and Safe Harbour

3.1.1 AI-Generated Content (Deepfakes, Synthetic Media, Misinformation)

- **Observation and Recommendation of the Committee:** The Committee observed (para 3.2.13) that the existing legal framework under the IT (Information Technology) Act, 2000 does not distinguish between synthetically generated and user-created content, despite the increasing misuse of deepfakes and AI tools for producing harmful or misleading material. To address this, the Committee recommends that, first, the law should be strengthened through explicit provisions that address AI-generated content. Second, it also proposes that MeitY develop a technological framework that mandates watermarking on all photos, videos, and similar content shared on digital platforms to help prove origin and make manipulation more difficult. To ensure the effective implementation and functioning of such an initiative, the Committee recommends that MeitY set uniform technical standards for media provenance, with CERT-In serving as the coordinator for monitoring and issuing detection alerts.

- **Commentary:** Previously, in the context of electoral integrity risks posed by generative AI, MeitY issued a series of advisories for intermediaries and platforms under the IT Act, 2000. The first advisory, issued in November 2023[21], emphasised intermediary obligations to identify and remove deepfake content within 36 hours of reporting, mandated that user agreements explicitly prohibit deepfakes, and reiterated strict compliance with the IT Rules, 2021, as a condition for retaining intermediary liability protection under Section 79(1) of the Act. Further strengthening this approach, MeitY issued a second advisory in December 2023[22] targeting AI-generated misinformation, particularly deepfakes. This advisory required platforms to clearly communicate prohibited content categories to users at registration and throughout platform usage, educate users regarding penal provisions under the IT Act, the Indian Penal Code (IPC), and other relevant laws and remove unlawful content proactively.

  In March 2024, MeitY introduced additional obligations[23], mandating that intermediaries/platforms: (i) prevent unlawful outputs under the IT Act/IT Rules; (ii) seek prior government approval before releasing any "under-tested" or "unreliable" model to Indian users; (iii) inform users that such models may

[21] PIB. (2023, Nov 7). Press Release <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1975445>
[22] PIB (2023, Dec 26), *Press Release* <https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542>
[23] MeitY. (2024, March 15). *Advisory* <https://www.meity.gov.in/static/uploads/2024/02/9f6e99572739a3024c9cdaec53a0a0ef.pdf >

be fallible; and (iv) file an action-taken/status report within 15 days. It also cautioned providers against enabling bias, discrimination, or threats to electoral integrity. On 15 March 2024, MeitY withdrew the prior-approval and 15-day reporting requirements, but retained the obligation to prevent unlawful outputs, expanding it to all laws in force and requiring intermediaries that facilitate AI-generated content to label outputs and embed durable metadata/unique identifiers capable of tracking subsequent edits and attributing changes to responsible users.

In December 2024, , MeitY had also called for Expressions of Interest under the IndiaAI Mission for watermarking and content-labelling tools to authenticate AI-generated material, which could serve as the building blocks of a provenance regime.[24] The Committee's proposal for uniform technical standards could gain traction if tied to international initiatives, such as the Coalition for Content Provenance and Authenticity (C2PA)[25], which utilises cryptographic methods to create tamper-evident metadata chains for digital media. Comparative frameworks such as the European Union's AI Act also offer useful direction; for instance, through transparency obligations on generative AI systems that require clear disclosures when content is AI-generated, safeguards against the generation of illegal content, and the publication of summaries of training data.

It is also worth noting that these recommendations sit within broader and unresolved questions about how to categorise and regulate AI-generated content and attribute content liability, particularly when such content may originate through a combination of user inputs, platform functionality, and generative models. In practice, this could give rise to multiple categories of content, including, but not limited to, traditional user-generated content (UGC), AI-assisted UGC (where human authorship remains primary but is shaped by AI tools), and fully AI-synthesised content (with minimal or no human authorship). This layering raises complex questions of attribution and responsibility. Should liability attach to the user who prompts the AI, the platform that provides the generative model, or both? If content emerges through hybrid processes, for instance, a user uploading a deepfake generated off-platform, or AI systems modifying existing UGC through auto-captioning or translation, how should accountability be apportioned? These distinctions matter, since they cut to the scope of safe harbour: while traditional UGC falls squarely within the *Shreya Singhal* framework, AI-assisted content blurs the line between hosting and creation, potentially narrowing the immunity platforms may legitimately claim.

[24] (2024, December 17). MeitY invites proposals to develop trusted AI ecosystem. *The Economic Times*. <https://economictimes.indiatimes.com/industry/services/retail/hes-into-puma-shes-into-zara-gender-gap-shows-in-gen-z-brand-love/articleshow/123494920.cms>

[25] Coalition for Content Provenance and Authenticity. <https://c2pa.org/>

3.1.2 Periodic Review of Safe Harbour Immunity

- **Observation and Recommendation of the Committee:** The Committee proposes (para 3.2.15) a periodic review of the safe harbour protections available to intermediaries under Section 79 of the IT Act.. This is grounded in the Committee's concern about the continued tenability of the liability exemption clause in light of emerging technological threats, growing instances of platform misuse, and repeated non-compliance with lawful takedown or data requests from law enforcement agencies.

