2026 INSC 1149

REPORTABLE

IN THE SUPREME COURT OF INDIA

CRIMINAL APPELLATE JURISDICTION

M.A. NOS. 2553-2554 OF 2026

In

Criminal Appeal Nos. 2161-2162 of 2024

IN THE MATTER OF:

JUST RIGHTS FOR CHILDREN ALLIANCE & ANR. …APPLICANTS

VERSUS

S. HARISH & ORS. …RESPONDENTS

O R D E R

Signature Not Verified

Digitally signed by VISHAL ANAND
Date: 2026.10.17 10:17:00 IST
Reason:

INDEX

I. BACKGROUND 3

II. FRAMEWORK FOR THE DETECTION AND REMOVAL OF CSEAM 8

A. Advanced Mechanisms for the Detection & Removal of CSEAM 8

i. Some Problems in the Existing Mechanism. 8

ii. Matching and Listing of Hash & URL of CSEAM. 9

iii. The Position in India. 14

B. Comprehensive National Database for the Detection and Removal of CSEAM 21

i. Need for a National Database for Hash & URL Lists of CSEAM. 21

ii. Indian Cyber Crime Coordination Centre's Sahyog Portal. ... 23

iii. Safeguards and Standard Operating Procedure for the Maintenance and Use of Hash & URL List Database. 25

a. Procedural Difference viz-a-viz CSEAM of 'Unknown Origin' and 'Known Origin' 27

b. Requirement of Proper Notice and Grievance Redressal .. 32

c. Additional Safeguards Required for the use of Hash & URL List Database. 34

C. Mechanisms for the Reporting of CSEAM. 37

i. Some Lacunas in the Existing Mechanism. 42

ii. Streamlining & Standardization of Reporting Mechanism. .. 45

iii. Efficacy of the Grievance Redressal Mechanism relating to CSEAM. 49

a. Misconception on what constitutes "CSEAM" and Misreading of our decision in Just Rights (supra). 50

b. Dedicated Grievance Officers for managing CSEAM and reports related thereto. 63

c. The Proper Authority and Timelines for reporting of CSEAM by Intermediaries. 70

d. Need for a Prescribed Form for the Reporting of CSEAM by the intermediaries. 74

e. Safeguards for the Grievance Redressal Mechanism in respect of CSEAM. 77

D. Penalties for persistent failures by Intermediaries in complying with the requirements of IT Rules. 83

i. Need to rethink and move beyond Section 79 of the IT Act. .83

ii. Exemplary Monetary Fines and Penalties. 87

iii. Scrutiny and Disgorgement of "Profits" from Paywalled Content. 96

E. Article 21 and the Right to Access Internet. 100

F. Awareness on Digital Safety, Sex Education and Measures to support Wellbeing of Children. 108

III. SUMMARY OF OUR CONCLUSION 122

I. BACKGROUND

1. We heard the learned counsel appearing for the applicants and Mr. Tushar Mehta, the learned Solicitor General appearing for the Union of India.

2. In our previous order dated 14.08.2026, we had expressed concerns over certain serious lapses on the part of various social media intermediaries and platforms, particularly in complying with the directions that were issued in our judgment dated 23.09.2024 in **Just Rights for Children Alliance & Anr. v. S. Harish & Ors.** reported in **2024 INSC 716**.

3. In **Just Rights** (supra) we had taken note of an alarming increase in child sexual exploitation and abuse material ("**CSEAM**") that were being circulated on social media platforms.

4. At that time, we had flagged how indirect links to such harmful material were being promoted and shared through social media algorithms to bypass the rigours of the special penal provisions

designed for the protection of children within the cyberspace, namely Section(s) 15 and 67B of the POCSO Act[1] and the IT Act[2], respectively.

5. In our judgment, more particularly at paragraph 109, we had this to say: -

> *"109. During the course of hearing, our attention was also drawn to a recent news article that reported how on social media, links to view child pornography were being circulated and sold for anywhere between Rs. 40 to Rs. 5,000. The news report indicates, how social media platforms are rife with child sexual abuse, and gave certain insight about the modus operandi of the distribution of such material on these platforms. It explained how the sellers and distributors of child pornographic material rather than sharing any downloads to such material, would ingeniously only share links to such material instead in lieu of money, so as to circumvent the penal provisions of the POCSO and IT Act, which criminalized only the storage of such material. By indefinitely forwarding links, they completely bypass the requirement of first storing such material onto any device, and similarly those who view such material also only use the links, without ever downloading such material onto their device."*
>
> (Emphasis supplied)

6. We had further taken note of the disquieting failure on part of the social media platforms in reporting such harmful activities to the Special Juvenile Police Unit, as required by the law.

[1] The Protection of Children from Sexual Offences Act, 2012 (for short, the "**POCSO Act**").
[2] The Information Technology Act, 2000 (for short, the "**IT Act**").

7. In this regard we had this to say: -

> *"256. It has been brought to the notice of this Court that social media intermediaries do not report such cases of child abuse and exploitation to the local authorities specified under POCSO and rather only comply with the requirements stipulated in the MOU. In view of the salutary object and the mandatory character of the provisions of Sections 19 and 20 of the POCSO read with Rule 11 of the POCSO Rules, we are of the considered view, that an intermediary cannot claim exemption from the liability under Section 79 of the IT Act for any third-party information, data, or communication link made available or hosted by it, unless due diligence is conducted by it and compliance is made of these provisions of the POCSO. We are also of the view that such due diligence includes not only removal of child pornographic content but also making an immediate report of such content to the concerned police units in the manner specified under the POCSO Act and the Rules thereunder.*
>
> *xxx xxx xxx*
>
> *258. In view of the overriding effect of the POCSO Act and the rules thereunder, merely because an intermediary is in compliance of the requirements specified under Section 79 of the IT Act, will not absolve it of any liability under the POCSO, unless it duly complies with the requirements and procedure set out under it, particularly Section 20 of POCSO Act and Rule 11 of the POCSO Rules. It is a settled position of law, that when a statute describes or requires a thing to be done in a particular manner; it should be done in that manner or not at all. Thus, social media intermediaries in addition to reporting the commission or the likely apprehension of commission of any offence under POCSO to the National Centre for Missing & Exploited Children (NCMEC) is also obligated to report the same to authorities specified under Section 19 of POCSO i.e., the Special Juvenile Police Unit (SJPU) or the local police."*
>
> (Emphasis supplied)

8. We had clarified in no uncertain terms that such failures would strip the social media platforms of the "Safe Harbour" protection provided by Section 79 of the IT Act.

9. We had hoped that the above *inter-alia* directions would bring a quietus to the disturbing widespread circulation of CSEAM on the internet.

10. We had hoped that we would not have to, once again, be confronted with the same sad state of affairs.

11. Despite more than two years having gone by since our judgment, it appears that there has been no progress worth the name. If anything, the recent news reports instead reveal an even more unsettling reality when it comes to the safety and wellbeing of our children.

12. We are deeply saddened to note that the news reports placed before us by the applicants flagging alleged incidents of paid promotions of CSEAM on social media platforms through redirect links and websites is only one rare instance of such harmful activities being discovered and brought to light.

13. There are millions of more such incidents freely available on social media platforms that may never come to the knowledge of the proper authorities, if no collective action is taken today by all stakeholders.

14. There comes a time when we must ask ourselves, how many more victims of such harmful content must continue to suffer, before our conscience is stirred into making collective effort in the right direction.

15. We are afraid that we cannot afford to wait any longer for an answer. Due to the lack of any earnest initiative shown on the part of either the regulatory authorities or the social media intermediaries for all these years, we are left with no choice but to take matters in our own hands.

16. We cannot emphasize this enough, that there can be no space for non-consensual sexually exploitative and abusive material on the internet, particularly on platforms that are readily accessible to the most impressionable and vulnerable of our society.

17. Thus, with the assistance from the Union of India through the Ministry of Electronics and Information Technology and the Ministry of Law and Justice, respectively, we propose to take the strictest of actions by

putting in place a workable framework for a safer future of our children.

18. In this regard, there are certain aspects which we must point out that merit a considered response, and we would like to hear the Union of India on the same.

II. FRAMEWORK FOR THE DETECTION AND REMOVAL OF CSEAM.

A. Advanced Mechanisms for the Detection and Removal of CSEAM

i. Some Problems in the Existing Mechanism.

19. As far as we understand, the current mechanism for the detection and removal of CSEAM relies heavily on individual instances of content being reported and subsequently removed. These reports originate either at the behest of the authorities or the users themselves.

20. Although, various social media intermediaries have deployed their own safeguards for a seamless continued detection and removal of such content, yet what is missing is any form of synergy insofar as detection and removal is concerned, across the internet.

21. When one social media platform detects and removes CSEAM, that detection does not automatically result in the same content being flagged and removed from all other social media platforms.

22. It is only when such content is also found by the other platforms, through their own mechanisms and safeguards that, the same comes to be removed.

23. This isolated mechanism of detection delays the removal of CSEAM across different platforms, delays which enable the continued circulation of such content to the various corners of the internet.

24. Even if some social media platforms are coordinating their efforts for the simultaneous removal of CSEAM once so detected by either of one of them, such arrangements are only informal, dependent entirely on which platforms choose to undertake such initiative and for how long.

ii. Matching and Listing of Hash & URL of CSEAM.

25. From what we have been able to understand, the practice that is globally in vogue for the seamless detection and removal of CSEAM is a process termed as "Hash and URL Data Matching & Listing".

26. The process works on a simple principle. Every component of a CSEAM content, be it the video frame or image or multiples of both, carries a unique digital data print identifier in alphanumeric form, which is known as the "Hash" identifier of that material. The hash identifier of any particular content remains unique to it, irrespective of where it is uploaded or by whom.

27. When any content is identified as CSEAM, specialised software is used to extract and generate the hash identifier and the same is added to a consolidated database known as a "Hash List".

28. This Hash List can then be used to crosscheck all other content, whether on the very same platform or on another. Where a match is found against a particular hash identifier, the algorithm automatically flags and removes that content without the need to rely on the conventional means of detection.

29. However, the above mechanism is not without limitations. Expert insights indicate that a new *modus operandi* has emerged for circumventing the hash list detection process. This is usually done by manipulating the video frame or imagery of the content, or a

combination of both, either by way of resizing it or reformatting it, so as to avoid detection.

30. It is for this reason that "Perceptual Hashing", an improved process of recent vintage assumes significance. Shorn of the details, this process, from what we understand, combines the original technique of extracting the hash identifier with an additional step of generating the audio-visual characteristics of the content. Characteristics such as colour-coding, object composition, audio cues, etc., are also used to generate the hash identifier for a content detected as CSEAM, which remains unique *dehors* any manipulation.

31. One another technological measure of similar significance that has caught our attention is URL Listing, which targets indirect links to CSEAM and other harmful content that are merely shared or exchanged on social media platforms without uploading or storing the same on the platform.

32. The news report that has been placed before us by the applicant herein reveals the prevalence of this very practice. It highlighted the circulation and promotion of CSEAM through links which would then

redirect users to other websites and platforms where such materials were offered for monetary considerations.

33. "URL Listing" thus, assumes significance. Unlike Hash Listing that generates a unique identifier for the CSEAM content, URL Listing proceeds by generating an identifier for the external location where the CSEAM content is hosted. It extracts all possible unique web-addresses where the CSEAM has been confirmed to have been uploaded, and then uses that data to block any future attempts to access it.

34. Various jurisdictions across the world have, in some form or manner, called for the deployment of one, or a combination of the aforesaid measures, with a view to ensure the effective detection and removal of CSEAM.

Country	Measures	Provision
United States	Hash Matching	**18 U.S.C. § 2258C(a)(2)** *"The elements authorized under paragraph (1) may include hash values or other unique identifiers associated with a specific visual depiction, including an Internet location and any other elements provided in a CyberTipline report that can be used to identify, prevent, curtail, or stop the transmission of child pornography and prevent the online sexual exploitation of children."*
	URL Listing	

United Kingdom	Hash Matching	**Ofcom, Illegal Content Codes of Practice for User-to-User Services, Recommendation ICU C9** *"ICU C9.3 The provider should ensure that, where technically feasible, perceptual hash matching technology is used effectively to analyse relevant content to assess whether it is CSAM.* *ICU C9.4 The provider should ensure that appropriate measures are taken to swiftly take down (or prevent from being generated, uploaded or shared) detected content that is CSAM [...]"*
	URL Listing	
South Korea	Hash Matching	**Enforcement Decree of the Telecommunications Business Act, Article 30-6(2)** *"2. Measures to restrict the transmission of search results, such as deleting search results by identifying whether the information the user is searching for corresponds to illegal footage, etc. that has previously been requested for reporting or deletion pursuant to Article 22-5(1) of the Act, by comparing the search term entered by the user with the title, name, etc. of the illegal footage;* *3. Measures to restrict the posting of the information after analyzing the characteristics of the information that the user wishes to post, comparing and identifying whether it corresponds to information that has been reviewed and decided by the [Korea Communications Standards Commission] as illegally filmed material, etc. In this case, comparison and identification must be made using any of the following technologies:* *(a) Technology developed and provided by national organizations;* *(b) Technology that has passed a performance evaluation conducted within the last two years by an institution or organization determined and notified by the Korea Communications Commission"*
	URL Listing	
Australia	Hash Matching	**Online Safety (Relevant Electronic Services—Class 1A and Class 1B Material) Industry Standard 2024** *"19 Detecting and removing known child sexual abuse material* *(1) This section applies to the following:* *(a) a pre-assessed relevant electronic service;* *(b) a Tier 1 relevant electronic service.* *(2) The provider of a service must implement appropriate systems, appropriate processes and appropriate technologies to:* *(a) detect and identify known child sexual abuse material that:*

		(i) is stored on the service; or *(ii) is accessible by an end-user in Australia using the service; or* *(iii) is being or has been accessed or distributed in Australia using the service; and* *(b) remove known child sexual abuse material from the service as soon as practicable after the provider becomes aware of it.* *Note 1: <u>The technologies that the provider may use include hashing technologies and machine learning</u>."*

iii. The Position in India.

35. From what we can discern, no such provision exists in India, requiring social media intermediaries to employ tools for Hash or URL Listing, at least to the same extent as found in other jurisdictions.

36. The closest analogue to any such statutory requirement in India can be found in some parts of Rule(s) 3 and 4 of the IT Rules[3]. The same reads as under: -

> *"**3. (1) Due diligence by an intermediary:***
> *(b) the intermediary shall inform its rules and regulations, privacy policy and user agreement to the user in English or any language specified in the Eighth Schedule to the Constitution in the language of his choice <u>and shall make reasonable efforts by itself, and to cause the users of its computer resource to not host, display, upload, modify, publish, transmit, store, update or share any information that</u>, –*
> *(i) is obscene, pornographic, paedophilic, invasive of another's privacy including bodily privacy, insulting*

[3] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (for short, the "**IT Rules**")

or harassing on the basis of gender, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or an online game that causes user harm,] or promoting enmity between different groups on the grounds of religion or caste with the intent to incite violence;

(ii) is harmful to child;

xxx xxx xxx

3. (3) Due diligence in relation to synthetically generated information:

(a) Where an intermediary offers a computer resource which may enable, permit, or facilitate the creation, generation, modification, alteration, publication, transmission, sharing, or dissemination of information as synthetically generated information, it shall ensure that, –

(i) it deploys reasonable and appropriate technical measures, including automated tools or other suitable mechanisms, to not allow any user to create, generate, modify, alter, publish, transmit, share, or disseminate, as the case may be, any such synthetically generated information that violates any law for the time being in force, including the Act, Bharatiya Nyaya Sanhita, 2023 (45 of 2023), Protection of Children from Sexual Offences Act, 2012 (32 of 2012), Explosive Substances Act, 1908 (6 of 1908), and includes any such synthetically generated information that, –

(I) contains child sexual exploitative and abuse material, non-consensual intimate imagery content, or is obscene, pornographic, paedophilic, invasive of another person's privacy, including bodily privacy, vulgar, indecent or sexually explicit; or

4. Additional due diligence to be observed by significant social media intermediary and online gaming intermediary.

(4) A significant social media intermediary shall deploy appropriate technical measures, including automated tools or

other suitable mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary under clause (d) of sub-rule (1) of rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule:

Provided that the measures taken by the intermediary under this sub-rule shall be proportionate having regard to the interests of free speech and expression, privacy of users on the computer resource of such intermediary, including interests protected through the appropriate use of technical measures:

Provided further that such intermediary shall implement mechanisms for appropriate human oversight of measures deployed under this sub-rule, including a periodic review of any automated tools deployed by such intermediary:

Provided also that the review of automated tools under this sub-rule shall evaluate the automated tools having regard to the accuracy and fairness of such tools, the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools."

