IN THE HIGH COURT OF UTTARAKHAND
AT NAINITAL
WRIT PETITION (PIL) No. 158 of 2018

In Re,
"In the matter of, Incidence of Gang Rape in a Boarding School, situated in Bhauwala, District Dehradun.
.....Appellant

Vs.

State of Uttarakhand and others. .....Respondents

Mr. Arvind Vashisth, Senior Advocate (Amicus Curiae).

Mr. Paresh Tripathi, Chief Standing Counsel for the State of Uttarakhand.

Mr. Rakesh Thapliyal, Assistant Solicitor General for the Government of India.

Coram: Hon'ble Rajiv Sharma, ACJ.
Hon'ble Manoj Kumar Tiwari, J.

Dated: 27th September, 2018

Rajiv Sharma, ACJ (Oral)

This Court has taken cognizance of the three news items, which appeared in the daily edition of *Amar Ujala* (vernacular Hindi), *Hindustan Times* and *Times of India*.

2. A startling revelation has been made that a minor student was raped in the School premises by four students. The Management, instead of taking prompt action against the culprits, has tried to hush up the matter. It is with great difficulty that an FIR was registered against the four students and the School Management under Sections 376 and 201 of I.P.C. and Sections 5/6/19/21 of The Protection of Children from Sexual Offences Act, 2012 (hereinafter referred to as "POCSO"). The matter is under investigation. Since all the four students were minor, they were produced before the appropriate forum.

3. We can take judicial notice of the fact that sexual assault against the minors is increasing. The children are not safe even in educational institutions. The young children are being sexually abused, exploited and assaulted. We have also taken cognizance of an incident, in WPPIL No.156 of 2018, which happened in a School Van at Haldwani.

4. We are also told at the bar that as per the news items, these boys had seen porn movies and, thereafter, called the minor girl to the store-room, where she was sexually assaulted. Unlimited access to these pornographic sites is required to be blocked / curbed to avoid adverse influence on the impressionable mind of the children.

5. We had appointed Mr. Arvind Vashisth, learned Senior Counsel as Amicus Curiae to assist the Court. He has drawn the attention of this Court to the Information Technology Act, 2000 (hereinafter referred to as "the Act").

6. Section 2(o) of the Act defines 'Data'.

7. Section 2(w) of the Act defines 'intermediary'.

8. Section 25 of the Act provides for 'suspension of licence by the Controller'.

9. Section 67 of the Act provides for punishment for publishing or transmitting obscene material in electronic form.

10. Section 67 –A of the Act, which came into force with effect from 27th October, 2009, provides for punishment for publishing or transmitting of material containing sexually explicit act, etc, in electronic form.

11. Section 67-B of the Act provides for punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

12. Section 79 of the Act reads as under:

> "79. **Exemption from liability of intermediary in certain cases**.— (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-section (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. (2) The provisions of sub-section (1) shall apply if— (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or (b) the intermediary does not— (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf. (3) The provisions of sub-section (1) shall not apply if— (a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act; (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner."

13. The validity of Section 79(3)(b) of the Act was challenged before the Hon'ble Supreme Court. The Hon'ble Supreme Court has upheld the validity of Section 79(3)(b) of the Act, but has made the following observations in the case of Shreya Singhal vs. Union of India reported in (2015) 5 SCC 1. Their Lordships of the Hon'ble Supreme Court in Paragraph 124.3 have held as under:

> "124.3. Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material. Similarly, the Information Technology "Intermediary Guidelines" Rules, 2011 are valid subject to Rule 3 sub-rule (4) being read down in the same manner as indicated in the judgment."

14. The Central Government has also framed Rules called 'The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. There is also a provision for blocking of information, in cases of emergency as per Rule 9.

15. Rule 10 provides that in case of an order from a competent court in India for blocking of any information or part thereof generated, transmitted, received, stored or hosted in a computer resource, the Designated Officer shall, immediately on receipt of certified copy of the court order, submit it to the Secretary, Department of Information Technology and initiate action as directed by the court.

16. The Central Government has also framed Rules called 'The Information Technology (Intermediaries Guidelines) Rules, 2011'. Due diligence is required to be observed by the intermediary. Rule 3 reads as under:

> "3. **Due diligence to be observed by intermediary**— The intermediary shall observe following due diligence while discharging his duties, namely: —
>
> (1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person.
>
> (2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —
>
> a) belongs to another person and to which the user does not have any right to;
>
> b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or

gambling, or otherwise unlawful in any manner whatever;

c) harm minors in any way;

d) infringes any patent, trademark, copyright or other proprietary rights;

(e) violates any law for the time being in force;

f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

g) impersonate another person;

h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation (3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2):

provided that the following actions by an intermediary shall not amount to hosting, publishing, editing or storing of any such information as specified in sub-rule: (2) —

(a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource; (b) removal of access to any information, data or communication link by any intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;

(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and

associated records for at least ninety days for investigation purposes.

(5) The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage lights of the users to the computer resource of Intermediary and remove noncompliant information.

(6) The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

(7) When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.

(8) The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal Information) Rules, 2011.

(9) The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.

(10) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to "perform thereby circumventing any law for the time being in force: provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.

(11) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule

> 3 can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

17. Rule 3(2)(b) provides that due diligence shall be observed by intermediary to avoid grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling contents.

18. Rule 3(2) (c) protects the minors from harm by intermediary.

19. The Ministry of Communication & IT, Department of Telecommunications, Government of India has issued the Notification on 31.07.2015. It was circulated to all the Internet Service License Holders, as per the list contained therein. The Department of Electronics & Information Technology (DELTy) has requested Department of Telecommunications to notify Intermediary for disablement of the URLs under the provision of Section 79(3)(b) of the Information Technology Act, 2000, as the contents posted on these websites infringed morality, decency.

20. Though the directions were issued to all the Internet Service License Holders, but till date, all the Intermediaries have not followed the same in letter and spirit. The sites are readily available to the children to view obscene and indecent acts, including pornography. It was expected from all the Internet Service License Holders that they would block these sites to protect the children of impressionable age. The psyche of the children of impressionable age is also affected, which, at

times, results in commission of crimes. The entire society, including parents, teachers, and school management is responsible to safeguard the interest of the children.

21. Accordingly, we issue the following mandatory directions:

i) There shall be a direction to all the Internet Service License Holders to punctually obey the Notification dated 31st July, 2015 and to block the publication or transmission of obscene material in any electronic form, transmitting of material containing sexually explicit act or conduct and also publishing or transmitting of material depicting children in sexually explicit act or conduct forthwith.

ii) Respondent no.4 is directed to suspend the licenses of the Internet Service License Holders under Section 25 of the Information Technology Act, 2000, if the Notification dated 31st July, 2015 is not complied with.

iii) Respondent no. 4 is directed to ensure due compliance of the orders.

iv) Respondent State is directed to ensure completion of the inquiry and investigation within a period of eight weeks from today and, thereafter, to put up the *Challan* in accordance with law in FIR No.390 of 2018, registered at P.S. Sahaspur, District Dehradun.

22. Counter affidavit(s) be filed on or before the next date of hearing.

23. List this matter on 11th October, 2018.

(Manoj Kumar Tiwari, J.) (Rajiv Sharma, ACJ.)

27.09.2018

Rathour