- **Commentary:** The stated objective is to rebalance platform immunity with accountability, reflecting a regulatory environment in which the relevance of safe harbour is being questioned. This issue was previously addressed during the Digital India Act (DIA) consultations in 2023[26], where the continued relevance of safe harbour as a default legal protection was itself brought into question, and proposals ranged from outright withdrawal to the creation of a license-based regime[27] under which only compliant platforms would retain protection. In November 2024, the IT Minister also reaffirmed the Indian government's intent to revisit the safe harbour provisions under Section 79, citing the growing misuse of platforms for spreading misinformation, inciting riots, and even enabling terrorism.[28] He emphasised the need for a new accountability framework, especially in India's complex socio-political environment.[29] Moreover, recent submissions made by the MIB to the Parliamentary Standing Committee on Communications and IT indicate that the government is considering revisions to intermediary due diligence requirements, including a potential reconfiguration of safe harbour protections, particularly in the context of curbing misinformation and fake news.[30]

  However, any reconsideration should preserve the core safe-harbour principle, i.e. intermediaries should not be treated as publishers of third-party content and incur liability only for failing to execute reasoned court orders or valid

---

[26] Deep, A. (2023, March 10). Centre to reconsider 'safe harbour' clause in IT law. *The Hindu.* <https://www.thehindu.com/news/national/centre-rethinking-safe-harbour-concept-in-it-act-revamp/article66599676.ece>

[27] Ganesan, A. (2023, Sept 19). Upcoming Digital India Bill May Do Away with Prevailing Safe Harbour Regime: Report. Medianama. <https://www.medianama.com/2023/09/223-digital-india-bill-safe-harbour-regime/>

[28] MIB.(2024, Nov 16). *Press Release.* https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2073917#:~:text=The%20spread%20of%20fake%20news,nation.%E2%80%9D%2C%20he%20added.

[29] (2024, November 18). Safe harbour clause for platforms needs a revisit, says Ashwini Vaishnaw. *The Indian Express.* <https://indianexpress.com/article/business/safe-harbour-clause-for-platforms-needs-a-revisit-says-vaishnaw-9673392/#:~:text=IT%20Minister%20Ashwini%20Vaishnaw%20(File,a%20National%20Press%20Day%20event.>

[30] Nair, S.K., Deep, A. (2025, May 7). Centre plans revision of 'safe harbour' clause in IT Act. *The Hindu* <https://www.thehindu.com/news/national/to-check-fake-news-government-rethinks-safe-harbour-for-online-platforms/article69544723.ece#:~:text=In%20a%20bid%20to%20disincentivise,way%20to%20address%20fake%20news.>

Section 69A directions within calibrated timelines. Shifting toward licence-style or permission-based immunity, or conditioning protection on vague "cooperation" standards, invites prior restraint, over-removal of lawful speech, and uneven enforcement.

3.1.3 Enhanced Accountability for Platforms

- **Observation and Recommendation of the Committee:** In paragraph 3.2.16, the Committee further notes that specific social media intermediaries have failed to cooperate with law enforcement agencies in cases involving morphed videos, fake profiles, misinformation, and communal content. Such non-compliance has been explicitly characterised as potentially abetting criminal activities and undermining public order. In response, the Committee has recommended that MeitY, in consultation with the MHA and the Ministry of Law and Justice, consider amending the IT Act to introduce explicit provisions holding social media intermediaries legally accountable for failing to act on lawful takedown orders within prescribed timelines. The suggested amendments include a system of graded penalties, ranging from monetary fines to potential suspension of operations in cases of persistent non-compliance, while underscoring the need for due process and appeal mechanisms to safeguard freedom of expression and procedural fairness.

- **Commentary:** The proposal to include the suspension of operations risks being disproportionate and overbroad, and the threat of suspension could compel platforms to err on the side of over-compliance to avoid the risk of being de-platformed altogether. This is particularly concerning in contexts where platforms serve as critical spaces for democratic deliberation, minority expression, and independent journalism. A current cautionary example is Nepal. Following an order that foreign platforms register and appoint a local contact within seven days, authorities blocked access to 26 services (including Facebook, Instagram, YouTube, and X) when most did not comply by the deadline.[31] The move triggered large, youth-led protests, at least 19 deaths, and ultimately a reversal of the ban within days.[32] Although the initial trigger was framed as procedural non-compliance (registration), the remedial measure proved to be disruptive and disproportionate at the national scale.[33] Global benchmarks tend to reserve platform access restrictions for narrow, high-risk scenarios and only as a last resort with due process.

[31](2025, Sept 9). Nepal bans 26 social media platforms: full list from facebook, instagram, whatsapp to youtube. *The Economic Times.* <https://economictimes.indiatimes.com/news/new-updates/nepal-bans-26-social-media-platforms-full-list-from-facebook-instagram-whatsapp-to-youtube/articleshow/123766916.cms>

[32]Ng, K. (2025, Sept 9). Nepal lifts social media ban after 19 killed in protests. *BBC News*. <https://www.bbc.com/news/articles/cp98n1eg443o>

[33] Dahal, P., Atkinson,E., Khan, I.(2025, Sept 10). What we know about Nepal anti-corruption protests as PM resigns. *BBC News.* <https://www.bbc.com/news/articles/crkj0lzlr3ro>

Under the EU's Digital Services Act, enforcement escalates through audits, corrective action plans, and fines (up to 6% of global turnover)[34].emporary service suspension is contemplated only where persistent, serious infringements cause grave harm (e.g., offences involving a threat to life or safety) and must follow a defined legal procedure. Human-rights guidance likewise warns that blanket blocking of services rarely meets necessity and proportionality tests; United Nations (UN) and Office of the United Nations High Commissioner for Human Rights (OHCHR) reports have repeatedly condemned shutdowns and generic platform blocks for their systemic impact on expression and access to information.[35].[36]