(Emphasis supplied)

37. These rules which came to be inserted by the Information Technology Amendment Rules, 2026, although a step in the right direction, yet, fall short as they do not speak of the specific tools and measures a social media intermediary must adopt.

38. Rule 3(1) sub-clause (b), *inter-alia,* requires that intermediaries make reasonable efforts to ensure that their users do not host, upload or disseminate any CSEAM and other non-consensual sexually exploitative and abuse material, including those generated artificially, and to further remove such material under sub-clause (c).

39. Whereas Rule 4(4), *inter-alia,* requires a "*significant social media intermediary"* to also deploy "*appropriate technical measures*" for the detection and removal of CSEAM, including materials which are identical in content to any material that was previously flagged and deleted "*on the computer resource of such intermediary*".

40. We would be remiss not to point out that the expression "*on the computer resource of such intermediary*" used in Rule 4 sub-rule (4) admits of certain ambiguities which need to be addressed.

41. In our considered view, the said expression narrowly confines the extent to which the technical measures must be deployed for the detection and removal of CSEAM.

42. The emphasis placed by Rule 4(4) on only that CSEAM content, which has been either detected or previously removed from the

intermediary's own computer resource, leaves unresolved two possible scenarios. *First,* the possibility of simultaneous flagging and removal of CSEAM content that was already removed on some other platform. *Secondly,* CSEAM content that is hosted on an external source and merely circulated on a particular platform *via* indirect links.

43. To state plainly, under this rule, even if a particular CSEAM was previously detected and removed by one intermediary, there is no corresponding obligation cast upon other intermediaries to automatically look for and remove the same, at least not until, such material happens to also be detected by them in due course of time.

44. This, in our view, confines the entire obligation of detection and removal of CSEAM exclusively to material that has been uploaded, circulated and detected on one intermediary's own resources.

45. We, *prima facie*, find this to be a matter of some concern, particularly when there are reported instances of CSEAM being indirectly circulated, and a less than ideal rate at which such material is currently being detected and removed. It is needless to reiterate that every

moment of delay in removing such harmful content only serves to add to the certain likelihood of further circulation to other platforms.

46. Even otherwise, the cumulative effect of the above rules is that social media intermediaries are only required to "*make reasonable efforts*" and "*deploy appropriate technical measures*" for the proactive detection and removal of CSEAM and other non-consensual sexually exploitative and abusive material from their platforms.

47. We are conscious of the fact that, at the current pace of advancement in technology, it is impractical to statutorily prescribe any particular set of tools and measures for a thriving, safe, and secure cyberspace. That being said, we see no reason why widely used tools and measures of proven mettle cannot be stipulated in the form of periodically revisable guidelines to ensure their uniform and proper adoption by one and all.

48. We do not, for a moment, doubt that certain social media intermediaries may already have employed one or more of the aforementioned tools and measures, or even a combination of all of them. However, the efficacy of such tools depends not only on their

deployment by some, but on their proper and uniform adoption by all, and that is precisely what specific guidelines in this regard can ensure.

49. All that we are trying to say is that while a rigid statutory prescription may not be the appropriate course, yet the same does not, however, mean that no guidelines should be put in place.

50. We would, therefore, like to hear from the Union of India on the tools and technological measures that have been put in place by intermediaries for the detection and removal of CSEAM from their platforms, including the use of perceptual hash-matching and URL listing. This is because, in the absence of such information, it would be difficult for us to assess whether the obligation to "*make reasonable efforts*" is, in practice, being discharged in any meaningful manner. We would further like to hear on the feasibility of a industry-wide use and deployment of such tools, if not already in use. Lastly, we would like the Union of India to come up with some comprehensive guidelines on the tools and technological measures that every intermediary would be expected to deploy for the detection and removal of CSEAM.

B. <u>Comprehensive National Database for the Detection and Removal of CSEAM</u>.

i. Need for a National Database for Hash & URL Lists of CSEAM.

51. We must, however, point out that the deployment of these tools cannot be the end of the matter. Unless the hashes and URLs of CSEAM identified by one intermediary are made accessible to all others, the very process of simultaneous flagging and removal of such material across platforms would remain illusory.

52. It is in this context that a national "Hash and URL List Database" assumes significance. As the name suggests, it is a common repository or pool of the hash identifiers and URL lists of all material which has been flagged and confirmed to be CSEAM across all platforms. The database is continuously updated in real time, and made accessible to all intermediaries and law enforcement agencies, to enable a seamless process of detection and removal of CSEAM on a rolling basis.

53. The significance of such a database may best be appreciated by contrasting it with the current state of affairs. At present, each intermediary, at best, maintains its own list of known CSEAM, compiled from what it has encountered on its own platform. The

result is a multitude of fragmented lists, each incomplete in itself. The multiplicity in efforts in the detection and removal of CSEAM that we seek to avoid cannot take place without such a database.

54. In other words, intermediaries would be in a position to crosscheck the content on their own platforms against the entire database, and not merely against what they themselves have encountered in the past. It is of note that such a database would not contain the harmful material itself, but only the hash identifiers and URLs by which it may be recognised.

55. There are outstanding examples of such databases that have played a pivotal role in reducing the circulation of CSEAM. Various jurisdictions have entrusted the maintenance of such databases to designated bodies and organisations that verify each entry before its inclusion and ensure that the database remains current.

Country	Database	Maintaining Authority
United States	NCMEC Industry Hash Sharing Platform	National Center for Missing & Exploited Children.
	NCMEC NGO Hash Sharing Platform	
United Kingdom	IWF Image Hash List	Internet Watch Foundation and Home Office, Government of United Kingdom.
	Child Abuse Image Database	
Canada	Project Arachnid	Canadian Centre for Child Protection.

Korea	Illegally Filmed Material Database	Korea Communication Standards Commission
Netherlands	Instant Image Identifier and Hash Check Service	Centre for Expertise on Online Sexual Child Abuse (EOKM) and the Dutch National Police.
Italy	CNCPO "black list"	National Center for the Prevention of Child Pornography on the Internet.
New Zealand	Digital Child Exploitation Filtering System	Department of Internal Affairs.

ii. Indian Cyber Crime Coordination Centre's Sahyog Portal.

56. In this regard, we are given to understand that some progress has taken place in the right direction. The Union of India has already developed and put in place a dedicated platform known as the "Sahyog Portal" to *inter-alia* streamline and automate the process of reporting and removal of unlawful content including CSEAM.

57. The Indian Cyber Crime Coordination Centre (I4C), the authority designated to manage and maintain the portal, has been onboarding social media intermediaries onto the same, with a view to coordinate the reporting and removal of CSEAM with the police machinery.

58. We acknowledge that the Sahyog Portal is, no doubt, a step in the right direction. It is also not lost on us that the portal, by virtue of having

already onboarded a considerable number of intermediaries, may well be the natural foundation upon which a Hash & URL List Database could be built.

59. That being said, we are mindful of the fact that, the portal, in its current form, functions only as a common platform to route individual reports and takedown notices.

60. Our expectations from the portal, however, are much more than what it is, as of now, capable of doing, and we are hopeful that the Union of India shares the same vision.

61. We say so because there is a discernible difference between a common portal that routes individual reports and takedown notices, and one which pools together the hash identifiers and URLs of all material confirmed to be CSEAM. The former acts only upon each instance of CSEAM as and when it is reported. Whereas the latter ensures that such material, once identified, is continuously detected and removed across all platforms, without waiting for it to be reported afresh.

62. We would, therefore, like to know from the Union of India whether it is contemplating the creation of a Hash & URL List Database either

within the fold of the Sahyog Portal, or as a standalone repository. If the Sahyog Portal is indeed contemplated to serve such a role, we would like to be apprised of the extent to which, it in its existing form is equipped to do so, and the time by which it can begin to fully function in that role.

iii. Safeguards and Standard Operating Procedure for the Maintenance and Use of Hash & URL List Database.

63. The creation of a Hash & URL List Database of the kind indicated above naturally gives rise to certain attendant concerns, particularly the operation and procedural integrity of the same.

64. If the experiences of existing databases in other jurisdictions is any lodestar, the process by which a particular material comes to be entered into the database as CSEAM, and thereby earmarked for detection and removal, is perhaps the most sensitive of all.

65. From what we have been able to understand, the process by which a hash identifier or URL finds its way into any such database generally unfolds in three distinct stages: -

(i) The *first* step of the process begins with the source of the material. The material which is ultimately entered into the database may come from a variety of sources. It may be reported by a member of the public, flagged by an intermediary on its own platform, forwarded by a law enforcement agency, or discovered by the body maintaining the database in the course of its own proactive search. It is of note, however, that the source of the material, by itself, is of little consequence, except in cases of hash matching, which we shall discuss in the later parts. Irrespective of where it originates, no material is to be mechanically entered into the database merely because it has been reported or flagged as CSEAM.

(ii) The *second,* and perhaps the most crucial stage, is that of assessment, through multiple tiers of verification. This begins with a preliminary screening of the material by specialised software, which makes an initial determination, based on certain characteristics of the material, as to whether it is likely to be CSEAM. The software, however, does not have the final word. At the second tier, the material so flagged is assessed by at least three trained human analysts, who would independently

determine whether the same constitutes CSEAM. This combination of software and human verification minimises erroneous inclusions and ensures that the database remains reliable to act upon.

(iii) It is only upon such material being confirmed to be CSEAM that the *third* stage commences, wherein the hash identifier and/or the URL of the material is generated and entered into the database. This entry is then made available to all intermediaries and law enforcement agencies to cross-check against and remove any content matching the same.

66. The above process is to be carried out on a continuous basis, and the database updated at regular intervals. The entries within the database are to be made through encrypted channels and strictly confined to the hash identifier and/or URL of the material confirmed to be CSEAM. At no point should the CSEAM itself be stored within the database.

a. Procedural Difference viz-a-viz CSEAM of 'Unknown Origin' and 'Known Origin'

67. Since the above exercise for the detection and removal of CSEAM through means of 'Hash Matching' would be over and above the existing ordinary process of detection and removal, namely by way of due diligence and receipt of reports, certain additional aspects emerge that require clarification.

68. While the object of the above two parallel processes remains the same, that being the removal of CSEAM, yet there are certain differences between the two, which must be reflected in the standard operating procedure that would eventually come to be.

69. For this, we propose to draw a distinction between removal of CSEAM of "*Unknown Origin*" and "*Known Origin*".

70. CSEAM of "*Unknown Origin*" would be all such material that has no corresponding match in the Hash & URL List Database but nevertheless was detected and subsequently removed on the basis of the intermediary's own tools and mechanisms. In other words, that harmful material, which was found to be CSEAM on the basis of either reports received or as a result of the intermediary's own due diligence.

71. Conversely, CSEAM of "*Known Origin*" would include all such material that is removed by an intermediary pursuant to a match being found against an already existing entry in the Hash & URL List Database.

72. The distinction is not merely one of nomenclature. It carries with it a significant difference in the procedure that an intermediary would be required to follow, as well as in the obligations that would ensue.

73. Where an intermediary removes CSEAM of "*Unknown Origin*", it would be expected that the said decision was preceded by some verification and due diligence on its part.

74. Upon such removal, the intermediary would be required to generate the hash & URL identifiers of such CSEAM for its own internal use, in order to remove all other instances of the material from its platform, pending its verification and inclusion in the national database.

75. In addition, the intermediary would also be obligated to promptly report the same to the proper authorities under the relevant law, and also to the designated body for the Hash & URL List Database, if not the same.

76. In the former, this would necessarily entail reporting such CSEAM to the SJPU[4], the local police or the cyber-crime portal, as required by Rule 11 of the POCSO Rules[5]. While in the latter, the report would be forwarded to the authority entrusted with the maintenance of the Hash & URL List Database.

77. Upon receipt, the authority would, in turn, independently verify the flagged content, in the manner indicated above[6], and in accordance with such procedure as may be prescribed.

78. Once the flagged content is confirmed to be CSEAM, the hash and/or URL identifier of the same would be entered into the database and made available to all other intermediaries, who would then detect and remove the same, following the process applicable to CSEAM of "*Known Origin*" which we shall now discuss.

79. Where an intermediary finds a match against an entry within the Hash & URL List Database i.e., CSEAM of "*Known Origin*", the intermediary

[4] The Special Juvenile Police Unit (for short, the "**SJPU**").
[5] The Protection of Children from Sexual Offences Rules, 2020 (for short, the "**POCSO Rules**".
[6] The "Three-Step" Process discussed in **Paragraph 66**.

would be required to immediately disable and remove the same, without awaiting any further verification at its end.

80. However, we acknowledge that no database, irrespective of how carefully it is maintained, is immune from any error.

81. Thus, with a view to obviate the possibility of any inaccuracies, the intermediaries would still be obliged to report all such removals, at least to the authority maintaining the Hash & URL List database.

82. Since this exercise is only to ensure the reliability of the database and the removals in consequence thereof, we see no good reason for applying the same threshold of immediacy to such reporting as required in the case of CSEAM of "*Unknown Origin*". The intermediaries may, instead, furnish the details of all such removals in a consolidated form on a weekly basis.

83. These reports would necessarily be required to be reviewed by both the intermediaries and the authorities by cross-verifying whether the material removed did, in fact, correspond to the entry against which the match was found. Such an exercise would serve as a continuous check upon the accuracy of the database itself. With it, the authorities

would be in a position to correct or de-list any inaccurate entry at the earliest.

84. An entry that is wrongly included, or a hash identifier that begins to throw up matches against lawful content, would come to light only if the removals made pursuant to it are periodically reported and reviewed. It would also minimise the risk of misuse of the database to remove lawful content from social media platforms.

b. Requirement of Proper Notice and Grievance Redressal

85. One another aspect that we deem necessary to clarify is the form and manner of notice that an intermediary is required to give in the event of removal of any content as CSEAM.

86. In every instance where an intermediary removes any material as CSEAM, it would be required to prominently display a notice in place of such material on its platform. The notice must, *inter-alia,* indicate whether such removal was pursuant to the intermediary's own detection, or on account of a match found against a known entry in the Hash & URL List Database.

87. This is crucial for ensuring that any person aggrieved by such removal, believing the same to be erroneous, is well aware of the proper authority before whom it may be challenged.

88. Where the removal is based on the intermediary's own detection, the challenge would lie against the intermediary under the grievance redressal mechanism, and thereafter, if necessary, before the Grievance Appellate Committee, as provided in Rules 3(2) and 3A of the IT Rules, respectively.

89. Where, however, the removal is for reasons of a known match with the Hash & URL List Database, the challenge would, in substance, lie against the correctness of such entry. The same would, therefore, have to be raised before the authority maintaining the database.

90. Thus, without proper notice of the reasons for removal, any person aggrieved would be made to run from pillar to post in search of the appropriate mechanism for redressal.

91. In this regard, it would be apposite to refer to Rule 4(4) of the IT Rules, which already requires a significant social media intermediary to

display a notice to any user attempting to access information identified under the said rule. What we have in mind is only a natural extension of the same.

