



WEB COPY

IN THE HIGH COURT OF JUDICATURE AT MADRAS

DATED: 09-07-2025

CORAM

THE HONOURABLE MR JUSTICE N. ANAND VENKATESH

WP No. 25017 of 2025

X

Petitioner(s)

Vs

1.The Union Of India

Rep By The Secretary to Government,
Ministry of Electronics and Information Technology
6, Lodhi Road, CGO Complex,
Pragati Vihar, Electronics Niketan,
New Delhi-110 003

2.The Director General of Police

Dr.Radhakrishnan Salai,
Mylapore, Chennai-600 004

Respondent(s)

[R2 suo motu impleaded vide Court order dated 09.07.2025, made in W.P.No.25017 of 2025]

PRAYER Writ Petition filed under Article 226 of the Constitution of India for issuance of a Writ of Mandamus, directing the respondent herein to act upon the



WEB COPY

petitioner representation dated 18.6.2025 by taking all appropriate measures, including but not limited to blocking/removing/issuing take down notices/issuing directions to all concerned intermediaries/websites/pornographic platforms/ telecommunication service providers to forthwith and on a continuing basis detect, remove, and block all content depicting the petitioners Non consensual intimate images and videos(NCII)which are being uploaded,shared re-uploaded, transmitted or distributed over the Internet and digital platforms, by employing technological solutions such as Hash Matching Technology, Artificial intelligence-based content recognition tools including Photo DNA, Google content safety Hash checkers, or any other similar tools or mechanisms, so as to ensure the effective removal of such content and to prevent its further dissemination on any Internet or digital platform at present and in the future.

For Petitioner(s): Mr.Abudu Kumar Rajaratnam
Senior Counsel
for Mr.Rajagopal Vasudevan

For Respondent(s): Mr.A.Kumaraguru
Senior Panel Counsel for R1

Mr.V.Meganathan
Government Advocate for R2

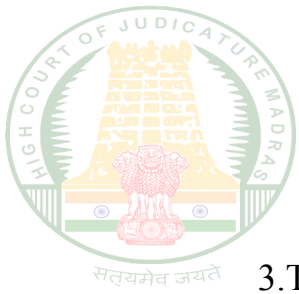


WEB COPY

ORDER

This writ petition has been filed for issue of writ of mandamus directing the 1st respondent to act upon the representation made by the petitioner dated 18.06.2025 by taking all appropriate measures of blocking / removing / issuing take down notices / issuing directions to all concerned intermediaries / websites / pornographic platforms / telecommunication service providers to forthwith and on a continuing basis detect, remove, and block all content depicting the petitioner's Non Consensual Intimate Images and Videos (NCII) which are being uploaded, shared, re-uploaded, transmitted or distributed over the Internet and digital platforms, by employing technological solutions, so as to ensure the effective removal of such content and to prevent its further dissemination on any Internet or digital platform in present and also in the future.

2.Heard the learned counsel for the petitioner and the learned counsel appearing on behalf of the respondents.



WEB COPY

3.The case in hand is a pathetic story of a young girl who was misled by a person in the guise of a love affair and he with a false promise of marrying her, subjected her to repeated sexual exploitation which was filmed without her knowledge and was transmitted across the Internet and digital platforms. The petitioner is now struggling to remove all those contents from the Internet/digital platform by making a representation before the 1st respondent to act upon the same. Since the 1st respondent is the only authority under the Information Technology Act, 2000 and Rules framed thereunder to issue directions for blocking and removal of such material.

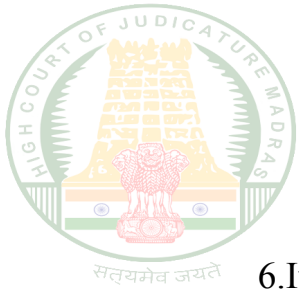
4.The petitioner is an Advocate practising before this Court and before the District Judiciary. The petitioner during her college days had a love affair with a person. This relationship became intimate, since the said person promised to marry the petitioner. The petitioner placed immense trust upon that person and due to constant promises and the emotional manipulation, the said person started sexually assaulting the petitioner repeatedly. The petitioner



WEB COPY

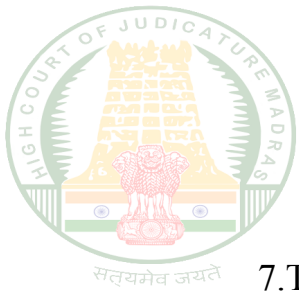
believed his words and submitted herself without being aware of the fact that the physical intimacy is being surreptitiously filmed and it is transmitted in the Internet and other digital platforms. The said person had shared the videos multiple times and which was downloaded and reloaded on various digital platforms. It is also being re-shared and displayed on pornographic websites as well as in the social media platforms.