- **Observation and Recommendation of the Committee:** The Report also extends this logic into the institutional framework. In Chapter 4, the Committee reiterates and recommends revisiting safe harbour protections, particularly when intermediaries fail to act after receiving legitimate requests regarding data access and the removal of online unlawful content, to ensure accountability of IT intermediaries whose platforms are being misused. The Committee observes that while Significant Social Media Intermediaries (SSMIs) are already required under the IT Rules 2021 to appoint compliance officers, many non-SSMIs are subject only to lighter obligations, and some foreign-based intermediaries lack a local presence altogether. In response (para 4.1.8), it recommends a mandatory national registration system for all intermediaries, ensuring local grievance and nodal officers, and proposes that SSMIs such as Facebook, WhatsApp, and Telegram be required to appoint regional nodal officers to strengthen coordination with law enforcement.

  The report also highlights the absence of victim compensation mechanisms and recommends amending the IT Act to hold platforms accountable for psychological, reputational, or financial harm resulting from their failure to address malicious content. The Committee observed that there is a need for a more user-friendly and transparent grievance redressal system to build public trust and ensure timely and effective complaint resolution. In this regard, it recommends standardising the process by adopting a uniform format for filing complaints and establishing clear timelines for acknowledgement and resolution. It also stresses public disclosure of grievance statistics, including data on complaints received, resolved, and pending. The Committee also links grievance redressal to broader regulatory concerns, suggesting that its integration with emerging data protection frameworks would create a more

[34] The enforcement framework under the Digital Services Act, *European Commission.* <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement>

[35](2022, June 24) Internet shutdowns impact human rights, economy, and day to day life. *United Nations News, Global Perspective Human Stories, United Nations.*< https://news.un.org/en/story/2022/06/1121242>

[36](2023, June 22) Internet shutdowns: UN report details 'dramatic' impact on people's lives and human rights, *United Nations Human Rights, Office of the Commissioner. United Nations.* <https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human>

cohesive system that addresses privacy, content moderation, and cybersecurity in a coordinated manner.

- **Commentary:** Shifting to a mandatory registration regime would move India from a conduct-based framework to a permission-based one, potentially raising entry costs for small and open-source services. Moreover, instead of solely relying on increasing compliance duties, a more effective strategy would involve direct evaluation of the efforts put in towards compliance. This approach should include regular dialogues between regulatory bodies and companies, creating a platform for mutual understanding and agreement on the best ways forward. Such interactions can lead to a deeper understanding of the challenges faced by companies and enable the development of more practical and impactful compliance strategies.

  While redress for unlawful content as well as psychological, reputational, or financial harm is essential, tying platform liability to a general "failure to address malicious content"[37] risks converting safe-harbour into de facto publisher liability for third-party speech. Unlike traditional publishers, intermediaries neither initiate nor editorially vet all content on their platforms. Making them liable for harm caused by content they host, without a clear, legally enforceable trigger, effectively transforms them into arbiters of speech, undermining both freedom of expression and the operational viability of platforms. The proposal also leaves unresolved key questions of causation, such as: (i) what degree of inaction leads to liability?, (ii) how is "malicious content" defined, by statutory offences, regulatory guidance, or platform judgment?, and (iii) should liability fall entirely on the intermediary, or be shared with the primary wrongdoer? Without carefully tailored safeguards, an expansive compensation regime risks undermining innovation while creating excessive compliance burdens, even for smaller intermediaries.

  In this respect, The Dialogue's Policy Framework #BreaktheSilo: Streamlining Gender Safety in the Digital Space[38] offers practical guidance for a multistakeholder, whole-of-society approach to online harms. It organises action into six linked stages: Access, Prevention, Intervention, Response & Redressal, Recovery & Healing, and Research, and sets out clear roles and duties for each stakeholder at every stage. Responsibilities are treated as shared and iterative, with coordination mechanisms and feedback loops that enable practice to improve over time, spreading effort across the entire safety pipeline rather than just its most visible points.

[37] Parliamentary Standing Committee on Home Affairs. (2025, August 25). "Cyber Crime – Ramifications, Protection and Prevention", Parliamentary Standing Committee on Home Affairs.(Para 4.1.11, Pg no.65). Report no.254 <https://sansad.in/getFile/rsnew/Committee_site/Committee_File/ReportFile/15/197/254_2025_8_12.pdf?source=rajyasabha>

[38] Shreya,S., Saxena, G. (2023, Oct 17). Policy Framework – #BreaktheSilo: Streamlining Gender Safety in the Digital Space. *The Dialogue.* <https://thedialogue.co/publication/policy-framework-breakthesilo-streamlining-gender-safety-in-the-digital-space>

3.2 Cybercrime: Legal and Institutional Framework

The Committee acknowledges that India has a robust legal and institutional framework to address cybercrime, particularly through the IT Act regime, as well as through operational mandates issued by CERT-In. It simultaneously recognises that this framework faces persistent challenges due to technological advancements and increasingly sophisticated tactics deployed by cybercriminals.

