IN THE HIGH COURT OF GUJARAT AT AHMEDABAD

R/WRIT PETITION (PIL) (WRIT PETITION (PIL)) NO. 9 of 2026

==========

VIKAS VIJAY NAIR
Versus
STATE OF GUJARAT & ORS.

==========

Appearance:
MR AMIT M PANCHAL(528) for the Applicant(s) No. 1
MR KAMAL TRIVEDI, ADVOCATE GENERAL with MR. G.H. VIRK, GOVERNMENT PLEADER and MR VINAY VISHEN, AGP for the Opponent(s) No. 1,2
MR ANKIT SHAH(6371) for the Opponent(s) No. 3,4

==========

CORAM: **HONOURABLE THE CHIEF JUSTICE MRS. JUSTICE SUNITA AGARWAL**
and
HONOURABLE MR.JUSTICE D.N.RAY

Date : 10/04/2026

ORAL ORDER
(PER : HONOURABLE THE CHIEF JUSTICE MRS. JUSTICE SUNITA AGARWAL)

1. A photocopy of the Notarised affidavit-in-reply filed on behalf of the respondent no.4 Union of India, Ministry of Home Affairs, has been supplied in the Court by Mr.Ankit Shah, learned advocate appearing for the said respondent. The learned advocate is directed to file the original in the Registry within a period of 24 hours.

2. In this public interest litigation, the petitioner has highlighted issues pertaining to widespread creation and circulation of AI generated videos on digital platforms posing serious threat to public order and functioning of a healthy democracy. The petitioner has also raised issues about the

inaction of the State in framing specific laws or regulatory mechanisms against deepfake/synthetic/digitally manipulated media AI generated contents. It is contended therein that the existing legal framework in India, including the Information Technology Act, 2000 and the related provisions under the IPC are inadequate to effectively regulate the creation, dissemination and circulation of fake and AI generated videos on digital platforms. This legislative vacuum underscores the urgent need for intervention of the Court to direct the appropriate Government to formulate a comprehensive and robust regulatory mechanism to curb the misuse of artificial intelligence in generating and circulating fake videos and photographs.

3. The contention in the writ petition is that there is an immediate requirement to curb the creation and use of such AI deepfakes which immediately penetrate the social fabric and create an impact which leads to irreversible situations. There is a need to frame laws regulating the fast paced advancement technology. The interim relief sought in the writ petition is to issue direction to restrain the respondents no. 5 to 9 who are intermediaries running various online social media portals and websites wherein content creation and distribution is being done.

4. On the presentation of the writ petition, by order dated 24.02.2026, we have sought response of respondents no.1 to 4, i.e. the State Government as well as Union of India, impleaded through the Ministry of Home Affairs and the Ministry of Electronics and Information Technology on the requirement of prescribing a regulatory framework.

5. In the affidavit filed on behalf of the respondent no.1, the State of Gujarat, it is submitted that the relevant regulatory architecture under the Information Technology Act, 2000 (in short as the "IT Act' 2000") primarily operates through three important statutory provisions, viz.; Section 69, which deals with interception, monitoring and decryption of information through computer resources; Section 69A, which deals with blocking of access for the public to any information hosted in any computer resources; Section 79, which deals with exemption from liability of intermediaries in certain cases.

6. Section 79 is noted hereinunder :-

> **"79. Exemption from liability of intermediary in certain cases.–**(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
>
> (2) The provisions of sub-section (1) shall apply if–
>
> (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
>
> (b) the intermediary does not–
>
> (i) initiate the transmission,
> (ii) select the receiver of the transmission, and
> (iii) select or modify the information contained in the transmission;
>
> (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central

> Government may prescribe in this behalf.
>
> (3) The provisions of sub-section (1) shall not apply if–
>
> (a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
>
> (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.
>
> Explanation.–For the purposes of this section, the expression —third party information‖ means any information dealt with by an intermediary in his capacity as an intermediary."

7. It is submitted by Mr. Kamal B. Trivedi, learned Advocate General appearing for the State that Section 79(3)(b) clearly indicates that an intermediary cannot claim exemption or immunity from its liability to expeditiously remove or disable the access to the material, any information, data or communication connected to a computer resource which is being used to commit the unlawful act. Upon receiving actual knowledge or on being notified by the appropriate Government or its agency, it becomes the liability of the intermediaries to remove or disable access to such incriminating material.