5.The petitioner came to know about the same when one of her friend informed her and aggrieved by the same, she gave a complaint which resulted in the registration of an FIR in Crime No.21 of 2025 for various offences under IPC, BNS and Information Technology Act and also under Section 4 of the Tamil Nadu Prohibition of Harassment of Woman Act, on 01.04.2025. The person who exploited the petitioner was added as A1 in that case and the administrator of the group who had transmitted the videos with other persons was added as A2. The criminal case is pending investigation.



WEB COPY

6. It came to light that the illegally recorded video depicting the petitioner in a vulnerable state has been shared and transmitted across more than 70 websites and various other telecommunication and digital platforms. It has also been downloaded and shared via Telegram, Google Drive links and other methods. It is also circulated on multiple websites under different uniform resource locators and it is also distributed privately through personal communications. The videos are now repeatedly shared, downloaded and re-uploaded on pornographic websites, social media platforms like Twitter and in other social media sites under various accounts, channels and pages. The distribution and transmission of the video reached such an extent that the petitioner who is a practising Advocate is now subjected to questioning about the video and its contents by various individuals including clients and peers in the same profession. Thus, the petitioner is being publicly shamed and she is ostracised by persons who are getting a different impression about the petitioner. In view of the same, the petitioner has lost her normal life and her dignity has been bartered and she is in a completely helpless state.



WEB COPY

7.The petitioner in order to control the reputational damage that has been caused to her image, made a representation to the 1st respondent for exercising the power under Section 67A of the Information Technology Act and to remove the content and prevent any further dissemination in the Internet and digital platforms. Since the same was not acted up, the present writ petition has been filed before this Court.

8.In the considered view of this Court, it is the duty of a Constitutional Court to safeguard the fundamental rights that has been guaranteed to all persons and not limited to just citizens when it comes to gross violation of Article 21 of the Constitution of India. Right to privacy and right to dignity is guaranteed under Article 21 of the Constitution of India. The same is being violated every second insofar as the petitioner is concerned. Therefore, this Court has to exercise its power and ensure that the untold agony faced by the petitioner is atleast mitigated by removing those contents as early as possible and to ensure that the petitioner is able to lead a normal life atleast in future.



WEB COPY

9.The learned Senior Counsel appearing on behalf of the petitioner brought to the notice of this Court the judgement of the Delhi High Court in W.P.(Crl)No.1505 of 2021 dated 26.04.2023, which involved a similar case where the Delhi High Court after considering the earlier judgements issued various directions.

10.It is relevant to take note of Paragraph No.8 of this judgement, since the Delhi High Court has recorded the stand taken by the Union of India and for proper appreciation, the same is extracted hereunder:

8. A Short Affidavit dated 22.12.2021 was filed on behalf of Respondent No.1 in the instant matter, stating that the Ministry of Electronics and Information Technology (MEITY) is the custodian of the Information Technology Act, 2000 (hereinafter referred to as "IT Act"). The Short Affidavit delineates the objective and relevant provisions of the said Act as well as the Information Technology (Intermediary Guidelines and Digital to Media Ethics Code) Rules,



WEB COPY

2021 (hereinafter referred to as the "IT Rules"). It notes that the IT Rules not only focus on the enhanced safety of women and children, but that it also provides for statutory timelines for grievance redressal and content takedown. The Short Affidavit, thereafter, goes on to note that the prayer of the Petitioner seeking delinking/de-tagging/de-referencing/de-indexing the name of the Petitioner would adversely affect the freedom of speech and expression of other individuals having the same name as the Petitioner or a similar name. The paragraphs of the Short Affidavit stating the aforesaid are as follows:

"5. It is submitted that the Ministry of Electronics and Information Technology (hereinafter referred to as "MEITY") is the custodian of the Information Technology Act, 2000 (hereinafter referred to as "IT Act, 2000") and Rules framed thereunder

6. It is submitted that the IT Act, 2000 contains provisions under Sections 66E, 67 and 67A, under Chapter XI thereof for violation of bodily privacy, publishing or transmitting obscene material and publishing or transmitting sexually explicit material in electronic form respectively. It is further



WEB COPY

submitted that Section 67B of the IT Act 2000 provides for punishing the publishing or transmitting of material depicting children in sexually explicit act in electronic form

7 It is submitted that Section 79 of the IT Act, 2000 contains safe harbor provisions for intermediaries as defined under Section 2(1)(w) thereof. It is further submitted that the intermediaries must inter alia observe due diligence guidelines as prescribed by the Central Government to ensure exemption from liability It is further submitted that to ensure open, safe, trusted and accountable Internet, the answering Respondent has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (hereinafter "IT Rules, 2021") on 25.02.2021. It is further submitted that the Part II of the IT Rules, 2021 have been framed under Section 79 of IT Act, 2000, which relates to due diligence to be observed by an intermediary. A copy of IT Rules 2021 is annexed herewith and marked as Annexure RA-1.