92. However, we make it abundantly clear that such notice shall be without prejudice to the obligation of the intermediary to preserve the material and all associated data, and to report the same to the proper authorities. Such notice shall also not reproduce or describe the material removed.

c. Additional Safeguards Required for the use of Hash & URL List Database.

93. Apart from the above, certain additional safeguards are also required to be put in place for the proper operation of such a database.

94. This is because an erroneous entry into the database would not only result in the removal of lawful content from one platform alone, but from every platform connected to the database.

95. This assumes all the more significance in the case of CSEAM of Known Origin, where the removal is triggered solely on the basis of a prior entry into the database. The removal follows automatically the

moment a match is found, with no occasion for the intermediary to await any independent determination apropos the material.

96. Thus, it goes without saying that the use of Hash & URL List Database indicated above must be accompanied by adequate safeguards, some of which we may indicate, with the actual modalities left to be worked out by the Union of India. They are: -

(i) ***First****,* each entry into the database must be preceded by multiple tiers of independent verification of the material. The preliminary screening may be through specialised software, but the final assessment must mandatorily be made by two or three trained human analysts, each of whom would independently determine whether the same constitutes CSEAM.

(ii) ***Secondly,*** for each entry**,** the authority managing the database must maintain a report of the findings recorded in the course of its assessment. Such report must also bear the digital signatures of the analysts concerned, to ensure accountability for every inclusion.

(iii) ***Thirdly***, a complete record must also be kept by such authority of every entry in the database, the source from which the material originated, the analysts who assessed the same, their

findings, and the date of its entry. Likewise, each and every access to the database, whether by an intermediary or an agency, must be logged. Such records must be preserved in a manner that permits the entries to be audited, and any lapse to be traced to its source.

(iv) ***Fourthly***, the Hash & URL List Database, and the entries made therein, must be subjected to periodic independent audits, the findings of which ought to be placed in the public domain, at least in an aggregated form.

(v) ***Fifthly,*** where it is found that a particular hash identifier or URL came to be wrongly entered into the database, the same must be promptly removed therefrom. Such removal must also be communicated to all intermediaries, so that the content removed in consequence of such wrong entry is restored with immediate effect.

(vi) ***Sixthly***, as stated earlier, there must be an effective mechanism by which any person aggrieved by the removal of content may raise a complaint, not merely with the intermediary, but also with the authority managing the database. The latter is important, where the removal is on account of a match with the

database. Since the intermediary would be merely giving effect to an entry made by the authority, it would be of little use to direct the aggrieved person to the intermediary alone.

97. Having regard to all the aforesaid, we would like the Union of India to frame a comprehensive Standard Operating Procedure for the use and operation of the Hash & URL List Database. It must delineate the roles of the authority managing the database, the intermediaries and the law enforcement agencies, and incorporate the safeguards indicated hereinabove.

C. <u>Mechanisms for the Reporting of CSEAM</u>.

98. The efficacy of any mechanism for the removal of CSEAM is ultimately measured by the process and the time within which such material is reported and consequently removed.

99. In **Just Rights** (supra), we had discussed at length the significance that the law attaches to the reporting of CSEAM, particularly under Section(s) 15, 19, 20 and 21 of the POCSO Act, respectively.

100. We observed that: -

> *"87. [...] In other words, the actus reus that is penalized under Section 15 sub-section (1) is the failure to delete, destroy or report any child pornography that was stored or in possession of any person with an intention to share or transmit the same. [...]*
>
> *xxx xxx xxx*
>
> *90. On the other hand, the mens rea which is required to constitute an offence under Section 15(1) is the intent to share or transmit a pornographic material involving a child, and the said intention is to be gathered or gauged from the actus reus itself i.e., by culling out the manner in which there was an omission to delete, destroy or report such a material or the reason behind the same. [...] Thus, it is the manner in which along with the attending circumstances attributable to the failure to delete, destroy or report that must sufficiently be indicative of the intent to share or transmit any material.*
>
> *xxx xxx xxx*
>
> *122. Thus, we are of the considered view that any form of intangible or constructive possession of any child pornographic material will also amount to "possession" under Section 15 of the POCSO in terms of the Doctrine of Constructive Possession. There is no requirement of a physical or tangible "storage" or "possession" of such material in Section 15 of the POCSO. We may clarify with a view to obviate any confusion that, where any child pornographic material is in the constructive possession of an accused, there the failure or omission to report the same would constitute the requisite actus-reus for the purposes of Section 15 sub-section (1) of POCSO.*
>
> *123. [...] Thus, when it comes to constructive possession of an accused, it is the failure or omission to report that constitutes the requisite actus-reus for the purposes of Section 15 sub-section (1) of POCSO.*
>
> *250. Section 19 read with 20 & 21 of the POCSO is one such step towards recognizing this collective responsibility of the*

society in curtailing the issue of abuse and exploitation of children. Section 19 places an obligation on any person who has an apprehension that an offence under POCSO is likely to be committed or has knowledge that such an offence has been committed, to report and provide information about the same to the Special Juvenile Police Unit or the local police. Section 19 further delineates the process and procedure in which such information or report has to be recorded by the authorities, and the course of action to be adopted. Section 20 extends such obligation to any and all personnel of media, hotels, hospitals, clubs or studios etc., to mandatorily report and provide information about any material or object which is sexually exploitative of a child (including pornographic, sexually-related or making obscene representation of a child or children) through the use of any medium to the authorities mentioned above. Any failure to do so, either in terms of Section 19 or 21 of POCSO shall be liable to be punished with imprisonment upto 6-months or fine or both. Further, any failure on the part of any employer or supervisor in reporting the commission of any offence or its apprehension in respect of a subordinate under his control, will also be liable to be punished with imprisonment which may extend to 1-year and also fine.

251. Thus, it is evident that, to achieve the avowed purpose, a legal obligation has been imposed under the POCSO Act on any person to report an offence to the relevant authorities specified therein if they have knowledge that an offence under the Act has been committed. This obligation also extends to individuals who have reason to believe that an offence under the Act is likely to be committed. In addition to imposing this legal duty under Section 19, the legislature being in seisin of the paramount importance in collectively addressing the problems of child abuse and exploitation, deemed it expedient to make the failure to discharge this obligation punishable under Section 21 of the Act. Such provisions have been inserted with a view to ensure strict compliance of the provisions under the POCSO and thereby to ensure that the tender age of children is not being abused and their childhood and youth is protected against exploitation.

xxx xxx xxx

222. We summarize our final conclusion as under: -

xxx xxx xxx

(II) *Sub-section (1) of Section 15 penalizes the failure to delete, destroy or report any child pornographic material that has been found to be stored or in possession of any person with an intention to share or transmit the same. The mens-rea or the intention required under this provision is to be gathered from the actus reus itself i.e., it must be determined from the manner in which such material is stored or possessed and the circumstances in which the same was not deleted, destroyed or reported. To constitute an offence under this provision the circumstances must sufficiently indicate the intention on the part of the accused to share or transmit such material."*

(Emphasis supplied)

101. In **Just Rights** (supra) our attention was also drawn towards a serious lapse on the part of some social media intermediaries in not reporting such harmful material in the manner prescribed by the law. The same reads as under: -

"25. She would further submit that Section 19 of the POCSO imposes mandatory reporting of an offence under the Act if there was an apprehension that such offence is likely to be committed or knowledge that such an offence has been committed. It was pointed out that the failure to discharge this obligation by itself is punishable under Section 21 of the POCSO. She pointed out that the social media platforms claim to report such instances to the National Center for Missing and Exploited Children (NCMEC), a US-based NGO, which then reports them to the National Crime Records Bureau (NCRB). However, Section 19 mandates reporting such cases to the Special Juvenile Police Unit (SJPU) or the Special Police.

Therefore, reporting to an NGO cannot absolve the social media platforms of its liability under Section 21 of the POCSO.

xxx xxx xxx

256. It has been brought to the notice of this Court that social media intermediaries do not report such cases of child abuse and exploitation to the local authorities specified under POCSO and rather only comply with the requirements stipulated in the MOU. [...]

(Emphasis supplied)

102. In this regard, we had this to say: -

"256. [...] In view of the salutary object and the mandatory character of the provisions of Sections 19 and 20 of the POCSO read with Rule 11 of the POCSO Rules, we are of the considered view, that an intermediary cannot claim exemption from the liability under Section 79 of the IT Act for any third-party information, data, or communication link made available or hosted by it, unless due diligence is conducted by it and compliance is made of these provisions of the POCSO. We are also of the view that such due diligence includes not only removal of child pornographic content but also making an immediate report of such content to the concerned police units in the manner specified under the POCSO Act and the Rules thereunder.

xxx xxx xxx

258. In view of the overriding effect of the POCSO Act and the rules thereunder, merely because an intermediary is in compliance of the requirements specified under Section 79 of the IT Act, will not absolve it of any liability under the POCSO, unless it duly complies with the requirements and procedure set out under it, particularly Section 20 of POCSO Act and Rule 11 of the POCSO Rules. It is a settled position of law, that when a statute describes or requires a thing to be done in a particular manner; it should be done in that manner or not at all. Thus, social media intermediaries in addition to reporting the commission or the likely apprehension of commission of any offence under POCSO to the National

Centre for Missing & Exploited Children (NCMEC) is also obligated to report the same to authorities specified under Section 19 of POCSO i.e., the Special Juvenile Police Unit (SJPU) or the local police."

(Emphasis supplied)

103. In view of the foregoing, we had, *inter alia*, put a suggestion for creating a more convenient mechanism for the general public to report any instance of CSEAM. The same reads as under: -

> *"260. We propose to suggest the following to the Union of India in its Ministry of Women and Child Development:*
>
> *xxx xxx xxx*
>
> *(ix) We urge the Parliament to consider amending Section 15 sub section (1) of POCSO so as to make it more convenient for the general public to report by way of an online portal, any instance of storage or possession of CSEAM to the specified authorities for the purpose of the said provision."*
>
> (Emphasis supplied)

i. Some Lacunas in the Existing Mechanism.

104. Under the IT Rules, more particularly, Rule 3(1)(d), an intermediary is required to remove or disable access to any unlawful content within three hours of receiving an order of a court or a reasoned intimation from the appropriate Government in that regard.

105. Rule 3(2)(b) of the IT Rules separately requires an intermediary to take all "*reasonable and practicable measures*" to remove any sexually

exploitative or abusive content *prima-facie* depicting any individual, within two hours from the receipt of a complaint made by such individual or any person on his behalf. Rule 3(2)(c) of the IT Rules further requires the intermediaries to implement a mechanism for the receipt of such complaints.

106. However, we find that none of the above timelines has been specifically made for the removal of CSEAM. Rule 3(2)(b) only comes into the picture, when a complaint is made by, or on behalf of, the individual depicted in the content.

107. A child victim is seldom in a position to know of, let alone report, the circulation of such material. A report made by any other member of the public who comes across CSEAM does not, squarely fall within the ambit of Rule 3(2)(b).

108. Such complaints are relegated to the ordinary grievance redressal mechanism under Rule 3(2)(a). Complaints made under the said mechanism are required to be resolved within a period of seven days from the receipt of such complaint.

109. Where, however, such complaint *inter-alia* pertains to any sexually exploitative or abusive content, the same, as per the Proviso to Rule 3(2)(a), must be resolved within thirty-six hours of receipt of such complaint.

110. Although, the IT Rules have prescribed a reasonable timeline within which the intermediaries must remove or disable any material as CSEAM, yet, experience has shown that, compliance with the same has been far from satisfactory.

111. The principal reasons for this state of affairs are twofold. *First,* the cumbersome nature of the reporting mechanism, which makes it difficult for the general public to raise complaints. *Secondly,* the less-than-ideal rate of resolution, as complaints pertaining to CSEAM are left to compete with complaints of every other nature for the attention of the Grievance Officers.

112. What is also of concern is that, insofar as intermediaries are concerned, no timeline has been prescribed within which they must report any CSEAM to the authorities specified under Rule 11 of the POCSO Rules.

ii. Streamlining and Standardization of Reporting Mechanism.

113. We are mindful of the fact that significant efforts have been made by social media intermediaries in improving the manner in which users report any content, and the process by which the same is dealt with.

114. Yet certain aspects still remain which require attention, to ensure a responsive mechanism for raising and resolving reports made by users of such platforms.

115. Rule 3(2)(a) of the IT Rules *inter-alia* requires an intermediary to prominently display, on the home page or screen of its website or application, as the case may be, the requisite details of its grievance officer as well as the mechanism through which the users may raise their complaints.

116. It appears, however, that compliance with even this basic requirement has been uneven. There have been instances where, despite repeated

reminders, the details of the grievance redressal mechanism and the grievance officer have not been published.

117. In other instances, the details so published have been found to be outdated or the instructions for raising a complaint not reflecting the mechanism actually in place.

118. That apart, we are also given to understand that certain intermediaries have created multiple convoluted channels through which a complaint may be raised. A user seeking to report any content, is often presented with a range of overlapping and often confusing categories, such as "*violation of community guidelines*", "*exploitation*", "*endangerment of safety*", "*privacy concerns*" or "*illegal activity*", each accompanied by a separate mechanism of its own.

119. This is compounded further by a complete lack of uniformity in the reporting mechanisms across intermediaries. Each intermediary has devised its own categories, its own terminology, and its own channels for reporting, with no common standard governing any of them. What one platform describes as "*child safety*" may be described by another

as "*sexual exploitation*", and by yet another as merely "*inappropriate content*".

120. The seriousness with which any report is dealt with is left to turn on the semantics and jargon, rather than on the nature of the content itself.

121. This has only led to unnecessary complexity in the grievance redressal mechanism, which, instead of facilitating reporting, only serves to confuse users and deter them from effectively using it.

122. In the limited cases where a complaint is actually lodged through one or more of the above channels, the same more often than not is closed on the ground that it ought to have been made through another mechanism. The user is then expected to begin afresh, often without being told which channel would be the appropriate one. In matters involving CSEAM, where every hour of delay aids circulation, such an approach is wholly unacceptable.

123. Another concern that has been brought to our notice is that certain reporting mechanisms often insist on personal details from the users. This creates unnecessary reluctance in the mind of those who merely wish to flag CSEAM, and as a result often choose not to report the same.

124. In our view, a distinct and clearly labelled category must be created through which CSEAM may be reported by the users. The nomenclature of such category must be simple and readily understandable by a person of ordinary prudence, irrespective of his age, literacy or familiarity with technology. The nomenclature must leave no room for doubt as to the nature of the content sought to be reported.

125. The mechanism through which such reports may be raised must also be accessible in no more than two steps from the content, profile, group or link in question. Such mechanism must also be uniform across all intermediaries and platforms.

126. The reporting mechanism must not insist upon any unnecessary or personal details from the user. The anonymity of the person reporting must be maintained at all stages, and under no circumstances must the identity of such person be disclosed.

127. Every report must be acknowledged by the intermediary upon receipt and be accompanied by a reference number through which the status of the same, and the action taken thereon may be tracked.

iii. Efficacy of the Grievance Redressal Mechanism relating to CSEAM.

128. A reporting mechanism, however accessible, is not an end in itself. It's worth lies not in the number of complaints it is able to receive, but in the number of complaints it is able to resolve properly.

129. A report which is lodged with ease, but is thereafter dealt with in a perfunctory manner, would leave the user no better off than if no report had been made at all.

130. The news report placed before us by the applicants reveals precisely this failure. It notes that, in some instances, despite reporting the

CSEAM content, the review mechanisms, upon assessment, held the same as not falling foul of the intermediary's "*standards*", and thus, allowed it to continue in circulation. The relevant excerpts read as under: -

> *"TTP said that it tried reporting ads via Meta's own reporting system and that of the 84 ads that ran in India, they were able to report 55. Meta only gives the option of reporting ads when they are live."*
>
> *"For 43 of these, TTP got a reply that said, "We've taken a look and found that this ad doesn't go against our Advertising Standards."*
>
> (Emphasis supplied)

131. If the "*standards*" applied by intermediaries in reviewing any reported CSEAM content are such that it permits the same to continue circulating, then this, in our view, is a matter of grave concern, and requires revisiting these "standards".

a. Misconception on what constitutes "CSEAM" and Misreading of our decision in Just Rights (supra).