8. It is submitted that Section 69A of the IT Act' 2000 empowers the Central Government or an officer specially

authorized by it to direct any intermediary to block for public access any information generated, transmitted, received, stored or hosted in any computer resource, which is not in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States, public order or for preventing incitement to the commission of any cognizable offence relating to the above, for the reasons to be recorded in writing by an order.

9. Sub-section (2) of Section 69 read with Section 87(za) provides that the procedure and safeguards for blocking access by the public shall be prescribed under the Rules framed by the Central Government, providing of operational workflow for blocking under Section 69A of the IT Act' 2000. It is stated in the affidavit by the State Government that a blocking request under Section 69A may be initiated by the Ministry, Department of the Government of India, State Government or a law enforcement agency through its designated Nodal Officer. The request must include details of the content, reasons for blocking and relevant legal justification. The request is forwarded to the designated officer appointed by the Central Government (usually within the Ministry of Electronics and Information Technology). The designated officer places the request before the Committee for examination of blocking requests which includes representations from various ministries such as Law, Home Affairs, Information & Broadcasting and CERT-In. The Committee examines whether the request satisfies the legal grounds under Section 69A.

10. Wherever feasible, the originator or intermediary hosting the content is given an opportunity to be heard before a final decision is made. If the Committee finds the content violative of the grounds specified under Section 69A, it recommends blocking the content. The final order is issued with the approval of the Secretary, Ministry of Electronics and Information Technology. The blocking order is communicated to the concerned intermediaries, internet service providers or hosting platforms, directing them to disable access to the specified content or website. For any urgent request, the designated officer may recommend immediate blocking without prior hearing with approval from the Secretary of the Ministry of Electronics and Information Technology. The committee subsequently reviews the decision within 48 hours. The Review Committee constituted under the IT Act framework, periodically reviews blocking orders to ensure that they comply with the legal requirements.

11. It is contended that Section 79 stands on a conceptually different footing from Sections 69 and 69A of the IT' Act, 2000. It is not essentially a sovereign surveillance provision nor a blocking power provision, inasmuch as, it is a liability allocation provision, which grants conditional exemption from liability to intermediaries in respect of third party information hosted or transmitted through their computer resources. Section 79 embodies what is commonly known as the doctrine of safe harbor, under which intermediaries are protected from the liability for user generated content provided they satisfy the statutory conditions laid down in the Act and comply with due diligence obligations prescribed by the Central

Government.

12. Section 79(3)(b) of the IT Act' 2000 read with the Rules mandates that digital intermediaries (social media, ISPs, etc.) lose their "safe harbour" immunity if they fail to expeditiously remove or disable access to unlawful content upon receiving actual knowledge of the Government notification. This provision forces compliance with takedown orders to prevent liability for user generated content.

13. It is further submitted that under the Due diligence obligations contained in the Rules, viz. the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (in short as the "Rules' 2021") framed in exercise of powers conferred by sub-section (1), clauses (z) and (zg) of sub-section (2) of Section 87 amended by the Amendment Rules, 2026 with effect from 20.02.2026, are the obligations of the intermediary in relation to synthetically generated information clearly delineated.

14. It is further stated that the legal meaning of the expression "actual knowledge" under Section 79 has been evolved through subordinate legislation and judicial interpretations and the Apex Court in **Shreya Singhal v. Union of India, (2015) 5 SCC 1**, read down the scope of "actual knowledge" in order to prevent unconstitutional chilling effects on free speech. The Court has clarified that the intermediaries cannot be expected to adjudicate upon the legality of user content merely on the basis of private complaints and that the takedown obligation under Section 79(3)(b) would be triggered only upon;

(i) an order of the Court of competent jurisdiction; or

(ii) a lawful notification or direction by the appropriate Government or its authorized agency, thereby reducing the risk of private censorship and preserving the constitutional freedom.

15. The Apex Court has, thus, preserved the constitutional balance under Article 19(1)(a) subject to the permissible restrictions under Article 19(1)(a) of the Constitution of India.

16. It is, thus, submitted that under the statutory duty of Due diligence under Section 79(3)(b) of the IT Act' 2000, an intermediary is required to remove or disable access to unlawful content upon receiving actual knowledge or lawful notice from the appropriate Government or its authorized agency of such unlawful content which fall foul of protection.