8. It is submitted that the answering Respondent has recently published a Frequently Asked Questions (FAQs)



WEB COPY



communicating the intent of the IT Rules, 2021 in simple and easy to understand language for all its stakeholders. A copy of the Frequently Asked Questions is annexed herewith and marked as Annexure RA-2

9. It is submitted that as stated hereinabove, the legislative intent the IT Rules, 2021 is to ensure open, safe, trusted and accountable Internet. It is further submitted that the IT Rules, 2021 prescribe the due diligence to be followed by all intermediaries as well as the additional due diligence to be followed by significant social media intermediaries (SSMI), i.e., the intermediaries having registered user base of 50 lacs or more in India.

10 It is submitted that the IT Rules, 2021 have been framed to provide for increased user safety, i.e., the intermediaries to respond to the direct requests by the affected individuals for content takedown in specific cases of content relating to breach of bodily privacy, impersonation, morphed imagery of the concerned individual in order to address the immediate need to prevent harm and emotional distress, particularly in instances of revenge porn and other similar



WEB COPY

instances

11. It is submitted that, as stated above, the IT Rules, 2021 have a clear objective of enhancing online safety of users, particularly women and children. It is further submitted that various provisions of the IT Rules, 2021 focus on enhanced safety of women and children. It is further submitted that these include:

"1. Specific inclusion of certain requirements to be explicitly conveyed in terms and conditions [Rule 3(1)(b)]

2. Reporting by the aggrieved individual in respect of revenge porn and similar content breaching physical privacy and taking action within 24 hours for content removal [Rule 3(2)(b)].

3. Enhanced grievance redressal mechanism by intermediaries [Rule 3(2)(a)].

4. Additional provision for SSMI to appoint a Resident Grievance Officer, a Chief Compliance Officer and a nodal contact person, all to be residents in India, and a physical contact address of the significant social



WEB COPY



media intermediary to be in India [Rule 4(1) and 4(5)].

5. The Rules also have provisions that intermediary shall cooperate with Law Enforcement Agencies (LEA) to identify the first originator of information related to rape and child sexual abuse material (CSAM) imagery for prosecution [Rule 4(2)]

6. The significant social media intermediaries shall endeavor to deploy technology-based measures to identify any imagery of child sexual abuse, rape etc. whether real or simulated in accordance with the safeguards in the Rules [Rule 4(4)].

12. It is submitted that the IT Rules, 2021 provide for the following statutory timelines for grievance redressal and content takedown:

1. Grievance Redressal 24 hours for acknowledgement and 15 days for disposal [Rule 3(2)].

2. Information takedown from platform upon actual knowledge based on court order or notice from



WEB COPY



appropriate government authorised by law: 36 hours

[Rule 3(1)(d)]

3. a Providing information on lawful request: 72 hours [Rule 3(1)(j)]

4. Removal of revenge porn (sexual extortion/non-consensual porn publication/sexual act or conduct involving impersonation, etc.) and other similar content: 24 hours [Rule 3(2)(b)].

13. It is submitted that in the present Petition, the grievance(s) of the Petitioner falls under Rule 3(2)(b) of the IT Rules, 2021 and accordingly, the Petitioner has an efficacious remedy to approach the intermediary directly or through any person on her behalf including law enforcement agencies for removal of URLs containing offending content.

14. It is submitted that the Petitioner's Prayer in clause (B) seeking delinking/de-tagging/de-referencing/de-indexing the name of the Petitioner from the search engines would adversely affect on the freedom of expression and speech of other individuals having the same or similar name as that of the Petitioner.



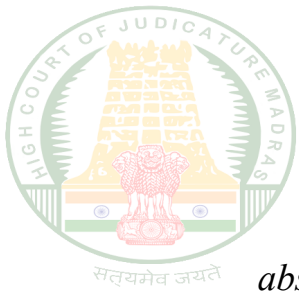
WEB COPY

15. It is submitted that the Rule 3(2)(b) of the IT Rules, 2021 empower the Petitioner to seek removal of the content by submitting the information/URLs to the intermediaries, who are obligated to remove such content within 24 hours"

11.The Delhi High Court after taking into consideration all the previous judgements and also the provisions of the Information Technology Act rendered the following findings at Paragraph Nos.59 and 60 which are extracted hereunder:

59. The fact that search engines do not host or publish or create content themselves is of no consequence when it comes to the question of removal of the access to the offending content. It is undeniable that they do have the ability, the capacity, and the legal obligation to disable access to the offending content; this responsibility of the search engine cannot be brushed under the carpet on the ground that it does not host content.