132. The news report placed before us reveals that, although most of the reported advertisements depicted photos and videos of children engaged in "*graphic sexual acts*", yet, some of them, did not explicitly contain any such material.

133. Instead, these advertisements, to avoid detection and consequent removal, promoted tools and applications capable of manipulating such photos and videos in order to create sexually exploitative and abusive material, without any such depiction in the advertisement itself.

134. It appears that it is these advertisements which, upon assessment by the intermediary, were held to not be violative of its "advertising standards", possibly for the aforesaid reason, that they did not explicitly contain any sexually exploitive or abusive content.

135. If true, we, *prima-facie,* find the same to be an egregious error on the part of intermediaries in their understanding of what constitutes CSEAM.

136. In **Just Rights** (supra), we had this to say: -

> *"227. The term "child sexual exploitation and abuse material" or "CSEAM" more accurately reflects the reality that these images and videos are not merely pornographic but are records of incidents, where a child has either been sexually exploited and abused or where any abuse of children has been portrayed through any self-generated visual depiction*."

137. Although, in **Just Rights** (supra) we had held that CSEAM means and includes images and videos "*where a child has either been sexually exploited and abused or where any abuse of children has been portrayed through any self-generated visual depiction*", yet the said observations must be understood in the proper context in which they were made.

138. The emphasis placed by us in **Just Rights** (supra) upon a visual depiction of sexual exploitation or abuse of a child, for any material to constitute CSEAM, was made only in respect of the penal provisions under the POCSO Act.

139. This is because the POCSO Act, being a penal statute that applies to intermediaries and individuals alike, must be construed strictly. Any criminal liability under the said Act cannot be fastened in the absence of an *actus reus*; hence, the above emphasis on visual depiction.

140. However, the IT Act and the rules framed thereunder, stand on a different footing. Although the IT Act does prescribe certain offences, yet, it is not a penal statute in its entirety. A substantial part of it,

together with the IT Rules, is regulatory in nature, and governs the conduct of intermediaries.

141. The obligations of intermediaries thereunder are, consequently, much broader in their sweep. An intermediary is expected not merely to remove material which explicitly depicts the sexual exploitation or abuse of a child, but to prevent any such harm from being uploaded, hosted, promoted or circulated on its platform in the first place.

142. Mindful of the above distinction, this Court, in **Just Rights** (supra), categorically explained the contrast between what is sought to be penalized under Section 15 of the POCSO Act and Section 67B of the IT Act, which the intermediaries appear to have lost sight of.

143. In **Just Rights** (supra) we had held that Section 67B of the IT Act is a comprehensive provision designed to address and penalize the various electronic forms of exploitation and abuse of children online.

144. We explained that the said provision not only punishes the electronic dissemination of child pornographic material, but also the creation,

possession, propagation and consumption of such material as-well as the different types of direct and indirect acts of online sexual denigration and exploitation of the vulnerable age of children.

145. The relevant observations read as under: -

> "*151. From the aforesaid, it is clear that Section 67B of the IT Act is a comprehensive provision designed to address and penalize the various electronic forms of exploitation and abuse of children online. It not only punishes the electronic dissemination of child pornographic material, but also the creation, possession, propagation and consumption of such material as-well as the different types of direct and indirect acts of online sexual denigration and exploitation of the vulnerable age of children*."

146. We explained how the scope of Section 67B sub-section (b) of the IT Act is far wider in its sweep. We said that "material" for the purpose of this provision, includes not only content depicting children in sexually explicit acts but also those involving children in any "*obscene or indecent contexts*".

147. We further explained how Section 67B sub-section (b) *inter-alia* penalizes even the advertising, promotion, exchange or distribution of any material that depicts children in any obscene or indecent or sexually explicit manner.

148. We held that even the act of facilitating or propagating the circulation or dissemination of such material through advertisements or promotions from any computer resource on the internet, would fall within the purview of the said provision.

149. The relevant observations read as under: -

> *"**(ii) Section 67B sub-section (b): -***
>
> *a. It penalizes the creation of any text or image-based content in any electronic form, that depict children in any obscene or indecent or sexually explicit manner. It further penalizes the collection, solicitation, browsing i.e., online viewing, or downloading of such material. Thus, even the mere viewing of any child pornographic material that is stored in a mobile phone would tantamount to 'browsing' of such material in electronic form. Lastly, it also penalizes the advertising, promotion, exchange or distribution of any such material. Here again, what is punishable is only the actual commission of any of the above-mentioned acts.*
>
> *b. The scope of Section 67B sub-section (b), is more expansive than the preceding sub-section because, (i) first, the term 'material' here includes any electronic content depicting children in sexually explicit acts as well as in obscene or indecent contexts, and (ii) secondly, the actus reus encompasses not just the act of disseminating but also the acts of creating, propagating, or engaging with or using such material.*
>
> *c. In other words, Section 67B sub-section (b) penalizes the actual commission of any of the following: -*
>
> *i. the act of producing or creating any text or digital image based electronic material (incl. videos) that depict children in any obscene, indecent or sexually explicit manner;*

ii. *the act of engaging or using such material by way of collecting, browsing, accessing, downloading, saving, seeking, actively searching such material from any computer resource, and;*

iii. *the act of facilitating or propagating the circulation or dissemination of such material by advertising, promoting, exchanging or sharing, distributing or offering for sale such material from any computer resource on the internet.*

(Emphasis supplied)

150. We also explained how Section 67B sub-section (d) of the IT Act penalizes any form or manner of facilitation of abuse of children online. We said that the said provision penalizes all forms of degradation, exploitation, or abuse of children on any online platform.

151. We held that any act, either direct or indirect, that has the propensity or likelihood to aid, enable or support the online abuse of children in any obscene, indecent, or lewd fashion would be punishable under the said provision.

152. The relevant observations read as under: -

> *"**(iv) Section 67B sub-section (d): -***
>
> *a. Section 67B sub-section (d) penalizes any form or manner of facilitation of abuse of children, online i.e., it penalizes any form of degradation, exploitation, or abuse of children on any online platform. The actus reus punishable under the said provision is the doing, aiding or abetting of any act,*

either directly or indirectly that would facilitate or enable the abuse of children online in any indecent, lascivious or prurient manner.

b. *It is pertinent to note, that under Section 67B sub-section (d) there is no requirement that the act in question must have been done only with an intention to facilitate the abuse of children online. What is rather required to constitute an offence under the said provision is that the act must be such which likely would facilitate the abuse of children online.*

c. *In other words, what is penalized is any act that has the propensity or likelihood to aid, enable or support the online abuse of children in any obscene, indecent, or lewd fashion.*

(Emphasis supplied)

153. We further cautioned that Section(s) 67, 67A and 67B of the IT Act are a complete code, and must be construed in a purposive manner that suppresses the mischief and advances the remedy, so as to ensure that the legislative intent of penalizing the various forms of cyber-offences relating to children is not defeated by a narrow construction of these provisions. The same reads as under: -

> *"153. Thus, Section(s) 67, 67A and 67B of the IT Act being a complete code, ought to be interpreted in a purposive manner that suppresses the mischief and advances the remedy and ensures that the legislative intent of penalizing the various forms of cyber-offences relating to children and the use of obscene / pornographic material through electronic means is not defeated by a narrow construction of these provisions."*

154. It is thus abundantly clear that CSEAM is not confined to only a "*visual depiction*" within the meaning of the POCSO Act.

155. For the purposes of the IT Act and the Rules thereunder, CSEAM encompasses every form of electronic material that is harmful to children, including any material having the propensity or likelihood to facilitate, propagate or enable their exploitation and abuse.

156. This would include any electronic material which facilitates, aids, promotes or enables the creation, circulation or consumption of any material which is sexually exploitative, abusive or is otherwise harmful to a child, even if the same contains no explicit visual depiction.

157. The obligations of the intermediaries for the detection and removal of CSEAM must, therefore, also be construed accordingly.

158. The IT Rules themselves make this abundantly clear. Rule 3(1)(b) requires an intermediary to make reasonable efforts to ensure that its users do not host, display, upload, publish, transmit or share any information that is, *inter-alia*, harmful to a child.

159. Rule 4(4), in turn, requires significant intermediaries to identify any material that depicts sexually exploitation or abuse of a child, "*whether explicit or implicit*", for appropriate action.

160. None of these provisions confine the obligations of the intermediaries only to materials which explicitly depict the sexual exploitation or abuse of a child.

161. An advertisement or promotion cannot escape the rigours of the IT Act and the IT Rules merely because it does not itself contain any depiction of a child.

162. Where an advertisement promotes a tool or an application which is capable of manipulating photos and videos of children into sexually exploitative and abusive material, the same facilitates the very creation of CSEAM, and thus, would squarely fall within the ambit of Section 67B sub-section (d) of the IT Act, as held in **Just Rights** (supra). Such content would equally attract the rigours of Rule 3(1)(b) of the IT Rules for being "*harmful to child*".

163. Thus, advertisements and promotions which, though contain no such depiction themselves, and instead direct users through links or

redirections to websites and platforms where CSEAM is hosted or offered, are still, in substance an advertisement of CSEAM itself.

164. We may once again remind one and all that the absence of any explicit depiction in such advertisements is not a mere happenstance. It is, more often than not, a deliberate design to escape detection. In **Just Rights** (supra), we had taken note of precisely this *modus operandi*, whereby indirect links to such material were circulated and shared in order to avoid detection and removal. At the cost of repetition, we once again reproduce the relevant observations made by us: -

> *"109. During the course of hearing, our attention was also drawn to a recent news article that reported how on social media, links to view child pornography were being circulated and sold for anywhere between Rs. 40 to Rs. 5,000. The news report indicates, how social media platforms are rife with child sexual abuse, and gave certain insight about the modus operandi of the distribution of such material on these platforms. It explained how the sellers and distributors of child pornographic material rather than sharing any downloads to such material, would ingeniously only share links to such material instead in lieu of money, so as to circumvent the penal provisions of the POCSO and IT Act, which criminalized only the storage of such material. By indefinitely forwarding links, they completely bypass the requirement of first storing such material onto any device, and similarly those who view such material also only use the links, without ever downloading such material onto their device.*
>
> *222. We summarize our final conclusion as under: -*
>
> *xxx xxx xxx*

(IX) *Section 67B of the IT Act is a comprehensive provision designed to address and penalize the various electronic forms of exploitation and abuse of children online. It not only punishes the electronic dissemination of child pornographic material, but also the creation, possession, propagation and consumption of such material as-well as the different types of direct and indirect acts of online sexual denigration and exploitation of the vulnerable age of children. Section(s) 67, 67A and 67B respectively of the IT Act being a complete code, ought to be interpreted in a purposive manner that suppresses the mischief and advances the remedy and ensures that the legislative intent of penalizing the various forms of cyber-offences relating to children and the use of obscene / pornographic material through electronic means is not defeated by a narrow construction of these provisions."*

(Emphasis supplied)

165. Thus, the assessment of any content for determining if the same is CSEAM cannot be confined to only a surface level review. Intermediaries must look at the content as a whole, including the text, captions, keywords, links and the function of the tool or application being promoted, in order to determine whether the same facilitates or has the propensity to result in the exploitation or abuse of children.

166. Where an advertisement, by its content, context or the manner in which it is held out, promotes or provides the use of any tool or application capable of sexually exploiting or abusing children, the same cannot be permitted to remain on any platform under the guise of conformity with "*advertising standards*".

167. It follows that the community guidelines and "*advertising standards*" of every intermediary must be brought in line to suppress such mischief, and the persons entrusted with the review of reported content must be trained accordingly. Content of this nature must also be capable of being reported under the distinct category for CSEAM as discussed in the earlier parts of this judgment.

168. We would, therefore, like the Union of India to indicate the measures it proposes to undertake to ensure that the standards applied by intermediaries in reviewing content and advertisements accurately covers all form of CSEAM, direct or indirect, as discussed above. We would also like the Union of India to issue comprehensive guidelines or advisories to all intermediaries in this regard.

b. Dedicated Grievance Officers for managing CSEAM and reports related thereto.

169. It also appears that despite proper grievance redressal mechanisms being put in place by the IT Act and the rules framed thereunder, the efficacy of the same is, to a considerable extent, constrained due to the nature of responsibilities entrusted to a grievance officer, which often exceed what they can reasonably discharge within the timelines prescribed.

170. Rule 3(2)(a) of the IT Rules requires every "*intermediary*" to appoint a "*Grievance Officer*". While Rule 4(1) requires every "*significant social media intermediary*" to appoint three distinct officers; a "*Chief Compliance Officer*" responsible for compliance with the IT Act and the rules thereunder, a "*Nodal Contact Person*" for coordinating with law enforcement agencies at all times, and the aforementioned grievance officer, designated as the "*Resident Grievance Officer*".

171. As per Rule 3(2)(a), every complaint or grievance regarding any content, duty or computer resource of the intermediary is, to be received and resolved by the Grievance Officer, or the Resident Grievance Officer, as the case may be.

172. The IT Rules, more particularly Rule 3(2) prescribes different timelines for the resolution of a complaint, depending upon the severity of the grievance. A complaint of a general nature is to be resolved within seven days. Whereas, a complaint seeking removal of any content prohibited under Rule 3(1)(b), which includes CSEAM, is to be resolved within thirty-six hours, and in case of a complaint of such content by the individual depicted therein, within two hours[7].

173. We have no reason to doubt that intermediaries and their grievance officers would be prioritising complaints in accordance with the urgency prescribed by the IT Rules. Nevertheless, we are of the view that such prioritisation may not be as effective as it appears.

174. We say so because the catalogue of urgent complaints under the IT Rules is a wide one. Complaints of CSEAM are one amongst several grievances which call for the same urgency. Rule 3(1)(b) lists several categories of prohibited material, apart from CSEAM, that must, under Rule 3(2)(a), be resolved within thirty-six hours from their receipt.

[7] Rule 3 sub-rule (2) sub-clause (b) of the IT Rules.

175. The aforesaid categories are not the only grievances which call for urgent action. Orders under Rule 3(1)(d) and complaints under Rule 3(2)(b) carry much shorter timelines of three and two hours respectively.

176. Yet, complaints carrying a timeline of two hours and those carrying a timeline of seven days are both left to the same grievance officers. An officer faced with several complaints, each demanding action within a matter of hours, must still attend to them one after another, and complaints of CSEAM would inevitably, at some occasion, have to await their turn.

177. Therefore, even amongst the complaints so prioritised, those of CSEAM would continue to compete with others of comparable urgency.

178. One must also be mindful of the fact that prioritisation does not by itself, create capacity to handle complaints, particularly, when one takes into account the volume of complaints that an "*intermediary*", and more so a "*significant social media intermediary*", would receive on a daily basis.

179. The number of complaints received is also seldom the same. In certain instances, particularly when any CSEAM of "*unknown origin*" begins circulating for the first time, the complaints in respect of the same often surge.

180. Prioritisation within the rules, in such instances, is of little help, without proper capacity. It may reorder the sequence in which complaints are taken up, but it cannot ensure that each of them receives the same attention required.

181. We are conscious of the fact that certain intermediaries, more particularly significant social media intermediaries, would have several grievance officers working round the clock for resolving the complaints received.

