GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2820
TO BE ANSWERED ON: 17.12.2025

STEPS TO CHECK ONLINE PORNOGRAPHY

†2820. SHRI HANUMAN BENIWAL:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) whether the Government has taken strict steps to check online pornography which is linked to the increasing violence and exploitation against women and minors;
(b) if so, the details of the steps and action taken by the Government in this regard during the last five years;
(c) whether the Government intend to take concrete measures to prevent children from accessing harmful online pornography content including social media apps;
(d) if so, the details thereof and the time by which the measures are likely to be taken and if not, the reasons therefor;
(e) whether the Government proposes to review and fix accountability against posts etc. made through websites, apps etc. which show pornography in the country; and
(f) if so, the details thereof along with the time by which it is likely to be done?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (f): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users, including women and children.

The Government is committed to ensure that the Internet in India is free from any form of unlawful content or information, particularly which may lead to violence against women and exploitation of minors.

Legal frameworks to counter unlawful content on digital platforms

Information Technology (IT) Act, 2000

The IT Act and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021), together, have put in place a stringent framework to deal with unlawful and harmful content in the digital space.

It imposes clear obligations on intermediaries to ensure accountability.

The IT Act provides punishment for various cyber offences such as identity theft (section 66C), impersonation (section 66D), privacy violations (section 66E), publishing or transmitting obscene or sexually explicit content (sections 67, 67A, 67B).

It also empowers Police to investigate offences (section 78), enter public place and search and arrest suspected person (section 80).

IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The IT Rules, 2021 cast due-diligence obligations on intermediaries, including social media intermediaries, and require them to implement these obligations effectively so as to prevent the hosting or transmission of unlawful content.

Key provisions under IT Rules, 2021:

Provision	**Details**
Restricted information under Rule 3(1)(b)	Restricts hosting, storing, transmitting, displaying or publishing information/content that, among other things, is: • obscene, pornographic, invasive of another's privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, or promoting hate or violence; • harmful to child; • deceives or misleads, including through deepfakes; • impersonates others, including via Artificial Intelligence; • threatens national security or public order; • violates any applicable law.
User Awareness Obligations	Intermediaries must clearly inform users through terms of service and user agreements about the consequences of sharing unlawful content, including content removal, account suspension, or termination.
Accountability in Content Removal	Intermediaries must act expeditiously to remove unlawful content upon court orders, reasoned intimation from Government, or user grievances, within prescribed timelines.
Grievance Redressal	• Intermediaries to appoint Grievance Officers • Mandates to resolve complaints through removal of unlawful content within 72 hours. • Content violating privacy, impersonating individuals, or showing nudity must be removed within 24 hours against any such complaint.

Grievance Appellate Committees (GACs) Mechanism	Users can appeal online at www.gac.gov.in if their complaints are not addressed by the intermediaries' Grievance Officers. GACs ensure accountability and transparency of content moderation decisions.
Assistance by Intermediaries to Government Agencies	Intermediaries must provide information under their control or assistance to authorised Government agencies for identity verification, or for the prevention, detection, investigation, or prosecution of offences, including cyber security incidents.
Additional Obligations of significant social media intermediaries (SSMIs) (i.e., social media intermediaries having 50 lakhs or above registered user base in India)	• SSMIs offering messaging services must help law enforcement trace originators of serious or sensitive content. • SSMIs to use automated tools to detect and limit spread of unlawful content.

In case of failure of the intermediaries to observe the legal obligations as provided in the IT Rules, 2021, they lose their exemption from third party information provided under section 79 of the IT Act. They are liable for consequential action or prosecution as provided under any extant law.

Digital Personal Data Protection (DPDP) Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) and Rules 2025 provides a legal framework for safeguarding children's privacy online.

It mandates parental consent for processing children's personal data and prohibits practices detrimental to their well-being such as tracking, behavioural monitoring or targeted advertising towards children.

It also prohibits processing of personal data which is detrimental to the well-being of children or involves tracking, behavioural monitoring or targeted advertising.

Bharatiya Nyaya Sanhita (BNS), 2023

The BNS, 2023 addresses the offences involving online harm, obscenity, misinformation and other cyber-enabled crimes, including those committed through social media platforms against women and children.

- Provides punishment for offences like obscene acts and songs (Section 296), sale of obscene material including display of any such content in electronic form (Section 294)
- Section 353 aims to curb the spread of misinformation and disinformation by penalizing the act of making false or misleading statements, rumours, or reports that can cause public mischief or fear.

Protection of Children from Sexual Offences (POCSO) Act, 2012

The POCSO act defines a child as any person below the age of 18 years and provides for provisions to safeguard children against sexual abuse and sexual harassment.

- Section 13 criminalises the use of a child in any form of media—whether electronic, printed, or broadcast—for the purpose of sexual gratification.
- Section 14 prescribes punishment of imprisonment for not less than five years and a fine for the first offence. For subsequent convictions, the punishment increases to imprisonment for not less than seven years and a fine.
- Section 15 lays out a graded punishment system for possessing, storing, or failing to report pornographic material involving children

Cinematograph Act, 1952

The Cinematograph Act, 1952 and the Cinematograph (Certification) Rules, 1983, Central Board of Film Certification, regulates the public exhibition of films including adult films.

According to the guidelines issued by CBFC, films which are considered unsuitable for exhibition to non-adults shall be certified for exhibition to adult audiences only.

Additional measures to strengthen the national response to cybercrimes:

To further strengthen the mechanism to deal with such cybercrimes in a coordinated manner, the Government has also taken several other measures, including the following:

- Ministry of Home Affairs (MHA) operates the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) to enable citizens to report all cybercrimes, with special focus on crimes against children
- Indian Cyber Crime Coordination Centre (I4C) has been established to ensure coordinated and comprehensive action against cybercrime, including child sexual exploitation
- Financial assistance is provided to States/UTs under the Cyber Crime Prevention against Women and Children Scheme for capacity building, including cyber forensic laboratories and training of police, prosecutors and judicial officers
- Government periodically blocks websites containing Child Sexual Abuse Material (CSAM) based on inputs from Interpol, routed through the Central Bureau of Investigation (CBI)
- Internet Service Providers have been directed to dynamically block CSAM websites using global databases such as the Internet Watch Foundation (UK) and Project Arachnid (Canada)
- ISPs have also been advised to promote parental control filters and block access to identified CSAM websites, including through international gateways
- Public awareness on cyber safety is promoted through initiatives such as @CyberDost, radio campaigns, and publication of handbooks for students and adolescents
- MoU between NCRB (MHA) and the National Center for Missing and Exploited Children (NCMEC), USA enables sharing of tipline reports on online child sexual exploitation, which are disseminated to States/UTs through the national portal for prompt action

*****