60. This Court painfully notes that there is an abysmal



WEB COPY

absence of a collaborative effort that should ideally be undertaken by the intermediaries and the State. The focus of such entities and authorities should be on the quick redressal of the complaint brought before them rather than the shirking of blame or making submissions on the onerous nature of their duties. In the process of shirking responsibility, precious time is lost in removal of the offending content and it enables the offender to keep reposting the content. It further encourages other potential offenders to undertake such dissemination of NCII content as they are aware of the lack of consequences. This in turn frustrates the legal redressal mechanism in place and the harm, both emotional and reputational, caused to the victim/user persists and perpetuates. In a conservative country like India where matters of this nature are not a part of dinner table conversations, NCII abuse does indeed lead to harrowing consequences and everlasting stigma for the victim. In light of this, the endeavour of every entity involved should be to expeditiously resolve the issue.

12. Ultimately, the Delhi High Court had issued directions and recommendations at Paragraph No.61 of the order, which is extracted hereunder:



WEB COPY

61. In view of the foregoing observations, this Court deems it fit to render the following directions and recommendations to the Respondent Intermediaries, the Ministry of Electronics and Information Technology (MEITY), as well as the Delhi Police, for ensuring that cases of the instant nature are dealt in a manner that minimises the trauma caused to the victim and resolves the problem at hand expeditiously:

i. On approaching the Court for a takedown order in a matter involving NCII content, the Petitioner must, along with the petition, file an affidavit in a sealed cover identifying the specific audio, visual images and key words that are being complained against, in addition to the allegedly offending URLs for ex facie determination of their illegality.

ii. The Grievance Officer, as defined under Rule 2(1)(k), who is appointed by the intermediary for receiving complaints of the users/victims must be appropriately sensitised. The definition of NCII abuse must be interpreted liberally by the intermediaries to include sexual content obtained without



WEB COPY



consent and in violation of an individual's privacy as well as sexual content obtained and intended for a private and confidential relationships.

iii. The "Online Cybercrime Reporting Portal", which is a central platform available on cybercrime gov in, must have a status tracker for the complainant, commencing from filing of a formal complaint to the removal of the offending content. The portal must specifically display the various redressal mechanisms that can be accessed by the victim in cases of NCII dissemination. This display should be in all languages specified in the Eighth Schedule. The cybercrime.gov.in website, along with every other website of Delhi Police, should also notably display the contact details/address of each District Cyber Police Station present in the National Capital Territory of Delhi.

iv. On the receipt of information, noting the nature of NCII content which is punishable under Section 66E of the IT Act and the distress that its continued existence may cause to the victim, the Delhi Police must immediately register a formal complaint in order to initiate an investigation and bring the



WEB COPY



perpetrators to book as soon as possible so as to prevent the repeated upload of the unlawful content.

v. Every District Cyber Police Station must have an assigned Officer who must liaise with the intermediaries against which grievances have been raised by the victim who has approached the Delhi Police and an endeavour should be made to ensure that the grievance is resolved within the time schedules stipulated under the IT Rules. The intermediaries are directed to cooperate unconditionally as well as expeditiously respond to Delhi Police, and thereafter follow the time schedules under the IT Rules.

vi. A fully-functioning helpline which is available round-the-clock should be devised for the purpose of reporting NCII content. Operators and individuals manning this helpline must be sensitised about the nature of NCII content and must, under no circumstances, indulge in victim-blaming or shaming the victim. Considering the impact that NCII content has on the mental health of its victims, these operators should also have a database of organisations with registered counsellors, psychologists and psychiatrists



WEB COPY

available for reference to the victims. The Delhi Legal Services Authority may also be apprised and engaged in case the victims need legal aid.

vii. Search engines must employ the already existing mechanism with the relevant hash-matching technology on the lines of the one developed by Meta as has been discussed above. They cannot be allowed to avoid their statutory obligations by stating that they do not have the necessary technology, which is patently false as has been exhibited during the course of hearing.

viii. The reporting mechanism under Rule 3(2)(c) of the IT Rules must be conveyed to the users by the intermediaries by way of prominent display of the same on the website of the intermediary. It is necessary for users to be made aware of the reporting mechanism and the onus for educating the users lies on the intermediaries.