182. However, we also cannot ignore the dismal manner in which complaints of CSEAM are presently being dealt with, as revealed by the news report before us. From what we can see, out of the fifty-five advertisements that were reported, forty-three of them were cursorily held to be compliant, while the remaining complaints elicited no

response at all from the grievance officers. The relevant excerpts read as under: -

> *"TTP said that it tried reporting ads via Meta's own reporting system and that of the 84 ads that ran in India, they were able to report 55. Meta only gives the option of reporting ads when they are live.*
>
> *For 43 of these, TTP got a reply that said, 'We've taken a look and found that this ad doesn't go against our Advertising Standards.'*
>
> *For 11 ads, they were told that the content had already been removed. They haven't received a response yet for one ad."*

183. Rule 3(2)(a) of the IT Rules requires the grievance officer of any intermediary to acknowledge the receipt of every complaint made to it within twenty-four hours. A significant social media intermediary, under Rule 4(6), is further required to provide a reference number by which such complaints may be tracked, and, "*to the extent reasonable*", furnish reasons for any action taken or not taken pursuant thereto.

184. The above stipulations were first introduced with the erstwhile IT Rules in 2021. It has been almost five years since these rules came into force. The intermediaries have had ample time to comply with the same. Yet, we find such compliance to be far from satisfactory.

185. In view of the serious lapses on the part of the intermediaries in complying with even the basic requirements under the IT Rules, we cannot help but wonder if such grievance officers are stretched beyond their capacity, particularly when it comes to complaints of CSEAM.

186. Rule 4(1)(d) of the IT Rules envisages all significant social media intermediaries to publish a monthly review of its grievance redressal mechanism, more particularly its compliance with the requirements set out in the IT Rules. We want to know from the Union of India what this exercise has yielded. What has been the extent of compliance by such intermediaries in the past five years.? Why is it that, even to this date, intermediaries continue flouting the IT Rules?

187. In any view of the matter, we deem it appropriate that every intermediary must have a dedicated grievance officer or team of grievance officers, for receiving and resolving complaints related to CSEAM. These officer(s) would be expected to further ensure the day-to-day compliance with the other requirements discussed by us in the earlier parts of this judgment, including the use of Hash & URL Listing

for the detection and removal of CSEAM, and the proper reporting of the same to the authorities.

188. This becomes all the more necessary, given that the present grievance officers appear to have been unable to correctly identify advertisements or material that indirectly promote CSEAM or other material harmful to children, as is evident from the news report. As such, the officer(s) responsible for handling complaints relating to CSEAM must be adequately trained in this regard.

189. Such officer or officers would also serve to ensure appropriate human oversight of the technical measures deployed for the detection and removal of CSEAM, as envisaged under Rule 4(4) of the IT Rules, and would further oversee the proper resolution of complaints related thereto.

190. Insofar as those complaints are concerned, where the nature of the grievance may not be apparent from the complaint itself, either due to the inadvertence of the user reporting it, or the convoluted nature of the existing mechanisms through which complaints are routed, we expect the intermediaries to put in place a proper mechanism for sifting through the complaints received by it.

191. Such mechanism must be capable of identifying, at the very threshold, complaints which pertain to CSEAM, irrespective of the heading under which the same may have been made. Complaints so identified must then be routed forthwith to the officer(s) appointed to resolve the same.

c. The Proper Authority and Timelines for reporting of CSEAM by Intermediaries.

192. We also find that none of the provisions within the IT Rules stipulates any timeline within which an intermediary must inform the authorities of any content, information, computer resource or link removed or disabled by it, either on the basis of any complaint or upon its own due diligence.

193. Rule 3(1) sub-clause (c) and (ca) of the IT Rules, respectively, are the only provisions which speak of the obligation of an intermediary to, *inter-alia,* report the commission of any offence under any law. However, the said provisions prescribe no timeline within which an intermediary must report such offences, and merely stipulate that

such report be made in "*accordance with the provisions of the applicable law*".

194. Similarly, Section(s) 19, 20 and 21 of the POCSO Act read with Rule 11 of the POCSO Rules, which together form the umbrella provisions pertaining to the reporting of any offence that may have been committed under the POCSO Act, prescribe no timeline within which a person or an intermediary must make such report.

195. In the same vein, the IT Act is also silent insofar as the reporting of offences committed under the said Act is concerned, including those under Section 67B.

196. This, to us, is a glaring omission within the IT Rules, more so in light of our categoric observations in **Just Rights** (supra) emphasizing the significance of such a requirement. The absence of a specific timeline is a matter of grave concern, particularly when it comes to CSEAM, where every hour of delay causes irreparable harm to the victim.

197. We therefore, deem it appropriate that some time-limit must be prescribed within which an intermediary, must report the commission

of any offence under any law to the appropriate authority, at least insofar as our children are concerned.

198. Thus, where an intermediary removes or disables any CSEAM in consequence of violation of Section 15 of the POCSO Act or Section 67B of the IT Act, the same must be reported to the proper authority in terms of Rule 11 of the POCSO Rules which would include the SJPU, the local police or the cyber-crime portal, as may be prescribed.

199. Keeping in mind our earlier discussions on the two separate processes, by which CSEAM is to be detected and removed, we propose the following: -

- **Proper Authorities to whom CSEAM must be Reported by Intermediaries.**
  - **(i)** Where an intermediary removes or disables any content, computer resource, information or link as CSEAM in consequence of violation of Section 15 of the POCSO Act or Section 67B of the IT Act the same must be reported in accordance with Rule 11 of the POCSO Rules.
  - **(ii)** The Proper Authority for this purpose would be the Special Juvenile Police Unit, the local police and/or the cyber-crime portal, as specified under Rule 11 of the POCSO Rules.

(iii) Where an intermediary removes or disables any CSEAM of "*Unknown Origin*" the same must also be reported to the authority entrusted with the maintenance of the Hash & URL List Database, if not already the same.

(iv) Where, however, an intermediary removes or disables any CSEAM of "*Known Origin*", upon a match being found against the Hash & URL List Database, the intermediary must furnish the details of all such removals by way of a consolidated report on a weekly basis, to the authority designated for maintaining the Hash & URL List database. The Union of India may, prescribe additional authorities to whom such reports must also be made.

- **Timelines within which CSEAM must be reported by Intermediaries.**

(i) Where an intermediary removes or disables any CSEAM of "*Unknown Origin*", on the basis of a complaint or grievance received by it, the same must be reported forthwith upon the resolution of such complaint, and in any case no later than two hours after such resolution.

(ii) Where an intermediary removes or disables any CSEAM of "*Unknown Origin*", on the basis of its own due diligence, the same must be reported within two hours from such removal.

(iii) Where an intermediary removes or disables any CSEAM of "*Unknown Origin*", on the basis of an order of a court of competent jurisdiction or reasoned intimation from the appropriate government, the same must be reported within two hours from such removal.

(iv) We reiterate, where an intermediary removes or disables any CSEAM of "*Known Origin*", upon a match being found against the Hash & URL List Database, whether pursuant to a complaint or not, the intermediary must furnish the details of all such removals, by way of a consolidated report on a weekly basis to the authority designated for maintaining the Hash & URL List database.

d. Need for a Prescribed Form for the Reporting of CSEAM by the intermediaries.

200. The reporting of CSEAM by intermediaries to the proper authorities in a timely manner, cannot, however, be the end of the matter. Any

report of CSEAM would only be of value, if the information contained therein can be meaningfully used by all authorities and stakeholders. Thus, the manner in which such reports are made is equally significant for removing CSEAM in a prompt manner.

201. At present, neither the IT Act nor the IT Rules prescribe any format in which intermediaries must report either the commission of any offence under any law, or the removal of any content, information, computer resource or link, pursuant to the provisions contained in the IT Rules.

202. We are of the considered view that there must be a standard prescribed pro-forma format in which every intermediary must report the detection and removal of any content, information, computer resource or link as CSEAM, to the proper authorities.

203. The form or content of such report must necessarily include certain relevant particulars, some of which we may indicate, with the actual modalities left to be worked out by the Union of India. They are: -

S. No.	Particulars
1.	**Hash Identifier and/or URL of the material.**
2.	**Date and Time of Detection and Removal.**
3.	**Descriptive Elements of the Material:**

	Keywords, Captions, Description associated with the material.
4.	**Type of Material:** Whether the material is an Image, Video, GIF, Link, Tool, Application, Advertisement etc. (including its file type or extension, where applicable).
5.	**Mode of Circulation or Hosting:** Whether the material was found in a public post; a user's status, story or biography; a private group or channel; a direct message; or the intermediary's gallery/cloud.
6.	**If depicting any Real Individual:** Whether the material depicts a real individual or is synthetically generated, including whether: - i. It is a morphed or synthetically manipulated depiction of a real individual, ii. It appears to depict a victim who is identifiable, or who has been previously identified.
7.	**Nature of Material:** Whether the material is of: i. Unknown Origin (including the Hash / URL identifier generated by the intermediary) or, ii. Known Origin (including the Hash / URL Entry matched against such material).
8.	**Mechanism through which Detected (including the necessary details of the same):** Whether the material was detected by way of: - i. Complaint by a user or victim, ii. Order of a court or reasoned intimation from appropriate government, iii. Match against the National Hash & URL List Database or iv. Intermediary's own due diligence and detection tools.
9.	**Assessment by the Intermediary (only in case of CSEAM of Unknown Origin):** The reasons recorded during the assessment of such material, including the details and e-signatures of the human analysts involved.

204. The format of such report must be in a machine-readable form, capable of being automatically processed by the computer resources of all necessary stakeholders.

205. A uniform machine-readable format would ensure that such reports can be meaningfully used for updating the Hash & URL List Database, and easily integrated with other repositories such as the National Crime Records Bureau (NCRB) and the National Database on Sexual Offenders (NDSO).

206. It would also facilitate better coordination with other stakeholders, such as Internet Service Providers (ISPs), and further aid investigating authorities such as the Special Juvenile Police Units and Cyber Cells in their endeavours to identify patterns in the distribution of CSEAM and the networks responsible for the same, to investigate and prosecute the perpetrators, and to track down and rescue the victims of such offences.

e. Safeguards for the Grievance Redressal Mechanism in respect of CSEAM.

207. To ensure that the grievance redressal mechanism and the officer(s) operating the same function responsibly and, in the manner, expected of them, we deem it appropriate to briefly discuss and reemphasize certain safeguards necessary for this purpose.

208. Every intermediary, in accordance with Rule 3(2)(a) of the IT Rules, must prominently display, on the home page or screen of its website or application, as the case may be, the requisite details of the grievance officer(s) as well as the mechanism through which users may raise their complaints.

209. Every intermediary must also ensure that such information is regularly updated, so as to accurately reflect the details of its grievance redressal mechanism and the officer(s) entrusted with the same.

210. In this regard, we would like the Union of India to apprise us of the extent of compliance with this requirement by the various intermediaries, and of the action taken, if any, against intermediaries found to be in default.

211. The grievance redressal mechanism of every intermediary must provide a distinct and clearly labelled category for the reporting of CSEAM. The nomenclature of such category must be simple, readily understood by any person irrespective of age, literacy or familiarity with technology, and must leave no doubt as to the nature of the content being reported.

212. Such mechanism must also be made accessible within two steps from the content, profile, group or link in question, and must be uniform across all intermediaries. The Union of India is thus requested to put in place certain guidelines for ensuring the same.

213. Any content reported as CSEAM or complaint thereof must be assessed thoroughly. Such assessment must be done keeping in mind the provisions of Section(s) 15 and 67B of the POCSO and IT Act, respectively. The assessment, must involve examining the content as a whole, including the text, captions, keywords, links and the function of the tool or application being promoted, in order to determine whether the same facilitates or has the propensity to result in the exploitation or abuse of children.

214. The grievance officer(s) persons entrusted with the review and resolution of such complaints must be adequately trained to identify CSEAM, including material which may not be explicit on its face but nevertheless carries either the likelihood of exploitation or abuse of children or is otherwise harmful to them.

215. The intermediaries must ensure that such officer(s) receive necessary training from time to time, particularly in respect of any and all new *modus operandi* that may emanate in the circulation of CSEAM. The intermediaries must also allocate adequate resources to the grievance redressal mechanism and the officer(s) entrusted with it, for continued efficiency of the same.

216. No report or complaint of CSEAM ought to be disposed without the same having been reviewed by a trained grievance officer. Automated tools may be used to assist the preliminary screening of such reports. However, the ultimate decision, must be taken by a trained grievance officer, entrusted with such duty. Such assessment, must record the findings of the office in the course of his assessment, and bear his digital signature, to ensure accountability.

217. We may remind that, Rule 4(4) of the IT Rules, already requires appropriate human oversight of the automated tools deployed by significant social media intermediaries. The requirement for recording the findings and affixing signature to the same is only an extension of this statutory requirement.

218. Every report or complaint relating to CSEAM, must be acknowledged within twenty-four hours from receipt, and must be accompanied by a reference number to track the status of the same. Any decision or action taken in respect of the same must be communicated to the complainant along with the reasons thereof.

219. We are conscious that Rule 4(6) as it presently stands, requires only significant social media intermediaries to provide the means for tracking complaints, and to furnish reasons for any action or decision by it "*to the extent reasonable*". We however are of the view that this compromises the accountability required in the resolution of complaints as grave as those of CSEAM. We therefore urge the Union of India to extend the aforesaid requirements to every intermediary insofar as complaints of CSEAM are concerned by introducing suitable amendments within the IT Rules.

220. Every intermediary must publish a monthly compliance report detailing the number of complaints received by it, the action taken in respect of the same, the time within which such complaints were resolved, and the content, information or link or any part thereof removed or disabled pursuant to such complaint or by its own due

diligence. Complaints pertaining to CSEAM must in particular be disclosed under a separate section within the report. Such reports must be periodically subjected to independent audit by an appropriate authority designated by the Ministry of Electronics and Information Technology, so as to oversee the continued compliance of the various requirements under the IT Rules. The Union of India is urged to make suitable changes within the IT Rules, more particularly Rule 4(1)(d), for setting out the above requirements.

221. It has been further brought to our notice that in many appeals preferred against the decisions of the grievance redressal mechanisms of intermediaries, the orders passed by the Grievance Appellate Committee are not complied with in a timely manner.

222. We would therefore like to know from the Union of India, the mechanism, if any, by which compliance with such orders is presently monitored, and the action taken against intermediaries found to be in default of the same.

D. <u>Penalties for persistent failures by Intermediaries in complying with the requirements of IT Rules</u>.

i. Need to rethink and move beyond Section 79 of the IT Act.

223. If there is one theme that can be discerned from all our discussions above, it is the persistent failure of intermediaries, in one form or another, to comply with the various requirements envisaged under the IT Rules.

224. One reason that may explain why the intermediaries, despite being given numerous opportunities, continue to flout the IT Rules is the absence of any meaningful consequence for failing to comply with the IT Act and the rules thereunder.

225. Under the IT Act and rules framed thereunder, an intermediary which fails to observe or comply with any of its regulatory requirements, faces only one consequence; the loss of the "safe harbour" protection afforded to it under Section 79.

226. Once such protection is lost, the intermediary along with any person responsible for such failure, as the case may be, becomes liable for any content or information hosted on its platform, and may be prosecuted

and punished for the same, under the relevant law for the time being in force. In the case of CSEAM, this would include offences under Section 15 and 67B of the POCSO and IT Act, respectively.

227. The consequence of an intermediary's failure to comply with the requirements of the law in discharge of its duty is confined to it being held liable for and proceeded against, *qua* a particular content or information, which constitutes an offence under any law for the time being in force.

228. In other words, it fastens a *post facto* liability upon the defaulting intermediary, only after an offence is committed, by the upload, publication or hosting of any particular content or information on its platform.

229. Although such an approach may be suitable where the harm sought to be addressed is capable of being remedies after the fact, yet the same cannot be said for CSEAM.

230. The harm that is occasioned by such material is not confined to the moment of its creation. Every instance of its circulation, every view, and every download, revictimizes the child depicted therein.

231. The continued circulation of CSEAM does irreparable harm to the society. It fuels the consumption and demand for such exploitative and abusive material; it normalises abuse of children and emboldens those who seek it out.

232. In such a scenario, the *post facto* prosecution and punishment, howsoever successful, of those responsible for allowing the upload, circulation and viewing of CSEAM, even if indirectly or inadvertently, can hardly undo the harm that has already been done.