3.2.1 VPNs and Other Privacy-Enhancing Technologies (PETs)

- **Observation and Recommendation of the Committee:** The Committee highlights the increasing use of encrypted communication platforms, Virtual Private Networks (VPNs), and the dark web in facilitating a wide array of unlawful and harmful activities, from narcotics and arms trafficking to child exploitation, cyber terrorism, and online radicalisation.[39] Inputs from enforcement agencies (para 2.3.11) such as the CBI and NIA reveal how these technologies are being leveraged to obscure identities, bypass jurisdictional enforcement, and frustrate evidence-gathering efforts. In particular, the NIA highlights the challenges in tracking activities routed through encrypted messaging apps and VPNs, especially when foreign platforms fail to comply with lawful requests for data disclosure, citing jurisdictional immunity.

  To address these challenges, the Committee recognises the effectiveness of existing legal tools, including CERT-In's data preservation mandates for VPN providers, while also highlighting persistent non-compliance among international actors (para 4.1.5 [a]). It recommends (para 4.1.7) a multi-pronged approach that includes enforcing VPN logging obligations, enhancing international cooperation, and adopting robust technical measures for lawful access. Notably, the Committee strikes a cautious balance by also recommending that these requirements be accompanied by strict safeguards to protect citizens' privacy. Additionally, it calls for greater investment in privacy-preserving technologies and public awareness campaigns on cybersecurity hygiene and responsible VPN use.

- **Commentary:** This dual emphasis on effective enforcement and privacy protection points to the Committee's recognition of the fine line between surveillance for security and upholding fundamental rights in the digital domain. However, its operationalisation will depend on how lawful access mechanisms are structured and whether procedural safeguards are meaningfully implemented in practice.

3.2.2 Strengthening Cross-Border Cooperation and Cybercrime Infrastructure

- **Observation and Recommendation of the Committee:** While the Committee appreciates (para 4.1.9) that the IT Act, 2000 and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS, 2023), enable law enforcement to act

[39] Kumar,R.(2025, July 19). Dark web, VPN make probe tough for Delhi police. *The Tribune.* <https://www.tribuneindia.com/news/delhi/dark-web-vpn-make-probe-tough-for-cops/>

in cross-border scenarios where Indian interests are impacted, it flags major operational hurdles in securing international cooperation. To address this, it calls for the establishment of a dedicated International Cybercrime Liaison Unit, staffed with specialised legal and technical experts. It also recommends strengthening Mutual Legal Assistance Treaties (MLATs) and other bilateral or multilateral frameworks, while initiating joint training exercises in digital forensics, virtual asset tracing, and blockchain analysis.

- **Commentary:** India's current tools are too slow for time-sensitive digital evidence, and non-participation in frameworks such as the Budapest Convention further limits access to provider data. In the near term, India should prioritise targeted bilateral data-access agreements with the United States and key European jurisdictions. In particular, pursuing a U.S. CLOUD Act, paired with procedural alignment on both sides, would create a faster, lawful channel to major providers. In parallel, the MLAT workflow should be modernised for the digital age. The new UN Cybercrime Convention[40] offers an additional avenue for cooperation, but its utility will depend on the speed of domestic ratification and the specificity of its procedural safeguards.

3.2.3 Capacity: Rank, Training, Labs, AI-Driven Computer Telephony Integration (CTI) for CERT-In

- **Observation and Recommendation of the Committee:** The Committee raises concerns (para 4.1.12) over the competence and rank of officers currently handling cybercrime cases. While Section 78 of the IT Act mandates investigation by an officer not below the rank of Inspector, the Committee argues that cybercrimes should be handled by officers of a higher rank who are well-trained in digital forensics, cyber law, and investigative techniques. It recommends introducing a certified foundational course in cybersecurity as a prerequisite for police recruitment and the establishment of dedicated cybercrime training and research centres across states, supported by advanced forensic labs accessible to law enforcement agencies nationwide.

  To further strengthen CERT-In's capabilities, the Committee recommends (para 3.15.6) adopting an AI-driven Cyber Threat Intelligence Platform that enables quicker and more intelligent identification and handling of cyber threats. Furthermore, the Committee encourages CERT-In to establish robust partnerships with start-ups and academic institutions to promote innovation and cultivate a skilled cybersecurity workforce. The Committee also recommends conducting regular, flexible cybersecurity drills in collaboration with sectoral teams to ensure CERT-In remains agile and prepared to tackle emerging cyber challenges promptly.

- **Commentary:** The emphasis on improving the rank, training, and technical capacity of cybercrime investigators is commendable. However, the effectiveness of these measures will hinge on institutional incentives, sustained

[40]United Nations Office on Drugs and Crime.
<https://www.unodc.org/unodc/cybercrime/convention/home.html>

funding, and clear lines of accountability, issues the Committee only gestures at. A model with public reporting on training uptake, case outcomes, and lab turnaround times would make these investments verifiable and outcome-oriented.

3.2.4 Early-Stage Preservation, Protocols, and NIA Coordination

- **Observation and Recommendation of the Committee:** The Committee notes the procedural gaps highlighted by the NIA (para 3.10.30), particularly the delays in data preservation during the early stages of cybercrime reporting. To address this, it recommends that the MHA establish standardised protocols and monitoring systems to ensure timely data preservation. It further urges that State police be directed to initiate preservation requests within the first 24 hours of a cybercrime complaint, to safeguard volatile digital evidence such as IP logs and server files before the NIA assumes control. The Committee also recommends that SSMIs be mandated to provide the required data to NIA promptly, regardless of the data centre's location.