17. It is submitted that the law enforcement agencies are facing several operational challenges in implementation of the notices issued under Section 79(3)(b) of the IT Act' 2000. The lawful notices issued to the intermediaries under the statutory legal framework by the law enforcement agencies in practice, encounter frequent delays, repeated procedural obligations and non-compliance by certain platforms. In certain cases, even after issuing show-cause notices, reiterating the legal provisions and grounds for removal, the intermediaries fail to provide any substantive reply and do not remove the offending content. This results in continued public availability of unlawful material despite lawful notification. One of such show-cause notice issued on 16.02.2026 from the office of the

Director General of Police to one of the intermediaries is extracted in the affidavit itself.

18. It is submitted that there are repeated demands for additional information by intermediaries even after providing the same. Many a times, the response of the intermediaries would be that the URL or link provided in the notice cannot be located despite the fact that the link corresponds to the unlawful content identified by the law enforcement agency. Such response often results into a situation where the content remains accessible through the same link on the platform.

19. Highlighting these issues, some suggestions for framing a policy providing for robust regulatory framework mandating immediate coordination mechanism between the investigating authority and the digital service providers have been made in the affidavit of the State Government and it is submitted that framing of appropriate Rules in exercise of Rule making powers of the Central Government would be the key areas to address the issue. The suggestions are:-

(i) Rules should prescribe dedicated and expedited response timelines for intermediaries. In particular, information sought by intermediaries, internet service providers, and hosting platforms from the concerned Central and State Enforcement Agencies should be made available instantaneously on a 24x7 basis.

(ii) Such rules should further mandate intermediaries, internet service providers, and hosting platforms

to comply with directions issued by the aforesaid Enforcement Agencies for immediate blocking of content. Such blocking should take effect forthwith, without prior hearing, pending approval of the Secretary, Ministry of Electronics and Information Technology (MeitY), and subject to subsequent review and hearing by the Specified Committee within a period of one month.

(iii) The rules should also provide that whereupon review by the Committee, the content in question is found not to contain any objectionable material, the same shall be permitted to be restored or uploaded without delay.

(iv) Provision should be made for real-time coordination and communication between the Enforcement Agencies on the one hand, and intermediaries, internet service providers, and hosting platforms on the other.

(v) The rules should further establish a clear escalation mechanism to be triggered in instances where intermediaries, internet service providers, or hosting platforms delay or fail to take the required action within the prescribed timelines.

(vi) The rules should mandate robust takedown protocols, particularly in respect of deepfake content. Such protocols should apply irrespective

of whether the content carries a disclaimer such as "AI Generated" or "Fake Information", or whether any such disclosure is absent.

(vii) The rules should expressly provide that reliance on internal policies or community standards of intermediaries, internet service providers, or hosting platforms shall not constitute a valid ground for refusing or delaying compliance with directions issued by the Enforcement Agencies, particularly where the content in question is in violation of Indian law.

20. It is submitted that the legal and regulatory framework governing online platforms must continue to evolve in order to effectively address the emerging risks associated with artificial intelligence technologies, deepfake contents and large scale digital misinformation. Such evolution must be guided by the principles of constitutional governance, ensuring that regulatory responses remain proportionate, lawful and consistent with the fundamental rights guaranteed under the Constitution. The State Government remains fully committed to ensuring the effective enforcement of digital laws and protection of citizens from unlawful online activities. The objective of the regulatory framework is not to restrict legitimate expression, but to ensure that the digital platforms are not misused for creation and dissemination of unlawful content capable of destabilizing public order or undermining democratic institutions.

21. In the affidavit filed on behalf of the respondent no.4, Union of India, Ministry of Home Affairs, it is submitted that policy and regulatory matters concerning intermediaries, digital platforms and online content regulation primarily fall within the domain of Ministry of Electronics and Information Technology, in terms of The Government of India (Allocation of Business) Rules, 1961, under the IT Act' 2000 and the Rules framed thereunder. The Ministry of Home Affairs, on the other hand, is primarily concerned with the matters pertaining to cybercrime, including, inter alia, coordination of law enforcement agencies, capacity building, and facilitation of, and provision of assistance to law enforcement agencies in the detection, prevention, investigation, and prosecution of cybercrimes across the State and Union Territories.

22. It is submitted that the legal, technological support system, institutional frameworks and enforcement mechanisms established by the Government of India to effectively address misuse of artificial intelligence technologies such as synthetically generated contents and deepfakes, are the measures designed to support and augment the enforcement agencies, at both, Central and State/Union Territory levels. These frameworks include measures in overcoming operational, technical, and coordination related challenges encountered in the detection, prevention, investigation and prosecution of such offences.