233. Even otherwise, Section 79 of the IT Act does not address the systemic lapses and their continuance the on part of the intermediaries in discharge of their duties in accordance with the law. Despite the requirement to observe due diligence in their functioning, the said provision springs into action not upon a wilful failure to do the same, but only after the commission of any offence in consequence thereof.

234. In other words, it does not address the failure to comply, but only the aftermath that follows such failure. An intermediary may persistently fail to comply with the requirements of the IT Act and the rules

thereunder, and yet face no consequence whatsoever, unless and until an offence comes to be committed through some particular content on its platform.

235. Several provisions of the IT Act and the IT Rules, particularly those relating to grievance redressal, detection of unlawful and harmful material and the timely reporting thereof, acknowledgement of complaints, etc., are provisions that are intended to serve as a safety-net for users. They are there to ensure that the experience of users, irrespective of the platform, remains fair, their dignity secure, privacy intact and safety uncompromised, in the course of their use of the internet. The failure in complying with such provisions may still adversely affect users and their right to use the internet, without constituting any offence in itself.

236. Section 79 of the IT Act, in such situations, proves to be an unusually inept provision. It is too drastic to be invoked for every instance of non-compliance, and too remote to deter the same. The result is that routine defaults go unchecked, while the consequence prescribed by law is seldom invoked.

237. This also renders certain provisions of the IT Rules otiose and redundant. Provisions which are preventive in nature, such as Rule 3(1)(b), which requires intermediaries to make reasonable efforts to prevent users from publishing any unlawful, exploitative or abusive content, remain hollow and, at best, curative in effect.

238. Should the IT Act and the rules framed thereunder remain a toothless tiger in such situations? The answer to the same must be an emphatic "no".

239. What is therefore, in our view, required is a distinct set of consequences that are attracted by the default itself. Consequences capable of being invoked without awaiting the commission of an offence, which keep the object of diligence and deterrence intact while remaining proportionate to the nature, gravity and frequency of the default.

ii. Exemplary Monetary Fines and Penalties.

240. Various jurisdictions across the globe follow suit with a similarly designed framework insofar as penalties and liabilities are concerned

for any non-compliance with the regulatory requirements, particularly in respect of CSEAM.

241. In the United States, Section 2258A of Title 18 of the United States Code casts an obligation upon providers of electronic communication and remote computing services to report any apparent instance of CSEAM which comes to their actual knowledge, to the CyberTipline of the National Centre for Missing & Exploited Children.

242. While sub-section (e) of the said provision prescribes the consequence for a knowing and wilful failure to make such report, in the form of a substantial monetary penalty.

243. With the REPORT Act of 2024, both the aforesaid aspects underwent significant change. It expanded the categories of instances within Section 2258A that must now be reported to *inter-alia* also include child-trafficking and the enticement of minors, along with considerably enhancing the penalties under sub-section (e) for the failure in doing so.

244. The penalty prescribed is graded on two distinct metrics. *First*, by the size of the intermediary or "*provider*". An intermediary with 100

million or more monthly active users faces a higher fine for such failure. *Second,* by the recurrence of the default, with a higher fine being prescribed for a second or subsequent failure.

245. Accordingly, a provider for its first instance of failure, would be fined up to $600,000 or $850,000, depending upon its size, with subsequent failures extending it to $850,000 and $1 million respectively.

246. Similarly, the United Kingdom's Online Safety Act, 2023 places a range of duties upon "*providers*" of user-to-user online services. These include duties to assess the risk of illegal content appearing on their services, to take proportionate measures to mitigate such risk, and to swiftly remove such content once they are alerted to it. CSEAM forms one of the most serious categories of illegal content under the said Act.

247. The Office of Communications or "Ofcom", the regulator for the enforcement of these duties, is vested with a wide array of powers. These include issuing notices requiring providers to furnish any information necessary to assess the extent of their compliance, provisional notices of contravention or non-compliance, followed by penalties upon confirmation; along with enforcement notices

requiring providers to take specific steps to comply, or use specific technology to detect illegal content.

248. The penalty for breach of any duty by an intermediary or "*provider*" is an exemplary fine of up to £18 million, or 10% of the worldwide revenue of such provider, whichever is greater. The fine may be imposed as a single amount, or at a daily rate, in case of a continuing breach, and must be appropriate and proportionate to the breach.

249. Within the European Union, Regulation (EU) 2022/2065, more popularly known as the Digital Services Act, governs the obligations of providers of intermediary services, particularly in respect of illegal content such as CSEAM.

250. This, *inter-alia,* includes putting in place an accessible mechanism to report illegal content, acting upon such reports promptly and notifying suspicions of criminal offences to law enforcement authorities.[8] While "*very large online platforms*" and "*very large online search engines*" must also assess and mitigate systemic risks of

[8] Arts. 16, 17 and 18 of the Digital Services Act; Regulation (EU) 2022/2065.

dissemination of illegal content and harm to children on their services.[9]

251. Insofar as penalties are concerned, the EU does not directly draw a distinction based on the size of the provider. Such distinction matters only for the authority overseeing the compliance, with "*very large online platforms"* and "*very large online search engines*" being regulated by the European Commission, and the remaining platforms by the Digital Services Coordinator of each Member State.

252. Article(s) 52, 74 and 76 of the said Regulation, *inter-alia,* set out the penalty for any infringement of these obligations. The consequence for such failure is, again, a substantial fine, of up to 6% of the annual worldwide turnover of the provider in the preceding financial year.

253. In the event of continuing defaults, a periodic penalty of up to 5% of the average daily worldwide turnover of such provider may be imposed for every day in default. The actual sum imposed must be effective, proportionate and dissuasive, keeping in mind the nature, gravity, duration and recurrence of the infringement.

[9] Arts. 34 and 35 of the Digital Services Act; Regulation (EU) 2022/2065.

254. In Australia, the eSafety Commissioner, the centralised regulator under the Online Safety Act, 2021, is armed with sweeping powers to compel the removal of harmful content, formulate industry standards of safety and enforce the same.

255. The industry standards, as revised from time to time, *inter-alia,* require various service providers to assess the risk of harmful content such as CSEAM, deploy appropriate systems to detect and remove the same, and furnish their reports to the Commissioner.

256. Any failure to comply with the above may, in the first instance, be met with a formal warning from the Commissioner, with subsequent or persistent breaches entailing a court ordered civil penalty of up to AU$ 49.5 million per breach.

257. In South Korea, the Telecommunications Business Act imposes obligations upon "*value-added telecommunications service providers*" in respect of "*illegal filmed materials*", an expression which includes CSEAM. Under Article 22-5 thereof, such providers must delete, or block access to, any such material upon becoming aware of it.

258. It further requires providers above a certain threshold of size or reach to take technical and managerial measures to prevent the circulation of such material in the first place. These include filtering content against material already determined to be illegal, restricting related search results, and maintaining a mechanism for users to report such material.

259. An intentional failure to delete, or block access to, such material attracts a "*penalty surcharge*" or fine of up to 3% of the sales of the provider, under Article 22-6 thereof. While a failure to implement any of the above preventive measures attracts an administrative fine of up to ₩50 million, under Article 104(1).

260. What can be discerned from the above is that, in most jurisdictions, the failure to comply with any regulatory requirements, particularly those relating to matters as serious as CSEAM, is itself visited with a consequence, usually exemplary fines, irrespective of whether any offence has been committed through such failure.

261. The quantum of such fines is determined having regard to the gravity, duration and recurrence of the default. Such quantum is also decided

upon the size or turnover of the intermediary, ensuring that the penalty remains an effective deterrent.

262. For the convenience of exposition, a tabular illustration of the same is given below: -

Country	Penalty Provided
United States	**18 U.S.C. § 2258A(e) (as amended by the REPORT Act, 2024.)** ***Failure to Report apparent CSEAM, Child-trafficking or Enticement of Minors.*** <u>First Instance of Default</u>: ▪ Fines up to $600,000 for providers with less than 100 million active monthly users. ▪ Up to $850,000 for providers with more than 100 million active monthly users. <u>Second or Subsequent Defaults</u>: ▪ Fines up to $850,000 for providers with less than 100 million active monthly users. ▪ Fines up to $1,000,000 for providers with more than 100 million active monthly users.
United Kingdom	**Online Safety Act, 2023, ss. 10 & 137; Sch. 13, paras 2(4) and 4(1).** ***Failure to comply with the duties in relation to illegal content, including CSEA Content (risk assessment, prevention and swift removal).*** <u>Individual Instance of Breach of Duty</u>: Fines up to £18 million, or 10% of the worldwide revenue of the provider, as a single amount. <u>Continuing Breach of Duty</u>: Fines up to £18 million, or 10% of the worldwide revenue of the provider, at a daily rate for all days in default.
European Union	**Digital Services Act : Regulation (EU) 2022/2065, Arts. 52, 74 & 76.** ***Failure to comply with obligations in relation to illegal content (resolution of complaints, reporting, assessment and mitigation of risks of dissemination).*** <u>Individual Instance of Breach of Obligation</u>

	Fines up to 6% of the annual worldwide turnover of the provider in the preceding financial year. Continuing Breach of Obligation Periodic fines up to 5% of the of the average daily worldwide turnover of the provider for every day in default.
Australia	**Online Safety Act, 2021, ss. 143-147 & 162.** ***Failure to comply or breach (Risk assessment, detection and removal or reporting).*** Penalty for Breach or Failure to comply Either a formal warning or a civil penalty up to AU$ 49.5 million per breach (discretionary).
South Korea	**Telecommunications Business Act, Arts. 22-5, 22-6 & 104(1).** ***Failure to delete or block CSEAM or implement preventive measures for its dissemination or circulation.*** Intentional Failure to Delete or Block Fine (Penalty Surcharge) of up to 3% of the sales of the provider. Failure to implement Preventive Measures Administrative fine of up to ₩50 million.

263. We, therefore, request the Union of India to take note of the aforesaid, and give a serious thought to putting in place a similar framework, which would be suitable and workable for India, in addressing the continued breach of various duties under the IT Act and its rules, intended for the safety of internet users, particularly when it comes to the circulation of CSEAM.

264. Keeping in mind the scope of the present *lis*, we further make it clear that the framework of penalties that we have contemplated to be

devised by the Union of India would be confined to those duties of intermediaries under the IT Act and the IT Rules that relate to or aid in the removal of CSEAM. This would include the detection and removal of such material, the maintenance of a proper grievance redressal mechanism, and the effective resolution of complaints pertaining to the same.

iii. Scrutiny and Disgorgement of "Profits" from Paywalled Content.

265. We are conscious that a medley of other penalties also find favour in some of the jurisdictions discussed above. For instance, both the United Kingdom and the European Union envisage a court ordered temporary suspension of business operations of erring intermediaries as a last resort against wilful persistent failures.

266. However, we need not dwell on this much. We are of the view that, for the present, penalties in the form of exemplary fines would suffice to meet the exigencies at hand. In any event, for cases of serious persistent failures, Section 79 of the IT Act would always be available as a last resort in such occasions.

267. There is, however, one another aspect of the matter which, in our view, calls for something more. It has come to our knowledge that several intermediaries permit their users to offer "*content*" on a pay-per-view or subscription basis, access to which is placed behind a paywall.

268. The content so offered is often promoted through questionable lewd means, under the guise of "exclusivity" by the content-creators and, in part, by the intermediaries themselves.

269. For the present moment, we are not concerned with the means by which such content is promoted to draw in users. What concerns us is that such paywalled content enjoys a far lower threshold of scrutiny on the part of the intermediaries than content generally available on their platforms. This makes such paywalls a potent means of indirectly offering and circulating illicit and harmful material or links thereto, including CSEAM.

270. What is of graver concern is the clandestine approach of intermediaries in turning a blind eye to the nature of content offered as well permitting the same to reach all users, including children on their platform. This is because intermediaries often stand to profit

from such content, whether by way of a share in the subscription or the fee so collected, or otherwise.

271. Which is why intermediaries often continue to feign ignorance to scrutiny of such content until the same is uncovered and exposed as an illicit means of circulating CSEAM or links thereto. By the time this happens, the harm has already been done, and the profits already earned.

272. We are, therefore, of the considered view that stricter penalties are required to discourage and put an end to this clandestine approach of some intermediaries of "*profiteering until prohibited*".

273. To that end, where any CSEAM or prohibited material is found to have been hosted, uploaded, promoted or circulated, directly or indirectly, through any paywall or subscription from which the intermediary derives any revenue, the revenue so derived from such content should be forfeited and disgorged. This should be in addition to any exemplary fine that may imposed for the contravention of any duties under the IT Act and the rules thereunder, as may be prescribed by the Union of India in due course.

274. The fines so imposed must also take into account the serious gravity of such breach of duties, and, where appropriate in the attending circumstances, such conduct must also attract the relevant action under Section 79 of the IT Act and proceedings under the appropriate penal laws.

275. We further put all intermediaries to strict notice that any content offered behind a paywall, or on a subscription basis, must be subjected to a rigorous scrutiny to ensure that the same does not violate the IT Act, the IT Rules or any other law for the time being in force.

276. Every intermediary must ensure that no CSEAM, or any other material having the propensity or likelihood to harm children, is offered, hosted, uploaded, promoted or circulated through such paywall or subscription, either directly or indirectly.

277. Intermediaries must further take all measures to ensure that any content, paywalled or otherwise, which depicts or promotes anything obscene, indecent or sexually explicit, or which is otherwise lascivious or prurient in nature, is not promoted to any children on their

platforms. Every care must also be taken to ensure that no child is able to subscribe to, or otherwise access, such content.

278. In this regard, we request the Union of India to frame appropriate guidelines for ensuring the proper scrutiny of paywalled and subscription-based content by intermediaries for the detection and removal of CSEAM. Guidelines must also be put in place for making use of reasonable and proportionate measures to moderate the nature of content that can be accessed or subscribed to by our children. Needless to say, such exercise must be done, keeping in mind Articles 14, 19 and 21 of the Constitution.

279. Lastly, the Union of India is requested to also consider whether the penalties that it may prescribe in respect of any breach of duty by an intermediary under the IT Act or the rules thereunder should also include the disgorgement of any revenue derived by such intermediary in case of misuse of paywalls and subscriptions by its users for the promotion, circulation, dissemination of CSEAM.

E. **Article 21 and the Right to Access Internet.**

280. We must, at this juncture, address ourselves on one another aspect that we deem necessary to clarify.

281. From what we have been able to gather, there has been a growing yet short-lived tendency across the globe in the recent past to limit the access of children below a certain age to the internet, more particularly to social media platforms, in the name of their safety.

282. In the course of the present proceeding, we too gave this our anxious consideration, and only thereafter, we decided consciously not to endorse the same.

283. We do not, for a moment, doubt the *bona-fides* with which such measures are usually proposed. We are also conscious of the fact that the internet, as it exists today, is far from safe for our children. The very necessity of the present proceedings is proof enough of the same.

284. That being said, we are of the considered view that any measure for the safety of children must be directed at the harmful material and those responsible for the same, and not at the children themselves.

285. We say so because, insofar as CSEAM is concerned, the wrongdoer is the person who creates, circulates, sells or seeks out such material, and the intermediary which fails to detect and remove the same. To keep the child

away from the internet on account of such failures would be to mistake the victim for the problem.

286. The means by which measures relating to age-based restrictions are achieved are themselves an overreach. Such processes, inevitably, always require identifying and ascertaining the age of each and every user, continuous collection and monitoring of sensitive data and an overall disproportionate risk of misuse and surveillance, the kind which finds no place within the right to privacy of our people.