3.2.5 Toward a Unified Cybercrime Law & Integrated Task Force; Penalties

- **Observation and Recommendation of the Committee:** The Committee notes that the current legal framework for cybercrime is fragmented across multiple statutes, resulting in judicial and enforcement inefficiencies. It recommends (para 4.1.18) drafting a unified and comprehensive cybercrime law that clearly defines offences, addresses challenges posed by emerging technologies, and incorporates flexible yet strong penal provisions. It further recommends the creation of a national-level Integrated Cybercrime Task Force with a mandate to investigate complex, transnational digital crimes. The Committee also calls for a review of penalties under the IT Act, many of which are currently bailable or carry low fines, and recommends introducing harsher punishments to enhance deterrence (para 4.1.10).

  The Committee underscores the importance of multi-stakeholder collaboration, both domestically and internationally. It calls for the development of interoperable platforms for real-time threat intelligence sharing and suggests creating a multilingual, citizen-friendly online portal for reporting cybercrimes. The Committee also highlights best practices from states like Telangana, Maharashtra, and Kerala, and encourages their replication nationwide with coordination from the MHA.

  The Committee also recommends (para 3.16.7) to the Ministry of Education that Cyber Awareness and Curriculum Integration, including cybercrime prevention and cyber hygiene education, be introduced into the school curriculum from early grades through senior secondary level, across both Central and State boards, to ensure universal access. It also recommends introducing a mandatory cyber education subject within non-technical courses in colleges and universities. These modules should include cyber awareness, digital safety, responsible online conduct, and fundamental data privacy principles to build a resilient digital generation.

3.3 Sectoral Governance

3.3.1 OTT and Digital Media

- **Observation and Recommendation of the Committee:** The Committee observes (para 3.2.17) that OTT platforms have become a dominant source of entertainment in India, with a reach even greater than traditional cinema and a significant audience comprising minors. It notes that, unlike films, which require mandatory pre-certification under the Cinematograph Act, OTT content currently operates on a self-classification model with only post-release grievance redressal mechanisms as per the IT Rules, 2021. While the current framework includes age ratings, parental controls, and a grievance mechanism, the Committee highlights the persistent gaps of pre-release checks and inadequate age verification systems, particularly in light of the vulnerability of minors to potentially harmful or age-inappropriate content.

  To achieve the same goal, the Committee proposes the establishment of an independent expert panel comprising child rights advocates, educators, legal professionals, social scientists, and community stakeholders. This panel would serve a dual role: first, as a post-release watchdog empowered to review user-flagged or trending content; and second, as a norm-setting body, it is tasked with formulating culturally sensitive content guidelines and recommending penalties for non-compliance.

- **Commentary:** The proposal of a Post-Release Review Panelentails significant overlapalready assigned to existing regulatory tiers under Level II and Level III under Part 3 of the IT Rules, 2021. Moreover, without a clear legal mandate, granting an independent body norm-setting and penal powers risks regulatory overreach and unconstitutional restrictions on speech. The expert panel may still serve a helpful function if repositioned as an advisory or thematic oversight body, specifically focused on children's content standards.

  Moreover, the Committee's emphasis on cultural ethos and sensitivity as a content benchmark, while well-intentioned, risks becoming a vague and overly subjective standard. Content suitability should be assessed using child development norms, psychological safety indicators, and precise age-based classification, rather than broadly moralistic or culturally leaning filters. Moreover, mandating enhanced age-verification and parental control mechanisms should not rely on intrusive or privacy-infringing identity verification methods (such as Aadhaar uploads or facial recognition), but instead leverage privacy-preserving technologies.

  In parallel, early in 2025, parliamentary deliberations had also floated the idea of a Unified Media Council overseeing OTT, print, TV, and digital platforms.[41]

[41] Agrawal, A.(2025, March 23). Parliamentary panel seeks common media council. *Hindustan Times.* <https://www.hindustantimes.com/india-news/parliamentary-panel-seeks-common-media-council-101742669710282.html>

While this signalled a push for harmonised editorial accountability across media, it also raised concerns about whether OTT-specific safeguards will be subsumed into broader structures or layered with additional compliance obligations.

3.3.2 App Store Ecosystem Regulation

- **Observation and Recommendation of the Committee:** The Committee emphasises the importance of robust data protection and security measures across the app ecosystem, recommending that all applications strictly adhere to the standards prescribed under applicable laws and regulations. It highlights the critical role of app stores (para 3.2.19) in ensuring user safety. It suggests introducing compliance requirements for them, including regular audits to detect and prevent the distribution of malicious or harmful applications. Additionally, the Committee sees value in promoting self-reliance and innovation, recommending the development of an indigenous app store to provide a secure and supportive platform for Indian startups. This approach aims to enhance consumer trust, strengthen cybersecurity, and encourage domestic technological growth.

- **Commentary:** While the Committee's push for compliance and auditing is well-intentioned, implementation choices will shape real-world outcomes. Additional obligations mayimpose higher compliance costs. These are likely to fall heaviest on smaller developers and new app stores. Regulator pre-publication checks for every app may add fixed costs, slow time-to-market, and undercut the goal of nurturing indigenous app-store entrants. This is particularly relevant for India's fast-growing app market, where Apple estimates the App Store facilitated ₹44,447 crore in developer billings with 1.1 billion iOS downloads[42], and Google Play/Android ecosystem generated ₹4 lakh crore and supported 35 lakh jobs in 2024. [43]

3.3.3 Digital Advertising

- **Observation and Recommendation of the Committee:** The Committee highlights the growing risks posed by unverified offshore advertisers in the Indian digital ecosystem, particularly in relation to deceptive, fraudulent, and misleading advertising practices. It recommends (para 3.3.4) that the MIB introduce a robust digital verification system for all offshore advertisers targeting Indian users. This system should include mechanisms such as mandatory upload of official documents, live video-based identity verification, and the adoption of zero-trust security frameworks, where every access request, including those related to ad edits, payment details, or identity changes, is continuously authenticated and monitored.

