$~24

* **IN THE HIGH COURT OF DELHI AT NEW DELHI**

% *Date of Judgment: 20th October, 2020*

\+ **W.P. (CRL.) 1080/2020**

MS X ..... Petitioner

Through: Mr Ashok Kumar Chhabra with Mr Dhruva Bhagat, Advocates.

versus

STATE & ORS. ..... Respondents

Through: Ms Nandita Rao ASC with Ms Gayatri Virmani, Advocates for the State/R1.
Mr Mukul Rohatgi, Senior Advocate with Mr Tejas Karia, Mr Ajit Warrier, Mr Gauhar Mirza, Mr Shijo George, Ms Hiral Gupta and Mr Dhruv Bhatnagar, for R2/Instagram.
Mr Sajan Poovayya, Senior Advocate with Ms Rakhsha Agrawal, Mr Shikhar Maniar, Ms Shruttima Ehersa and Ms Sakshi Jhalani, Advocates for R3/Google LLC.
Mr Anurag Ahluwalia, CGSC with Mr Abhigyan Siddhanth, Advocates for UOI/R5.

CORAM:
HON'BLE MR. JUSTICE VIBHU BAKHRU

VIBHU BAKHRU, J. ***(ORAL)***

1. The learned counsel for the parties were heard through video-conferencing.

2. The petitioner has filed the present petition, *inter alia*, praying that directions be issued to respondent nos. 2 to 4 to remove webpages as are mentioned in paragraph no. 15 of the petition.

3. The petitioner is a young woman. She states that in the year 2012, she was sixteen years old and was studying in a well-known School in Delhi. She came to be acquainted with a boy (hereafter 'the Accused'), who was studying in the same class. And, within a short span of time she became very close friends with him. However, he was very possessive and would not permit her to talk to anyone else. On several occasions he had snatched her phone and read all her messages. She alleges that the accused started emotionally blackmailing her and compelled her to send her intimate photographs to him. He threatened that if she didn't, he would commit suicide. She succumbed to the said tactics and started sending him her "intimate pictures". She states that the relationship with the Accused was very abusive and therefore, she broke up her relations with him.

4. After completing her schooling, she secured admission in University of Bath, United Kingdom and in August, 2014 she proceeded to the UK for further studies. She alleges that the Accused did not stop pursuing her and used to call her about 50 to 70 times a day. She used to avoid his calls but he would persist by calling her

from unknown numbers. She states that one day he landed up at her residence in Bath, U.K. and physically assaulted her. She alleges that he tried to throttle her; he placed a knife on her neck; and threatened to kill her. The petitioner was constrained to lodge a police complaint against the Accused. The matter was brought before the Magistrate Court of the Province of Bath, United Kingdom. The Accused pleaded guilty and on 04.01.2017, the Court passed an order restraining the accused from contacting the petitioner by any means including electronic, means for a period of two years, that is, till 04.01.2019. In addition, the Accused was also restrained from entering the City of Bath for a period of two years.

5. The Accused returned to India in the year 2017. The petitioner states that in the year 2019, she decided to proceed to Melbourne, Australia for higher studies. She claims that in October – November 2019, she became aware that the Accused had posted her intimate pictures on various platforms such as Twitter, Instagram, YouTube, etc. She claims that the photographs uploaded were the same that were sent by her to the Accused when she was a minor and the Accused had misused the said photographs and placed them on the internet.

6. The print-outs of the objectionable material are stated to have been filed with the present petition as Annexure B. But the said material is not on record. However, this Court is informed that the said material has been shared with the investigating agency. After becoming aware that the Accused had placed her photographs on the

net, the petitioner filed a complaint against the Accused before the Special Cell, Cyber Crime Department, Delhi Police. Pursuant to the said complaint, an FIR bearing No. 129/2019 for commission of offence punishable under Section 67–67A of the Information and Technology Act, 2000 (hereafter 'the IT Act') was registered. Thereafter, the petitioner's statement under Section 164 of the Code of Criminal Procedure, 1973 was recorded.

7. The petitioner also sent notices to respondent nos. 2 to 4 through her advocates calling upon them to immediately remove the webpages containing her objectionable photographs. She contends that despite forwarding the same, the said webpages/URLs were not removed from the platforms provided by the respondent nos. 2 to 4. The petitioner has mentioned forty such URLs (on the platform under the control of respondent no. 2 – Facebook Inc). She has also mentioned nine URLs on the platform www.youtube.com (YouTube) which is hosted by respondent no.3 – Google LLC and two webpages posted on the platform of respondent no.4 (Telegram). The petitioner's prayer made in the present petition is limited to seeking a direction to remove the said URLs (webpages) as set out in paragraph no. 15 of the petition.

8. The present petition was listed on 17.07.2020 and on that date, this Court directed respondent nos. 2 and 4 to ensure that the URLs mentioned in paragraph no. 15 of the petition are removed. This direction was issued as there was no dispute that the webpages contained objectionable photographs of a minor girl.