287. The right to freedom of speech and expression under Article 19(1)(a) of the Constitution has never been understood as being confined to the right to speak alone. It has always been construed to include the right to know and to receive and impart information and ideas. [See, **Secretary, Ministry of Information & Broadcasting v. Cricket Association of Bengal, (1995) 2 SCC 161**]

288. The internet is, without a doubt, the marketplace of ideas, creative expression and information. Its value is priceless, not merely in the information it holds, but in the access it affords, to adults and children alike. For many children, particularly in remote areas, it is often the only source of learning and information. Likewise for children with

special needs, the internet is often the only place where they are able to find company in others like them.

289. In **Anuradha Bhasin v. Union of India** reported in **(2020) 3 SCC 637**, a three-Judge Bench of this Court examined the legality of suspension of internet services. It held that the freedom of speech and expression and the freedom to carry on any trade or business through the medium of the internet is constitutionally protected as a fundamental right under Article 19(1)(a) and 19(1)(g) of the Constitution.

290. Although, this Court in **Anuradha Bhasin** (supra) refrained from expressing any view on whether the right to access the internet is, by itself, a fundamental right and left the question of law open for future discourse, yet, this issue is no longer *res-integra*.

291. In **Pragya Prasun & Ors. v. Union of India** reported in **2025 INSC 599**, a two-Judge Bench of this Court of which one of us (J.B. Pardiwala J.) was part of, had the occasion to consider the exclusion of persons with disabilities from the digital KYC process. Holding such exclusion to be violative of Article 21, this Court, speaking through R. Mahadevan J., held that the right to digital access is an intrinsic component of the right to life under Article 21 of the Constitution and that it is the

obligation of the State to proactively design and implement inclusive digital ecosystems that serve not only the privileged but also the marginalized, those who have been historically excluded. The relevant observations read as under: -

> *"17. At this juncture, we may also wish to observe that in the contemporary era, where access to essential services, governance, education, healthcare, and economic opportunities is increasingly mediated through digital platforms, the right to life under Article 21 of the Constitution must be reinterpreted in light of these technological realities. The digital divide – characterized by unequal access to digital infrastructure, skills, and content – continues to perpetuate systemic exclusion, not only of persons with disabilities, but also of large sections of rural populations, senior citizens, economically weaker communities, and linguistic minorities. The principle of substantive equality demands that digital transformation be both inclusive and equitable. As already pointed out, persons with disabilities encounter unique barriers in accessing online services due to the lack of accessible websites, applications and assistive technologies. Similarly, individuals in remote or rural areas often face poor connectivity, limited digital literacy, and a scarcity of content in regional languages, effectively denying them meaningful access to e-governance and welfare delivery systems. In such circumstances, the State's obligations under Article 21– read in conjunction with Articles 14,15 and 38 of the Constitution must encompass the responsibility to ensure that digital infrastructure, government portals, online learning platforms, and financial technologies are universally accessible, inclusive and responsive to the needs of all vulnerable and marginalized populations. Bridging the digital divide is no longer merely a matter of policy discretion but has become a constitutional imperative to secure a life of dignity, autonomy and equal participation in public life. The right to digital access, therefore, emerges as an intrinsic component of the right to life and liberty, necessitating that the State proactively design and implement inclusive digital ecosystems*

that serve not only the privileged but also the marginalized, those who have been historically excluded."

(Emphasis supplied)

292. In view of the foregoing, we have no hesitation in saying that the right to access and use the internet is a fundamental right of every individual under Article 21 read with Article 19(1)(a) of the Constitution. Our children, irrespective of their age enjoy the same rights, and to deny the same altogether would be as absurd as saying children below a certain age do not have a conscience worth protecting or a freedom of speech worth expressing. The safety of our children and their freedom are not at odds with each other. Our children are entitled to both.

293. The experience of other jurisdictions which have deployed such restrictions is equally instructive in discerning that the efficacy of these measures remains far from established.

294. The same reveals that children do not cease to use the internet merely because the law prohibits them from doing so. They continue to use the same, albeit without the knowledge of their parents or the

authorities. They move to other platforms and websites that are unregulated and even more unsafe.

295. Such restrictions also make children who are being enticed or threatened on the internet reluctant in reporting the same to parents, guardians and trusted adults out of fear of reprisal for using the internet. This would significantly undermine the safety of our children, who are already apprehensive about confiding such incidents, even without such restrictions, and defeat the avowed object of the POCSO Act.

296. Even otherwise, keeping children away from social media platforms would, by no stretch of imagination, reduce incidents such as those revealed in the news report placed before us. Without proper safeguards, and earnest efforts by all stakeholders in the detection and removal of CSEAM, such material will continue to circulate and embolden those who seek out the same.

297. All that we are trying to say is that any blanket restriction on the access of internet by children is nothing more than unproven measures of proven disproportionality. No jurisdiction has, so far, been able to demonstrate that children are any safer on account of such measures.

298. Its efficacy is at best contested, and without question, not a substitute for the initiative and efforts required from all the stakeholders, be it the intermediaries, the law enforcement agencies, the Ministry of Electronics and Information Technology or the courts.

299. However, this does not mean that there should be no age-based restrictions. We acknowledge that, some form of safeguards are necessary for the safety our children online and the moderation of the content accessible at their fingertips.

300. In this regard, there could be a system that places greater emphasis on parental consent, guidance and oversight on the access to social media platforms by children along with a dedicated "child mode" for such accounts with measures proportionate to the object of ensuring their safety.

301. These may include accounts being made private by default, restrictions on contacts and messages from unknown adults, moderation of advertising and content accessible to children. Such measures may be implemented for pre-teens, with a reasonable and proportionate means to verify parental consent in respect of the same.

We leave the actual modalities of the same to the wisdom of the Union of India.

302. We may clarify with a view to obviate any confusion that, nothing stated hereinabove would preclude the Union of India from restricting the access of children to specific categories of content or services that are inherently harmful to them, such as adult content websites etc.

303. We further make it abundantly clear that nothing in the framework that we have proposed, or the suggestions made in the earlier parts of this judgment, should be understood as an endorsement to use or repurpose such measures for anything other than the detection and removal of CSEAM and the overall creation of an accessible space within the internet free from such harm. We make it clear, that the use of Hash & URL List databases and other similar measures shall be confined to the detection and removal of CSEAM alone.

F. <u>Awareness on Digital Safety, Sex Education and Measures to support Wellbeing of Children</u>.

304. Before we close this matter, we must address ourselves on one another aspect. Our discussion thus far has largely been centred on the obligations of intermediaries in respect of CSEAM, the measures

necessary to stop those who propagate and circulate such material, and the gaps within the existing framework that allow it to finds its way onto the internet.

305. But this cannot be the end of the matter. The safety of our children is not complete without adequate efforts towards inculcating in them the awareness to recognise danger, the confidence to speak up and the safe practices to follow, on and off the internet.

306. Our children today come onto the internet much before they come to understand it. A child is able to use a phone long before he or she is able to tell the difference between a friend and a stranger posing as one, an innocent request from an inappropriate one, a harmless game from a carefully laid trap. Those who prey upon our children are well aware of this, and it is this very gap which they exploit.

307. In **Just Rights** (supra) we had discussed the widespread misconceptions surrounding sex education and how the same has long stood in the way of the safety of our children. We said that: -

> *"238. In India, the misconceptions about sex education are widespread and contribute to its limited implementation and effectiveness. Many people, including parents and educators,*

hold conservative views that discussing sex is inappropriate, immoral, or embarrassing. This societal stigma creates a reluctance to talk openly about sexual health, leading to a significant knowledge gap among adolescents.

239. One prevalent misconception is that sex education encourages promiscuity and irresponsible behaviour among youth. Critics often argue that providing information about sexual health and contraception will lead to increased sexual activity among teenagers. However, research has shown that comprehensive sex education actually delays the onset of sexual activity and promotes safer practices among those who are sexually active.[18]

240. Another common belief is that sex education is a Western concept that does not align with traditional Indian values. This view has led to resistance from various state governments, resulting in bans on sex education in schools in some states. This type of opposition hinders the implementation of comprehensive and effective sexual health programs, leaving many adolescents without accurate information. This is what causes teenagers and young adults to turn to the internet, where they have access to unmonitored and unfiltered information, which is often misleading and can plant the seed for unhealthy sexual behaviours."

(Emphasis supplied)

308. Accordingly, we laid considerable emphasis on positive age-appropriate sex education. We had said that such education is not confined to the biological aspects of reproduction alone. It extends to consent, healthy relationships and respect for others, and plays a critical role in preventing harmful sexual behaviour, including the distribution and viewing of CSEAM. We said that: -

"234. Given the severity and far-reaching consequences of child sexual exploitation, there is a clear legal and moral imperative to take strong action against those who produce, distribute, and consume CSEAM. This includes not only criminal penalties for those involved in CSEAM but also preventative measures, such as education and awareness campaigns. [...]

xxx xxx xxx

236. In our society, where social stigma and notions of honour and shame are deeply entrenched, the social repercussions for victims are particularly severe. Many victims face intense social stigmatization and isolation, finding it difficult to form and maintain healthy relationships due to trust issues and trauma-related challenges. The stigma attached to being a victim of CSEAM can create significant barriers in social interactions, causing victims to withdraw and feel alienated from their communities. The continuous re victimization through the sharing and viewing of these materials perpetuates the victims' suffering. Each instance of someone viewing or distributing the material represents a new violation, making it harder for victims to heal. This ongoing trauma can severely impact their self-esteem and self-worth, leading to long-term emotional and psychological damage. Furthermore, the impact extends to their education and employment opportunities. Many victims struggle to concentrate on their studies or work due to the overwhelming emotional burden they carry. This can lead to academic underachievement, difficulty in securing employment, and economic hardships, compounding their sense of insecurity and instability.[17]

237. Providing compassionate and comprehensive support is crucial to help victims heal and reclaim their lives. Therapeutic interventions, including trauma-informed counselling and support groups, can offer a safe space for victims to process their experiences and begin to heal. Legal and social support services are also essential to help victims navigate the complexities of their situation and rebuild their lives.

xxx xxx xxx

243. Positive age-appropriate sex education plays a critical role in preventing youth from engaging in harmful sexual behaviours, including the distribution, and viewing of CSEAM.[20] Positive sex education focuses on providing accurate, age-appropriate information about sexuality, consent, and respectful relationships. Research indicates that comprehensive sex education can significantly reduce risky sexual behaviours, increase knowledge, enable healthy decision-making, reduce misinformation, delay sexual debut, decrease the number of sexual partners, and increase contraceptive use. The research done in India has shown the need for comprehensive sex education programs. A study of over 900 adolescents in Maharashtra found that students not exposed to scientific literature on reproductive and sexual health were more likely to initiate sex early.[21]

244. Furthermore, positive sex education promotes healthy attitudes towards sexuality and relationships, which can counteract the distorted perceptions often associated with the consumption of child pornography. It can also help foster greater empathy and respect for others, reducing the likelihood of engaging in exploitative behaviours. Comprehensive sex education programs also teach youth about the importance of consent and the legal implications of sexual activities, helping them understand the severe consequences of viewing and distributing child pornography.

245. It is of paramount importance that we begin to address misconceptions around sexual health, and promoting a comprehensive understanding of sex education's benefits is essential for improving sexual health outcomes and reducing the incidence of sexual crimes in India. This is especially crucial given India's growing population."

(Emphasis supplied)

309. We also examined Section(s) 43 and 44 of the POCSO and held that the obligation cast upon the appropriate Government and the

Commissions for Protection of Child Rights, respectively, to give wide publicity to its provisions is not confined merely spreading awareness about the provisions of the POCSO Act. We said that the steps and efforts expected of them under the said provisions includes the obligation to impart sex education and awareness amongst children and stakeholders. The relevant observations read as under: -

> *"248. We are of the considered view that the obligation of the appropriate government and the commission under Section(s) 43 and 44 of the POCSO respectively, does not end at just spreading awareness about the provisions of the POCSO. Since, one of the salutary and avowed object of the POCSO was the deterrence of offences of child sexual abuse and exploitation, thus, as a natural corollary, the obligation of the appropriate government and the commission under the aforesaid provisions will also entail imparting of sex education and awareness amongst the general public, children as well as their parents and guardians, particularly in schools and places of education. The steps and efforts of the appropriate government and the commission towards the compliance of Section(s) 43 and 44 must go beyond just the textual wording of the said provisions and ought to earnestly take into account the pragmatic necessities for curtailing the issue of child abuse, exploitation and addiction to pornography."*
>
> (Emphasis supplied)

310. With the aforesaid in mind, we in **Just Rights** (supra) had made certain suggestions to the Union of India in its Ministry of Women and Child Development, at paragraph 260 of our judgment. The same reads as under: -

"260. We propose to suggest the following to the Union of India in its Ministry of Women and Child Development: -

xxx xxx xxx

(iii) *Implementing comprehensive sex education programs that include information about the legal and ethical ramifications of child pornography can help deter potential offenders. These programs should address common misconceptions and provide young people with a clear understanding of consent and the impact of exploitation.*

(iv) *Providing support services to the victims and rehabilitation programs for the offenders is essential. These services should include psychological counselling, therapeutic interventions, and educational support to address the underlying issues and promote healthy development. For those already involved in viewing or distributing child pornography, CBT has proven effective in addressing the cognitive distortions that fuel such behaviour. Therapy programs should focus on developing empathy, understanding the harm caused to victims, and altering problematic thought patterns.*

(v) *Raising awareness about the realities of child sexual exploitative material and its consequences through public campaigns can help reduce its prevalence. These campaigns should aim to destigmatize reporting and encourage community vigilance.*

(vi) *Identifying at-risk individuals early and implementing intervention strategies for youth with problematic sexual behaviours (PSB) involves several steps and requires a coordinated effort among various stakeholders, including educators, healthcare providers, law enforcement, and child welfare services. Educators, healthcare professionals, and law enforcement officers should be imparted training to identify signs of PSB. Awareness programs can help these professionals recognize early warning signs and understand how to respond appropriately.*

(vii) *Schools can also play a crucial role in early identification and intervention. Implementing school-*

based programs that educate students about healthy relationships, consent, and appropriate behaviour can help prevent PSB.

(viii) *To give meaningful effect to the above suggestions and work out the necessary modalities, the Union of India may consider constituting an Expert Committee tasked with devising a comprehensive program or mechanism for health and sex education, as well as raising awareness about the POCSO among children across the country from an early age, for ensuring a robust and well-informed approach to child protection, education, and sexual well-being*.

(Emphasis supplied)

311. More than two years have passed since then. We may also remind that, the same emphasis was also laid almost thirteen years back, in **Shankar Kisanrao Khade v. State of Maharashtra** reported in **(2013) 5 SCC 546**, which found favour and came to be endorsed by us in **Just Rights** (supra). We want to understand from the Union of India as to what steps it has taken in all these years to implement the aforesaid suggestions.

312. We are also of the view that awareness of digital safety and sex education are not two separate subjects, but two sides of the same coin, and must be addressed as such.

313. Children from an early age must be made aware of the persons they should meet and interact with, the ability to tell inappropriate requests, gestures and advances, the respect for their own dignity and of those around them, and most importantly where and whom to turn to when inappropriate any unpleasant incident does unfortunately occur. These are all concerns and measures crucial for the safety of their presence online inasmuch as for their lives outside.

314. We have already laid significant emphasis on the measures necessary on the part of intermediaries in making the internet safer of children. The need for awareness amongst children on digital safety and positive age-appropriate sex education is a necessary corollary of the same. The catena of safeguards that we have proposed would be of limited avail if the children for whose benefit they exist are unaware of them.

315. In view of the foregoing, we are of the considered view that the following measures must be undertaken by the Union and the State Governments, the National and State Commissions for Protection of Child Rights, educational institutions, intermediaries and all other concerned stakeholders, for ensuring the safety of our children: -

(i) Children, from the primary stage, must be taught in an age-appropriate manner about their bodies, the difference between safe and unsafe touch, and the significance of consent.