23. The provisions in IT Act' 2000 provide the legal framework to address the offences arising from misuse of computer resources involving misuse of synthetic or

manipulated digital content including deepfakes. The amendments introduced by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (notified on 10.02.2026 and effective from 20.02.2026) have been structured in two categories, viz. (i) Due diligence obligations applicable to all intermediaries, including SMIs, under Rule 3 of the Amended IT Rules, 2021 and (ii) Enhanced accountability and due diligence obligations specific to Significant Social Media Intermediaries (SSMIs) under Rule 4 of the Amended IT Rules, 2021.

24. Reference has been made to Rule 3(3)(a) inserted by the Amendment Rules of 2026 to submit that under the said Rules, intermediaries covered by Rule 3(3) are mandated to deploy reasonable and appropriate technical measures including automated tools or other suitable mechanisms to ensure that users are not permitted to create, generate, modify, alter, publish, transmit, share or disseminate synthetically generated information which violates any law for the time being in force. The said provision specifically requires intermediaries to prevent the dissemination of high risk categories of unlawful synthetically generated information, included inter alia in clauses (i) to (iv) of clause (a) of sub-rule (3) of Rule 3 of the amended Rules.

25. It is submitted in the affidavit filed on behalf of the Union of India, Ministry of Home Affairs that SAHYOG portal – a centralized unified platform has been created by the Ministry of Information Technology and Department of Telecommunications (DOT) for routing intimations under

Section 79(3)(b) of the IT Act' 2000 read with Rule 3(1)(d) of the IT Rules' 2021. The portal has been operational since October 2024, facilitating immediate, coordinated and time bound action by bringing all authorized law enforcement agencies and intermediaries on a single platform, enabling swift takedown of unlawful synthetically generated information and access to subscriber information, logs and judicial evidence for identification of offending users.

26. It is further submitted that as on date, 524 IT intermediaries have been onboarded on the SAHYOG portal, which includes respondents no.5 and 6 herein as well . It is submitted that the SAHYOG portal has attained substantial milestones in lawful data requests facilitating more than 16,000 police stations from all States/Union territories to raise lawful data requests. The portal is being used for child sexual exploitation and abuse material reporting and broadcasting of Hashes to all intermediaries, thereby providing a comprehensive mechanism for both content takedown, investigative support and preventing recurrence under the existing legal framework.

27. It is submitted that vide Gazette notification dated 1303.2024, the Central Government in exercise of powers conferred by clause (b) of sub-section (3) of Section 79 of the IT Act' 2000 has formally designated the Indian Cyber Crime Coordination Centre, Ministry of Home Affairs, as the authorized agency of the Central Government to perform the functions under the said provision. The said notification specifically empowers the Indian Cyber Crime Coordination

Centre to notify intermediaries regarding instances of information, data or communication links residing in or connected to a computer resource controlled by the intermediary, which is being used to commit any unlawful act.

28. It is further submitted that while certain intermediaries such as respondents no.5 and 6 have undertaken API based integration, resulting in significant improvement in speed, efficiency and traceability of compliance actions, others including respondent no.7 herein have not yet onboarded or fully integrated with the portal and often fail to respond to the statutory notices issued under Section 79(3)(b) of the IT Act' 2000. There is a categorical assertion with regard to non-responsiveness of respondent no.7 intermediary herein to the intimations given to it containing unlawful contents including synthetically generated information. The assertion is that during the period, a total of 94 intimations were given to the respondent no.7 intermediary comprising 60 intimations in 2024 (relating to 1029 URLs), 33 intimations in 2025 (relating to 121 URLs) and 1 intimation in 2026 (relating to 10 URLs) aggregating 1160 URLs containing unlawful contents, including synthetically generated information.

29. It is submitted that as against the aforesaid intimations, a formal response has been received by the authorities only against 13 intimations (12 pertaining to 2024 and merely 1 pertaining to 2025). Although partial action has been reported by respondent no.7 intermediary in disabling 788 notified URLs in 2024, 70 in 2025 and 6 in 2026, but the alarming low rate of formal responses, results in lack of

meaningful cooperation with the lawfully issued directions. Such conduct not only amounts to breach of enhanced Due diligence obligations cast upon the intermediaries under the amended IT Rules of 2026, but also severely impedes the ability of law enforcement agencies to ensure timely removal or disabling access to unlawful content and to carry out effective investigations.

30. It is submitted that wider adoption and full integration of the SAHYOG portal by all intermediaries is essential to ensure uniform, time-bound compliance with the three hour takedown requirement under the amended IT Rules, 2026.