---

[42] (2025, April 28). New study finds App Store ecosystem in India facilitated ₹44,447 crore in billings and sales in 2024. *Apple Newsroom.* <https://www.apple.com/in/newsroom/2025/04/app-store-ecosystem-in-india-facilitated-rs-44447-crore-in-billings-and-sales/>

[43] (2025, July 23).Google Play,Android fuel Rs 4 lakh crore app revenue, economy boost in India during 2024: Report.*The Economic Times.* <https://economictimes.indiatimes.com/tech/technology/google-play-android-fuel-rs-4-lakh-crore-app-revenue-economy-boost-in-india-during-2024-report/articleshow/122852998.cms?from=mdr>

- **Commentary:** The MIB repeatedly cautioned against offshore betting and gambling platforms, especially their reliance on surrogate advertising, through a series of advisories. Previously, in 2022[44] and 2023[45], the Ministry warned television broadcasters, newspapers, and digital publishers to refrain from carrying such advertisements. In August 2023, another advisory broadened the scope significantly to include online advertisement intermediaries, social media platforms, and ASCI itself.[46] The advisory explicitly identified surrogate techniques, including betting operators masking as news portals, sports blogs, or OTT content with branding designed to mimic gambling sites. It also warned that violations could invite action under the Consumer Protection Act, 2019, the Cable Television Networks Regulation Act, 1995, the Press Council Act, 1978, and the IT Rules, 2021. Importantly, it situated the concern not only in terms of consumer harm but also in terms of financial security, highlighting the risks of money laundering, fund outflows, and disproportionate exposure of youth and children, particularly during major sporting events such as cricket tournaments.

  In May 2024, the Supreme Court mandated self-declaration certificates (SDCs) for advertisements in sensitive sectors[47], including food, health, and education, requiring advertisers to attest compliance with applicable frameworks, including the Food Safety and Standards Act, 2006, the Drugs and Magic Remedies (Objectionable Advertisements) Act, 1954, and the Consumer Protection Act, 2019. The SDC regime introduced a formal compliance mechanism at the point of ad release, marking a shift toward greater accountability in high-risk categories.

  Building on these developments, the MIB has indicated its intent to establish a rules-based framework for online advertising. In December 2024, through its Third Report on Demands for Grants (2024-25*)*, MIB informed the IT Committee that it was in the process of formulating rules for online advertising.[48] This direction was reiterated in a July 2025 parliamentary briefing, where draft rules were noted to be under inter-ministerial consultation.[49] These initiatives build on the July 2023 amendment to the

---

[44] *PIB*. (2022, Oct 3). *Press Release* <https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1864846#:~:text=The%20Ministry%20has%20stated%20that%20such%20advertisements%20are%20not%20in,Saurabh%20Singh >

[45] MIB. (2023, April 6). *Advisory.* <https://mib.gov.in/sites/default/files/2024-02/06.04.2023%20Advisory%20on%20Betting%20Advertisements%20%281%29.pdf>

[46]MIB,.(2023, Aug 25). *Advisory* <https://mib.gov.in/sites/default/files/2024-02/Advisory%20dated%2025.08.2023%20with%20enclosures%20%282%29.pdf>

[47] *Indian Medical Association vs Union Of India* [WP (CIVIL) NO. 645/2022]

[48] Farooqui, J. (2025, Jan 2). Working on rules for regulating online ads: MIB tells parliamentary panel. *The Economic Times.* <https://economictimes.indiatimes.com/industry/services/advertising/working-on-rules-for-regulating-online-ads-mib-tells-parliamentary-panel/articleshow/116868373.cms?from=mdr>

[49]PRESS RELEASE., (2024, Dec 18). "The Third Report (Eighteenth Lok Sabha) of the Standing Committee on Communications and Information Technology (2024-25) on DFG (2024-25) relating to the ministry of information and broadcasting. *Lok Sabha Secretariate*"<https://sansad.in/getFile/lsscommittee/Communications%20and%20Information%20Technology/pr_files/PRESS%20RELEASE%20(E)%20OF%203RD%20REPORT%20OF%20MIB.pdf?sourc

Allocation of Business Rules, which brought online advertising, online films and audiovisual content, and digital news explicitly within MIB's remit.[50]

3.3.4 Telecom: Spam/Fraud Rails, MNVS, UTMs

- **Observation and Recommendation of the Committee:** The Committee commends the DoT for significant initiatives leveraging telecom resources against cybercrime, notably the Sanchar Saathi portal for citizen identity protection and the Centralized International Out Roamer (CIOR) system, which blocked over 1.35 crore spoofed calls in a single day and reduced such incidents by 98%. ItThe Committee also notes the innovative use of AI, facial recognition, and the Financial Fraud Risk Indicator (FRI) in preventing telecom-related fraud. Further, the Digital Intelligence Platform (DIP) has been recognised for facilitating real-time collaboration across key sectors, including banks and law enforcement, to identify and act against telecom-linked financial fraud. To To keep pace with evolving fraud techniques,the Committee recommends enhanced integration and automation of data flows between platforms such as Sanchar Saathi, DIP, and law enforcement databases to improve speed and coordination in response efforts.