(ii) Equally important is the need to inculcate in our children an understanding of healthy relationships and respect for one another. Experience has shown that on occasions, it is children themselves who capture, upload or circulate intimate or non-consensual images of their own peers, often without realising the gravity of what they do. Thus, it is imperative that they be taught to respect the dignity of their peers, and be cautioned against all forms of inappropriate conduct.

(iii) They must also be taught the ways to use the internet safely. Measures to protect their personal data and privacy online, to recognize signs of enticement, sexual extortion, and other similar exploitative and abusive practices.

(iv) They must equally know whom they can approach in such situations, and how. This would include a trusted adult at home and in school, as well as the appropriate channels for reporting any wrongful behaviour or incident, both on and off the internet.

(v) Above all, children must be encouraged to come forward without fear and report such incidents. They must be assured that speaking up on these matters will never be met with any reproach, and they will be given all the help and support with complete confidentiality.

(vi) Children must also be made aware of the significance of the POCSO Act and the IT Act, particularly the various provisions criminalizing the viewing, possession or circulation of CSEAM, as-well as of their rights under these enactments.

(vii) Digital safety and age-appropriate sex education must form a part of the core curriculum. They must be developed by the NCERT and the SCERTs in consultation with child psychologists, educators and parenting experts. It must accommodate the diverse levels of literacy across the country through use of text-based courses, pictorial representations, illustrations and audio-visual content.

(viii) The Union of India has made considerable efforts in putting in place helplines and portals for supporting victims of such incidents and facilitating commensurate actions against the perpetrators. Self-help mechanisms such as the Child Helpline

'1098', the Cyber Crime Helpline '1930' and the National Cyber Crime Reporting Portal, along with the details of State-wise nodal officers of the same must therefore be displayed in every classroom, hostel, library and computer laboratory, as well as on the website of every school and educational institution.

(ix) Devices and networks within the premises of educational institutions and schools must be equipped with filters to prevent access to harmful content in a reasonable and proportionate manner. These measures must also extend to hostels, child care institutions, tuition and coaching centres with a greater rigour.

(x) Teachers and other school staff must be adequately trained on digital safety measures and age-appropriate positive sex education. The training must, *inter-alia,* cover the signs of grooming, abuse and online harassment; the manner of responding to any disclosure by a child; the obligation to report under Section(s) 19 and 21 of the POCSO Act; and the confidentiality to be maintained in respect of the child. The non-teaching staff of educational institutions must also be adequately sensitised to respond to such situations.

(xi) Parents and guardians are, in most cases, the first line of defence. Yet many are themselves unfamiliar with the technology their children use. Which is why, awareness programmes must be organised for them at regular intervals by all schools and educational institutions. These must, *inter-alia*, cover the risks that children face online; the parental controls and safety settings available on devices and platforms; the signs that a child may be in distress; and the correct approach in responding to the same.

(xii) Parents in particular must be sensitised on monitoring the online activity of children and on how to avert the risks of creating mistrust or miscommunication with their child from such parental supervision.

(xiii) The Union and State Governments in conjunction with the respective Commissions for Protection of Child Rights **shall** create awareness on the POCSO Act, of the various forms in which the abuse and exploitation of children may occur, particularly those through digital means such as CSEAM. Such campaigns must be sustained, and not sporadic. They must be disseminated through all forms of media such as televisions,

social media, telecommunication channels and SMSs, OTT platforms, as-well as print media and public signage.

(xiv) The Union and State Governments along with the respective Commissions for Protection of Child Rights **shall** also create awareness amongst all stakeholders of the measures for the digital safety of children and the various helplines and support portals available. They **shall** also sensitise parents, guardians, teachers and all others standing *in loco parentis* on the appropriate manner of responding to incidents of abuse and exploitation of children.

(xv) Intermediaries must also put in place periodic reminders to children on the safe use of their platforms and the safety centres, privacy settings and help options available to them. They must display cautionary prompts where any child attempts to connect, message or interact with any unknown adult and appropriate warnings where any user enters any search term or query associated with CSEAM.

(xvi) The Union and State Governments **shall** also create support mechanisms for victims such abuse or exploitation, whether online or otherwise. This includes ready access to counselling,

psychological support and therapy by trained professionals, free of cost, for as long as may be necessary. Proper follow-up mechanisms shall also be put in place to oversee the continued wellbeing of victims.

III. SUMMARY OF OUR CONCLUSION

316. We summarise our final conclusion as under: -

1. Detection and Removal of CSEAM through Hash Matching and URL Listing.

1A. The Union of India shall provide information, by way of an affidavit, on the tools and technological measures that have been put in place by intermediaries for the detection and removal of CSEAM from their platforms.

1B. Appropriate guidelines or standard operating procedure shall be framed by the Union of India for the use of perceptual hash-matching and URL listing by all significant social media intermediaries for the detection and removal of CSEAM from their platforms.

1C. The above guidelines or standard operating procedure shall further stipulate other tools and technological measures that must

be deployed by every intermediary for the detection and removal of CSEAM. In this regard, appropriate amendments shall also be made to the IT Rules, where necessary.

1D. Such guidelines or standard operating procedure shall be revised periodically by the Ministry of Electronics and Information Technology.

1E. The Union of India shall further indicate, by way of an affidavit, the feasibility of an industry-wide use and deployment of such tools by all intermediaries.

2. Creation and Use of National Hash & URL List Database.

2A. The Union of India shall create a National Hash & URL List Database for the sole purpose of the detection and removal of CSEAM. Such a database may be created as part of the Sahyog Portal or as a standalone repository.

2B. Any entry within the National Hash & URL List Database shall only be made after a thorough assessment of the material through multiple tiers of verification. Such assessment may involve preliminary screening of the material by specialised software; however, the final determination or screening shall be done by at

least three trained human analysts, who would independently determine whether the material in question constitutes CSEAM.

2C. Where any material upon such assessment is confirmed to be CSEAM, the perceptual hash identifier and/or the URL of the material would be generated and entered into the National Database.

2D. All entries within the National Hash & URL List Database shall be made through encrypted channels and strictly confined to the hash identifier and/or URL of the material confirmed to be CSEAM.

2E. Every entry within the National Hash & URL List Database shall be used by intermediaries to cross-check against and remove any content on their platform that matches the same. Law enforcement agencies shall further use the same process to identify, detect and remove any such material matched against an entry within the database across the internet.

2F. The process of detection and removal of CSEAM by cross-checking against an entry within the National Hash & URL List Database shall be done alongside and in addition to the ordinary existing process of detection and removal of CSEAM.

2G. Where an intermediary finds a match against an entry within the Hash & URL List Database i.e., CSEAM of "*Known Origin*", the intermediary shall immediately disable and remove the same, without awaiting any further verification at its end.

2H. Where, an intermediary detects and removes any CSEAM of "*Unknown Origin*", the same must be preceded by proper verification and due diligence on its part in accordance with the IT Rules. The intermediary in such a case shall also be obligated to promptly report the same to the proper authorities under the relevant law, and also to the designated body for the Hash & URL List Database, if not the same.

2I. Upon receipt of such report, the designated body for the Hash & URL List Database shall assess the flagged material in question in the manner indicated above. Where the same is confirmed to be CSEAM, the hash and/or URL identifier of the same would be entered into the database.

3. Display of Proper Notices in place of any material Removed as CSEAM.

3A. In every instance where an intermediary removes any material as CSEAM, it would be required to prominently display a notice in place of such material on its platform.

3B. The notice must, *inter-alia,* indicate whether such removal was pursuant to the intermediary's own detection, or on account of a match found against a known entry in the Hash & URL List Database.

4. Grievance Redressal against any material Removed as CSEAM.

4A. Where any material is removed as CSEAM by the intermediary's own detection, the challenge against such removal shall lie under the grievance redressal mechanism, and thereafter, if necessary, before the Grievance Appellate Committee, as provided in Rules 3(2) and 3A of the IT Rules, respectively.

4B. Where, however, any material is removed for reasons of a known match with the National Hash & URL List Database, the challenge would lie before the authority designated and entrust for maintaining the said database. In this regard, Union of India shall frame appropriate guidelines for creating a grievance redressal mechanism within the authority maintaining the National Hash & URL List Database.

5. Proper Authority for the reporting of CSEAM by Intermediaries.

5A. Where an intermediary removes or disables any content, computer resource, information or link as CSEAM in consequence of violation of Section 15 of the POCSO Act or Section 67B of the IT Act the same must be reported in accordance with Rule 11 of the POCSO Rules.

5B. The Proper Authority for this purpose would be the Special Juvenile Police Unit, the local police and/or the cyber-crime portal, as specified under Rule 11 of the POCSO Rules.

5C. Where an intermediary removes or disables any CSEAM of "*Unknown Origin*" the same must also be reported to the authority entrusted with the maintenance of the Hash & URL List Database, if not already the same.

5D. Where, however, an intermediary removes or disables any CSEAM of "*Known Origin*", upon a match being found against the Hash & URL List Database, the intermediary must furnish the details of all such removals by way of a consolidated report on a weekly basis, to the authority designated for maintaining the Hash & URL List database. The Union of India may, prescribe additional authorities to whom such reports must also be made.

6. Timelines within which CSEAM must be reported by Intermediaries.

6A. Where an intermediary removes or disables any CSEAM of "*Unknown Origin*", on the basis of a complaint or grievance received by it, the same must be reported forthwith upon the resolution of such complaint, and in any case no later than two hours after such resolution.

6B. Where an intermediary removes or disables any CSEAM of "*Unknown Origin*", on the basis of its own due diligence, the same must be reported within two hours from such removal.

6C. Where an intermediary removes or disables any CSEAM of "*Unknown Origin*", on the basis of an order of a court of competent jurisdiction or reasoned intimation from the appropriate government, the same must be reported within two hours from such removal.

6D. We reiterate, where an intermediary removes or disables any CSEAM of "*Known Origin*", upon a match being against the Hash & URL List Database, whether pursuant to a complaint, the intermediary must furnish the details of all such removals, by way of a consolidated report on a weekly basis to the authority designated for maintaining the Hash & URL List database.

7. Publication of requisite details of Grievance Officers and Grievance Redressal Mechanism.

7A. Every intermediary, in accordance with Rule 3(2)(a) of the IT Rules, must prominently display, on the home page or screen of its website or application, as the case may be, the requisite details of the grievance officer(s) as well as the mechanism through which users may raise their complaints.

7B. Every intermediary must also ensure that such information is regularly updated, so as to accurately reflect the details of its grievance redressal mechanism and the officer(s) entrusted with the same.

7C. Union of India shall furnish information, by way of an affidavit, of the extent of compliance of the above requirements by the various intermediaries, and of the action taken, if any, against intermediaries found to be in default.

8. Access to the Grievance Redressal Mechanism.

8A. The grievance redressal mechanism of every intermediary must provide a distinct and clearly labelled category for the reporting of CSEAM.

8B. The nomenclature of such category must be simple, readily understood by any person irrespective of age, literacy or familiarity with technology, and must leave no doubt as to the nature of the content being reported.

8C. Such mechanism must also be made accessible within two steps from the content, profile, group or link in question, and must be uniform across all intermediaries. The Union of India is thus requested to put in place certain guidelines for ensuring the same.

9. Working of the Grievance Redressal Mechanism and Dedicated Grievance Redressal Officers for Reports relating to CSEAM.

9A. Any content reported as CSEAM or complaint thereof must be assessed thoroughly. Such assessment must be done keeping in mind the provisions of Section(s) 15 and 67B of the POCSO and IT Act, respectively.

9B. The assessment, must involve examining the content as a whole, including the text, captions, keywords, links and the function of the tool or application being promoted, in order to determine whether the same facilitates or has the propensity to result in the exploitation or abuse of children.

9C. The grievance officer(s) persons entrusted with the review and resolution of such complaints must be adequately trained to identify CSEAM, including material which may not be explicit on its face but nevertheless carries either the likelihood of exploitation or abuse of children or is otherwise harmful to them.

9D. The intermediaries must ensure that such officer(s) receive necessary training from time to time, particularly in respect of any and all new *modus operandi* that may emanate in the circulation of CSEAM.

9E. The intermediaries must also allocate adequate resources to the grievance redressal mechanism and the officer(s) entrusted with it, for continued efficiency of the same.

9F. No report or complaint of CSEAM ought to be disposed without the same having been reviewed by a trained grievance officer. Automated tools may be used to assist the preliminary screening of such reports. However, the ultimate decision, must be taken by a trained grievance officer, entrusted with such duty.

9G. Such assessment, must record the findings of the office in the course of his assessment, and bear his digital signature, to ensure accountability.

9H. Every report or complaint relating to CSEAM, must be acknowledged within twenty-four hours from receipt, and must be accompanied by a reference number to track the status of the same. Any decision or action taken in respect of the same must be communicated to the complainant along with the reasons thereof.

9I. We are conscious that Rule 4(6) as it presently stands, requires only significant social media intermediaries to provide the means for tracking complaints, and to furnish reasons for any action or decision by it "*to the extent reasonable*".

9J. We however are of the view that this compromises the accountability required in the resolution of complaints as grave as those of CSEAM. We therefore expect the Union of India to extend the aforesaid requirements to every intermediary insofar as complaints of CSEAM are concerned by introducing suitable amendments within the IT Rules.

9K. Every intermediary must also publish a monthly compliance report detailing the number of complaints received by it, the

action taken in respect of the same, the time within which such complaints were resolved, and the content, information or link or any part thereof removed or disabled pursuant to such complaint or by its own due diligence.

9L. Complaints pertaining to CSEAM must in particular be disclosed under a separate section within the report. Such reports must be periodically subjected to independent audit by an appropriate authority designated by the Ministry of Electronics and Information Technology, so as to oversee the continued compliance of the various requirements under the IT Rules.

10.Other Significant Measures and Safeguards.

10A. Union of India shall further consider putting in place a framework for imposing exemplary monetary fines on intermediaries for the breach of any duties under the IT Act and the IT Rules.

10B. The quantum of such penalties must be determined having regard to the gravity, duration and recurrence of the default as well as the size and turnover of the intermediary.

10C. Where any CSEAM or prohibited material is found to have been hosted, uploaded, promoted or circulated, directly or indirectly, through any paywall or subscription from which the intermediary derives any revenue, the revenue so derived from such content should be forfeited and disgorged.

10D. We further put all intermediaries to strict notice that any content offered behind a paywall, or on a subscription basis, must be subjected to a rigorous scrutiny to ensure that the same does not violate the IT Act, the IT Rules or any other law for the time being in force.

10E. Every intermediary must ensure that no CSEAM, or any other material having the propensity or likelihood to harm children, is offered, hosted, uploaded, promoted or circulated through such paywall or subscription, either directly or indirectly.

10F. Intermediaries must further take all measures to ensure that any content, paywalled or otherwise, which depicts or promotes anything obscene, indecent or sexually explicit, or which is otherwise lascivious or prurient in nature, is not promoted to any children on their platforms. Every care must also be taken to

ensure that no child is able to subscribe to, or otherwise access, such content.

10G. The Union of India shall frame appropriate guidelines for ensuring the proper scrutiny of paywalled and subscription-based content by intermediaries for the detection and removal of CSEAM.

10H. The said guidelines shall also prescribe reasonable and proportionate measures to moderate the nature of content that can be accessed or subscribed to, by the children.

317. In view of the foregoing, we direct the Union of India through the Ministry of Electronics and Information Technology and the Ministry of Law and Justice to take appropriate action for overseeing and implementing the suggestions, measures and safeguards discussed in the earlier parts of this judgment.

318. For this purpose, the Union of India shall formulate appropriate guidelines, Standard Operating Procedures and suitable amendments to the IT Act and the IT Rules, where necessary.

319. The Union of India by the next date of hearing shall, by way of an affidavit, indicate the progress made in this regard and the steps taken

towards compliance of the aforesaid directions, along with any other suggestions that it may deem fit to offer.

320. Post it on 10.12.2026.

……. J.
(J.B. PARDIWALA)

……. J.
(K.V. CHANDRAN)

New Delhi.
October 15, 2026.