31. The reference has been made to para '254' of the decision of the Apex Court in **Just Rights for Children Alliance v. S. Harish [2024 SCC OnLine SC 2611]** to submit that the Apex Court has reiterated the role of intermediaries in expeditiously removing or disabling access by them upon receiving "actual knowledge" or on being notified by the appropriate Government or its agency in case any information, data or communication link residing in or connected to a computer resource controlled by the intermediary being used to commit an unlawful act.

32. It is submitted that the portal significantly enhances the ability of law enforcement agencies to report promptly to rapidly spreading unlawful content, including deepfake material, thereby addressing the very concern highlighted in the present petition regarding the need for coordinated response mechanisms.

33. The submission is that SAHYOG portal has received judicial recognition and affirmation in the order of the High Court of Karnataka in the case of **X Corp. vs. Union of India and Ors, in Writ petition No. 7405 of 2025**. In addition to the legal framework, the Government of India has operationalized robust technological and institutional mechanisms including the SAHYOG portal enabling real time coordination between law enforcement agency and intermediaries for content takedown, data disclosure, investigation support and bi-directional sharing, thereby addressing the very concern relating to coordination and response timelines raised in the present petition.

34. However, the primary challenge lies not to the absence of law or institutional mechanisms, but to the inconsistent, partial, or inadequate compliances by certain intermediaries, particularly in relation to :-

i. adherence to time-bound takedown obligations (including the 3-hour rule);

ii. implementation of prominent labelling, metadata, and verification requirements for SGI;

iii. deployment of proactive detection and prevention mechanisms;

iv. identification and removal of identical or previously flagged unlawful content; and

v. timely and complete sharing of data with law

enforcement agencies for investigation purposes.

vi. Action by intermediaries against users who are repeatedly sharing unlawful contents and ensuring that the users are verified users and prevention of creating user accounts using anonymous identifiers and technology.

35. It is submitted that the scale and speed of dissemination of unlawful content, particularly through AI generated deepfakes, automated bot networks and encrypted or semi-anonymous platforms has introduced significant risks to public order, individual rights, financial security, and national security. These risks are further compounded where intermediaries do not fully cooperate with statutory mechanisms or delay compliance with lawful directions.

36. The submission of the learned counsel appearing for the Union of India, Ministry of Home Affairs is that the present matter requires strengthening of compliance, accountability and uniform implementation of the existing statutory and regulatory regime by intermediaries coupled with effective utilization of established platforms such as SAHYOG.

37. Taking note of these contentions made in the affidavits of the State Government and the Union of India, Ministry of Home Affairs, it seems that the issues which need consideration by us essentially is about the strict enforcement and uniform implementation of the existing statutory regime in the larger public interest, as is submitted on behalf of Union of India through Ministry of Home Affairs as well as the

State respondents, where concerns have been shown with regard to the implementation of the statutory provisions at the ends of the intermediaries.

38. Taking note of the above, we deem it fit and proper to issue notice to the intermediaries, impleaded herein as respondents no.5 to 9, returnable on 08.05.2026. The petitioner shall take steps for service of notice upon the said respondents within a period of one week from today.

39. We direct that the said respondents are required to answer to not only the stand of the petitioner, but also that of the State and the Central Government in the matter of practical implementation of the legislative framework and the institutional mechanisms developed for greater alignment of all intermediaries to ensure strict compliance of Due diligence obligations under the Amended Rules of 2026. The response by the respondents no.5 to 9 shall be filed by the next date fixed.

40. In the meantime, it is directed that the respondents no. 5 to 9 intermediaries shall ensure to bring them onboard on the SAHYOG portal developed by the Indian Cyber Crime Coordination Centre, Ministry of Home Affairs for better coordination and time bound action by bringing all authorized law enforcement agencies and intermediaries on a single platform. And to ensure swift action/response to the statutory notices issued under Section 79(3)(b) of the IT Act' 2000 ensuring adherence to time bound takedown obligations in strict compliance of the provisions of the Rules' 2021 as amended by the Amendment Rules of 2026 with effect from

20.02.2026. Effective and meaningful responses/action of the respondents intermediary will be key to the due diligence obligations enforced upon them under the statutory framework.

41. We also direct Mr. Ankit Shah to also file a response of the respondent no.3, the Secretary, Ministry of Electronics and Information Technology, Union of India to the issues raised in the writ petition, by the next date fixed.

42. The matter be listed on 08.05.2026.

(SUNITA AGARWAL, CJ)

(D.N.RAY,J)

BIJOY B. PILLAI