  On the regulatory front, the Committee recommends the strengthening of frameworks governing the use of automatic calls, bulk SMSs, and Voice over Internet Protocol (VoIP) to prevent their exploitation for phishing and spam campaigns. Continued investment is encouraged in indigenous AI-based solutions such as ASTR (AI and Facial Recognition-powered SIM verification) to tackle identity fraud at the source during SIM issuance (para 3.4.10). The Committee records that about 570 banks and financial institutions are using DIP to access the Mobile Number Revocation List (MNRL) and fraud indicators, leading to action on 20.89 lakh accounts. It recommends ensuring swift sharing of risk alerts and revocations from all institutions to minimise manual delays in addressing fraud. (para 3.4.11)

  In response to the growing volume of complaints against Unregistered Telemarketers (UTMs), the Committee recommends that the Telecom Regulatory Authority of India (TRAI) develop real-time detection tools to identify and block such actors proactively. It calls for the creation of a centralised blacklist database, accessible across all Telecom Service Providers (TSPs), to enable swift and coordinated disconnection of offending numbers (para 3.5.18).

  Recognising the importance of public awareness in curbing telecom-related fraud, the Committee recommends intensifying multilingual, cross-platform awareness campaigns, particularly targeting rural and regional populations.

---

e=loksabhadocs#:~:text=The%20Standing%20Committee%20on%20Communications,BIND%20Scheme%2D%20Challenges%20and%20Measures>

[50]Cabinet Secretariat,. (2023, July 28). *Notification.* <https://cag.gov.in/uploads/ae_circulars_office_orders/CircularsOfficeOrders-064febc5c859e72-26175217.pdf>

Citizens should be better informed about how to report fraud and secure their mobile credentials. It also recommends scaling the Mobile Number Validation Service (MNVS) nationally, in partnership with banks, Non-Banking Financial Companies (NBFCs), and fintechs, to limit the use of phone numbers in mule or fraudulent accounts (para 3.4.9).

- **Commentary:** The MNVS platform under the Draft Telecom Cybersecurity Amendment Rules published in June 2025 is still in the draft proposal stage, but at least one major bank has already begun piloting the new mechanism.[51] The draft rules propose a tiered pricing model, with a rate of ₹1.5 per request for authorised government entities and ₹3 per request for all other entities. By expanding MNVS to non-licensee entities, such as fintechs and OTT apps, the rules risk overreach into digital services governance through telecom law. Without clear guardrails, this could lead to fragmented compliance burdens, identifier-based exclusion risks (especially for users with ported/shared SIMs), and potential misuse of KYC-linked data without sufficient due process or purpose limitation.

  In the context of spam, TRAI issued amendments to the Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018, in February 2025 (the Second Amendment Regulations, 2025). While these reforms represent an essential step toward addressing the scale of spam and fraudulent communications, they are not without structural and operational challenges. The TCCCPR framework, as amended, imposes significant compliance burdens, particularly on smaller enterprises, by requiring strict technical and procedural standards without considering the volume of communication, business model, or sectoral risk. It also introduces regulatory redundancy, particularly where consent frameworks under TCCCPR now overlap with those under the Digital Personal Data Protection Act, 2023 (DPDPA). The absence of interoperability between the Digital Consent Acquisition (DCA) and other sector-specific or app-based consent mechanisms may result in duplicative obligations, increased costs, and user consent fatigue. Moreover, enforcement could remain fragmented, if there is limited coordination among TRAI, DoT, and other regulators, such as the RBI or MeitY. These limitations in the TCCCPR regime must be acknowledged and addressed, particularly in light of the Committee's call for further regulatory tightening. Without such corrective efforts, the layering of new controls on top of an already burdensome system risks compounding inefficiencies rather than resolving the systemic problem of unsolicited and fraudulent communication.

[51] (2025, June 27). Digital safety: DoT proposes stricter cybersecurity rules; central Mobile Number Validation Platform to combat fraud. *Times of India* <https://timesofindia.indiatimes.com/business/cybersecurity/digital-safety-dot-proposes-stricter-cybersecurity-rules-central-mobile-number-validation-platform-to-combat-fraud/articleshow/122106834.cms>

3.3.5 Financial Influencers

- **Observation and Recommendation of the Committee:** The Committee observes (para 3.8.9) that the rise of financial influencers, or "finfluencers," in India has prompted growing regulatory attention due to the risk of misinformation, fraud, and manipulation in digital investment advice. It highlights the issue, noting the proliferation of unregistered finfluencers who use social media platforms to promise unrealistic returns and promote questionable financial products.

  To address this, the Committee recommends thatSSMIs permit only Securities and Exchange Board of India (SEBI)-registered financial influencers to market and advise on investments, and that SEBI explore the use of a "verified tick" for registered advisors. It further urges mandatory disclosures and conduct norms such as registration numbers, disclaimers, and potential conflicts of interest on their profilesThe Committee has also called for a coordinated approach between SEBI and MeitY to identify and remove non-compliant content and accounts swiftly. The Committee also urges (para 3.8.10) collaboration with platforms to leverage AI tools for content monitoring, enable public reporting of suspect promotions, undertake strict enforcement against misleading information, and run regular investor awareness campaigns.