9. On 28.07.2020, respondent no.2 (Facebook Inc.) submitted that the directions issued on 17.07.2020 had been complied with and the offending URLs on the Instagram platform as mentioned in paragraph no. 15 of the petition had been removed. Similarly, it was reported that seven out of the nine URLs on YouTube had also been removed.

10. On 26.08.2020, it was submitted before this Court that although the URLs mentioned in paragraph no. 15 to the petition were removed but further webpages containing the offending images had been uploaded on Instagram, YouTube and other platforms.

11. It appears that the offending images had been widely distributed and the same are also being uploaded by several persons other than the Accused. This brought into the sharp focus the problem of preventing circulation of identified objectionable material on the platforms operated on the net.

12. Respondent no.2 (Facebook Inc.) has filed an affidavit, *inter alia*, affirming that it has implemented a number of measures to combat the spread of child porn (CP) including working with National Centre for Missing and Exploited Children (NCMEC) which is a non-profit organization involved in helping to find missing children, reduce child sexual exploitation and prevent child victimization. NCMEC has created Cyber Tipline, providing an online mechanism to receive reports of suspected CP content on the internet. It is affirmed that once Facebook identifies a child porn (CP) image on its platforms, it immediately removes the same. The contents of the relevant account are preserved for ninety days pursuant to the applicable law,

and the facts and circumstances associated with the same are reported to NCMEC. It is further affirmed that Facebook has also adopted a policy that prohibits any CP content on its platforms and the said policy is widely disseminated. In addition to disseminating its policies, there are other measures prevent CP content on the Facebook and Instagram Services and the same include (i) an option for anyone to report the said content, (ii) use of Photo DNA to identify any known or apparent CP image, and (iii) active identification of key words related to CP content.

13. Respondent no.3 (Google LLC) has also filed an affidavit claiming that it has adopted various protocols to deal with the child pornography or Child Sexual Abuse Materials (CP/CSAM) on its YouTube platform. As in the case of Facebook, Google also states that it has issued robust Community Standards and Policies that prohibit its users from uploading any content that endangers the emotional and physical wellbeing of minors.

14. Respondent no.3 has also affirmed that hundreds of new content are uploaded on YouTube every minute and a combination of people and machine learning is deployed at a scale for detecting, reviewing and removing content that violates its Community Guidelines. It is further affirmed that the measures adopted include (a) removal of objectionable content on individual reporting; (b) Trusted Flagger Program to provide robust tools to individuals, government agencies and non-governmental organizations (NGOs) for effectively notifying objectionable content on YouTube; (c) dedicated web-form for

government agencies; (d) round the clock review team for reported content.

15. It is stated that the Google LLC has a dedicated web form that can be used by government agencies to report content that may be unlawful, including CSAM related material, which is then expedited for review by the relevant support teams. This web form can be accessed at "http://support google.com/legal/contact/Ir_gov_india" In addition, it is stated that when action is taken in respect of a video based on YouTube policies or applicable local law, a message is put, where the content once was, to explain to viewers the reasons for removing the said video. It is stated that "video hashing" technology is also deployed to prevent re-uploads of identical copies of video content that was once removed for any violation of the Community Guidelines. It is also affirmed that Google also deploys Artificial Intelligence and Machine Learning (ML) tools to address the issue of CP on its platforms.

16. The Government of India (Ministry of Electronics and Information Technology) has also filed an affidavit referring to various legislative provisions enacted to address the issue of pornographic content on the net. Section 67B of the IT Act prescribes the punishment to be imposed for committing an offence for publishing or transmitting material depicting children in obscene, indecent or in a sexually explicit manner.

17. Mr Ahluwalia, learned counsel appearing for Government of India submitted that National Crime Records Bureau (hereafter

NCRB) acts as a nodal agency for technical and operational functions of On-Line Cyber Reporting Portal: "www.cybercrime.gov.in." The incidents reported on the portal are shared with the law enforcement agencies. NCRB has also entered into a Memorandum of Understanding (MoU) with NCMEC to receive Cyber Tipline reports relating to suspected CP content.

18. Mr Poovayya, learned senior counsel appearing for respondent no.3 (Google LLC) submitted that when any CP content hosted on its platform is reported, the same is removed immediately. However, it is difficult to prevent uploading of the same prior to the content being reported. He submitted that respondent no.3 does use artificial intelligence to prevent the uploading of CP content in respect of any known and reported image. However, the said technology has its limitations because a known hash file or a digital fingerprint is then applied for removing images with the same value. Thus, even a minor change in the properties of the image would enable it to evade discovery/action through the automated processes. Although current automated processes have their inherent limitation, there is an ongoing effort to develop more effective automated tools.

19. Mr Rohatgi, learned senior counsel appearing for respondent no. 2 advanced submissions to the similar effect.

20. There is no dispute that intermediaries would be required to take down or remove unlawful content on receiving information regarding the same. Section (79)(1) of the IT Act grants conditional immunity to the intermediaries and expressly provides that an

intermediary shall not be liable for any third party information data or communication link made available or hosted by it. However, this is subject to the provisions of Sub-sections (2) and (3) of Section 79 of the IT Act. Clause (b) of Sub-section (3) of Section 79 of the IT Act is relevant and reads as under:-

> "(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner."