ix. The timeframe as stipulated under Rule 3 of the IT Rules must be strictly followed without any exceptions, and if there is even minor deviation from the said timeframe, then the



WEB COPY

protection from liability accorded to a search engine under Section 79 of the IT Rules cannot be invoked by the search engine.

x. When a victim approaches a Court or a law enforcement agency and obtains a takedown order, a token or a digital identifier based approach must be adopted by search engines to ensure that the de-indexed content does not resurface. This means that the user/victim may be assigned a unique token upon initial takedown of NCII content. If the user/victim subsequently discovers that the same content has resurfaced, then it is the responsibility of the search engine to use the tools that already exist to ensure that access to the offending content is immediately ceased without requiring the victim to approach the Courts or other authorities again and again for removal of the same. The search engine cannot insist on requiring the specific URLs from the victim for the purpose of removing access to the content that has already been ordered to be taken down, and the victim cannot be made to face humiliation or harassment by having to approach the authorities or Courts seeking the same relief.



WEB COPY

xi. As a long-term suggestion, a trusted third-party encrypted platform may be developed by MEITY in collaboration with various search engines under Rule 3(2)(c) for registering the offending NCII content or the communication link by the user/victim. Accordingly, the intermediaries in question may assign cryptographic hashes/identifiers to the said NCII, and automatically identify and remove the same through a safe and secure process. This would reduce the burden on the victim/user to constantly have to scour the internet for NCII pertaining to them and having to request for the removal/de-indexing of individual URLs. Utmost importance should be accorded to the fact that the privacy of the user/victim must remain inviolable and the data collected for the purposes of using the hash-matching technology is not stored and misused. On account of the vulnerability of the data involved, the platform must be subject to greatest of transparency and accountability standards.

13. The Delhi High Court had taken tremendous effect in somehow trying to find a solution for this threatening problem faced by young girls across the



WEB COPY

country. This lengthy exercise that was undertaken by the Court has to be followed up by the respondent, since it is the duty of the State to safeguard the fundamental rights of its citizens. It is only the respondent who has been vested with the power, even as per their own stand taken before the Delhi High Court, to initiate action under the Information Technology Act for removal of the contents from the Internet and social media platforms.

14. In the light of the above discussion, there shall be a direction to the respondent to immediately act upon the complaint given by the petitioner on 18.06.2025 and take appropriate measures to block / remove / issue take down notices / issue directions to all concerned intermediaries / websites / pornographic platforms / telecommunication service providers to forthwith detect, remove and block all content depicting the petitioner's Non Consensual Intimate Images and Videos (NCII) which are being uploaded, shared, re-uploaded, transmitted or distributed over the Internet and digital platforms and ensure the effective removal of such content and prevent its further



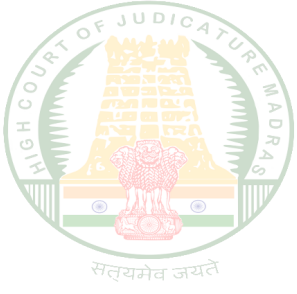
WEB COPY

dissemination on any Internet or digital platform at present or in the future. This exercise shall be completed by the 1st respondent, within a period of 48 hours.

15. Post this writ petition under the caption 'For Reporting Compliance' on 14.07.2025.

16. The learned Senior Panel Counsel appearing on behalf of the 1st respondent shall also take written instructions from the 1st respondent on the future course of action that is going to be taken by the 1st respondent based on the directions that has already been issued by the Delhi High Court. This Court is inclined to keep this writ petition pending in order to issue continuing mandamus to atleast ensure that such situations are effectively dealt with in future.

17. In order to create awareness among the police, the Director General of Police is *suo motu* added as the 2nd respondent in this writ petition.



WEB COPY

18.A copy of this order shall also be marked to the Director General of
Police.

09-07-2025

Index: Yes/No

Speaking/Non-speaking order

Internet: Yes

Neutral Citation: Yes/No

ssr

Note: Issue Order Copy on 09.07.2025



WEB COPY

To

1.The Union Of India

Rep By The Secretary to Government,
Ministry of Electronics and Information Technology
6, Lodhi Road, CGO Complex,
Pragati Vihar, Electronics Niketan,
New Delhi-110 003

2.The Director General of Police

Dr.Radhakrishnan Salai,
Mylapore, Chennai-600 004



WEB COPY

VERDICTUM.IN



27/27

WP No. 25017 of 2025

N.ANAND VENKATESH J.

SSR

WP No. 25017 of 2025

09-07-2025