- **Commentary:** These proposals emerge in parallel to SEBI's ongoing crackdown on misleading financial content. SEBI has already removed over 15,000 deceptive sites and penalised high-profile finfluencers for offering unregistered investment advice, such as PR Sundar and Asmita Patel. While influencers currently fall outside the purview of SEBI's Investment Adviser and Research Analyst regulations, they may still be held accountable under broader provisions, such as Section 12-A of the SEBI Act and the PFUTP Regulations, which prohibit misleading and manipulative practices.[52] India's concerns echo global regulatory developments.

  In the United States, the Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA) have taken action against financial influencers who fail to disclose promotional arrangements or provide misleading investment advice. These agencies emphasise the importance of transparency, and recent enforcement actions show the risk of civil and criminal penalties for non-compliance. Notably, the SEC fined Kim Kardashian $1.26 million for promoting a crypto token without disclosure.[53]

  In the United Kingdom, the Financial Conduct Authority (FCA) has issued guidance on social media promotions and brought criminal charges against

[52] Raj, R.(2025, March 23). SEBI's Crackdown On Unregistered 'Finfluencers': Key Measures By The Regulator. *Outlook Money* <https://www.outlookmoney.com/news/sebis-crackdown-on-unregistered-finfluencers-key-measures-by-the-regulator >

[53] Ghosh, S.(2022, Oct 10). Explained | Why did the U.S. SEC charge Kim Kardashian for 'touting' cryptocurrency?. *The Hindu.* *<https://www.thehindu.com/business/markets/explained-why-did-the-us-sec-charge-kim-kardashian-for-touting-cryptocurrency/article65975497.ece>*

influencers promoting high-risk investment schemes.[54] The FCA warns that promotions lacking balanced information or proper authorisation may breach financial promotion rules under the Financial Services and Markets Act (FSMA).

Beyond the securities market, influencers and endorsers are also subject to consumer protection and advertising rules. that mandate clear disclosures, due diligence, and liability for misleading claims. Under the Consumer Protection Act, the CCPA's 2022 Guidelines treat influencer posts as advertising, require truthful, substantiated endorsements, and mandate clear, platform-native disclosures wherever there is a "material connection" (payment, gifts, affiliate links, etc.), with penalties and endorsement bans available for violations. In January 2023, the government issued "Endorsement Know-hows!" to effectuate these duties for celebrities, influencers and virtual influencers, specifying prominent disclosure labels and placement so users can't miss them. In parallel, the advertising self-regulator The Advertising Standards Council of India (ASCI) also requires prominent, standardised disclosure tags on influencer ads and holds both advertisers and creators responsible for substantiating claims, with tighter expectations for higher-risk categories.

The regulatory treatment of India's fast-growing creator economy merits close attention in the coming months, given sustained action across finance, advertising, and content regulation. As discussed above, these developments signal that creator obligations are moving from soft guidance to conduct norms and enforceable duties. This shift matters because the creator economy has become both a commercial and cultural force, with around 40 lakh active creators and the influencer marketing segment valued at approximately ₹3,000-₹3,600 crore as per a 2025 report.[55] While many creators are not yet fully monetising, the figures underscore the rapid scale and stakes of the creator and influencer economy.

In the South Asian context, the creator economy encompasses not only commerce but also speech and counter-speech, facilitating new forms of participation, cultural production, and dissent. Regulation, therefore, needs to be carefully balanced: strong enough to tackle illegal and harmful content, yet measured enough to preserve space for legitimate expression and innovation. As the Supreme Court itself has urged through its calls for broad-based digital guidelines, the challenge ahead is to consolidate scattered practice into clear, rights-respecting rules that can both safeguard users and sustain a vibrant creator ecosystem.

---

[54] (2025, Sept 10). First court appearance for three 'finfluencers' charged in FCA-led global crackdown on illegal promotions. *Financial Conduct Authority.* <*https://www.fca.org.uk/news/press-releases/first-court-appearance-three-finfluencers-charged-fca-led-global-crackdown-illegal-promotions*>

[55] (2025, Sept 19), India's 3.5-4.5 Million Creator Economy Powers ₹3,500 Crore Influencer Marketing Industry Growth: Kofluence Influencer Marketing Report, 2025. *Business Standard.* <https://www.business-standard.com/content/press-releases-ani/india-s-3-5-4-5-million-creator-economy-powers-3-500-crore-influencer-marketing-industry-growth-kofluence-influencer-marketing-report-2025-125070800524_1.html>

IV. Conclusion

Taken together, the recent parliamentary recommendations, executive advisories, and judicial interventions illustrate how India's framework for platform governance and online safety is in flux. This layered evolution signals that the boundaries between content regulation, platform accountability, and public order are increasingly porous, with multiple institutions exercising overlapping authority.

As India moves forward, the challenge will be to balance innovation and free expression with robust safeguards against digital harms. Coherence, transparency, and due process must be at the centre of any new regime. Without them, fragmented rules and ad hoc enforcement risk creating uncertainty for platforms, overreach in state action, and chilling effects on legitimate expression. A harmonised approach, anchored in statutory clarity, institutional coordination, and proportionate accountability, will be critical to ensure that online spaces remain open, safe, and resilient in the face of evolving technological and societal risks.

thedialogue.co

@_DialogueIndia

@TheDialogue_Official

@The-Dialogue-India

@TheDialogue