21. In ***Shreya Singhal v Union Of India: (2015) 5 SCC1*** the Supreme Court read down the scope of 'actual knowledge' as used in Clause (b) of Sub-section (3) of Section 79 of the IT Act to "receiving actual knowledge from a court order or on being notified by the appropriate government or its agency". Thus, the question whether the intermediaries are required to remove offending content on an order of court or appropriate government and its agencies is no longer *res integra.*

22. It is not disputed by respondent nos.2 and 3 that on being notified about any CP content being hosted on its platform or its site, they would be obliged to remove the same. However, as noted earlier, the issue in the present case is whether respondent nos.2 and 3 are also required to ensure that such CP content is not hosted on their

platforms. In this regard, it is relevant to refer to Section 20 of the Protection of Children from Sexual Offences Act, 2012, which reads as under:-

> "20. Any personnel of the media or hotel or lodge or hospital or club or studio or photographic facilities, by whatever name called, irrespective of the number of persons employed therein, shall, on coming across any material or object which is sexually exploitive of the child (including pornographic, sexually-related or making obscene representation of a child or children) through the use of any medium, shall provide such information to the Special Juvenile Police Unit, or to the local police, as the case may be."

23. Rule 11 of the Protection of Children from Sexual Offences Rules, 2020 also makes it obligatory for intermediaries to report any CP content or any information regarding storage and dissemination of such content to Special Juvenile Police Unit or local police. The said Rule is set out below:

> "11. Reporting of pornographic material involving a child.—(1)Any person who has received any pornographic material involving a child or any information regarding such pornographic material being stored, possessed, distributed, circulated, transmitted, facilitated, propagated or displayed, or is likely to be distributed, facilitated or transmitted in any manner shall report the contents to the SJPU or local police, or as the case may be, cyber-crime portal (cybercrime.gov.in) and upon such receipt of the report, the SJPU or local police or the cyber-crime portal take necessary action as

per the directions of the Government issued from time to time.

(2) In case the "person" as mentioned in sub-rule (1) is an "intermediary" as defined in clause (w) of sub-section (1) of section 2 of the Information Technology Act,2000, such person shall in addition to reporting, as provided under sub-rule(1), also hand over the necessary material including the source from which such material may have originated to the SJPU or local police, or as the case may be, cyber-crime portal (cybercrime.gov.in) and upon such receipt of the said material, the SJPU or local police or the cyber-crime portal take necessary action as per the directions of the Government issued from time to time.

(3) The report shall include the details of the device in which such pornographic content was noticed and the suspected device from which such content was received including the platform on which the content was displayed.

(4) The Central Government and every State Government shall make all endeavors to create widespread awareness about the procedures of making such reports from time to time."

24. Ms Rao, learned ASC appearing for the State referred to the statutory framework in various countries to address the issue of child exploitation and protection of children from offences.

25. Given the statutory framework, it would be necessary for the intermediaries to take all effective measures that may be available with them to ensure that the CP content is not hosted on their platforms. The respective affidavits filed by respondent nos.2 and 3

also indicate that they are using Artificial Intelligence and other tools to remove the offending content from their platforms.

26. This Court is also informed that National Crime Report Bureau (NCRB) has also entered into a Memorandum of Understanding with NCMEC to report all offending CP content in order that the same can be removed from all other platforms as well.

27. In the circumstances, this Court directs the concerned police agencies to forward offending material relating to the petitioner, which undeniably falls within the scope of sexual explicit material relating to a child, to the NCRB. The NCRB shall also use the protocols available in terms of the Memorandum of Understanding entered into with NCMEC or otherwise to notify the offending material in order that the same can be actioned and removed from other platforms as well.

28. Respondent nos.2 and 3 are also directed to use such measures as available with them to remove, the contents which are similar to the contents of the URLs as mentioned in paragraph no. 15 of the present petition. Of course, this would be within the limitation of technology and the tools available with the said respondents.

29. This Court is also informed that during the pendency of the present petition, the following Web pages/URLs containing the offending material have cropped up on Instagram:

(i) https://instagram.com/_.cute_dhavnii._?igshid=1fl3nhc2qybra;
(ii) https://instagram.com/cute___dhavani__?igshid=10wt31gf5f676;

(iii) https://instagram.com/cute_dhavni_____?igshid=1ehct797632e;
(iv) https://instagram.com/cutie___dhvani?igshid=1kdb6w314ngym;
(v) https://instagram.com/cutie_dhavnii?igshid=1a8ksbp0qkzg9; and
(vi) https://instagram.com/cutie_._dhvani?igshid=1rmlic5z4ol5p

30. Respondent nos. 2 is directed to take effective steps for removal of the aforesaid URLs as well.

31. The police authorities shall also use the protocols and resources available with NCRB and or other concerned agencies to identify the persons who are re-uploading the offensive content in India and take such actions as warranted, in accordance with law.

32. The petition is disposed of with the aforesaid directions.

VIBHU BAKHRU, J

OCTOBER 20, 2020
pkv