4

PARLIAMENT OF INDIA
LOK SABHA

COMMITTEE ON THE EMPOWERMENT OF WOMEN
(2025-2026)

(EIGHTEENTH LOK SABHA)

FOURTH REPORT

MINISTRY OF HOME AFFAIRS

AND

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

'CYBER CRIMES AND CYBER SAFETY OF WOMEN'

LOK SABHA SECRETARIAT
NEW DELHI

March, 2026/Chaitra, 1948 (Saka)

FOURTH REPORT

COMMITTEE ON THE EMPOWERMENT OF WOMEN
(2025-2026)

(EIGHTEENTH LOK SABHA)

'CYBER CRIMES AND CYBER SAFETY OF WOMEN'

Presented to Lok Sabha on 23.03.2026
Presented to Rajya Sabha on 23.03.2026

LOK SABHA SECRETARIAT
NEW DELHI

March, 2026/Chaitra, 1948 (Saka)

E.W.C. No. ---

PRICE: Rs._____

Published under Rule 382 of the Rules of Procedure and Conduct of Business in Lok Sabha (Fifteenth Edition) and printed by M/s Akashdeep Printers, 20, Ansari Road, Daryaganj, New Delhi – 110002.

CONTENTS

	PAGE NO.
Composition of the Committee on the Empowerment of Women (2025-2026)	v
Introduction	vi

REPORT

PART- I

NARRATION ANALYSIS

1.	**Introductory**	1-2
2.	**Expanding Public Awareness & Community Outreach**	3-13
3.	**Strengthening Investigation, Forensics & Law Enforcement Capacity**	13-23
4.	**SOP for investigation**	23-26
5.	**Leveraging Technological Advancements to enhance Cyber Security Frameworks**	26-29
6.	**Budget Allocation for Research & Development**	29-31
7.	**Role of Social Media Intermediaries in Ensuring Online Safety for Women**	31-52
8.	**Inter-Ministerial and Inter-State Coordination**	53-54
9.	**International Issues & Cooperation**	54-56
10.	**Counselling and Rehabilitation of Cyber Victims**	56-57
11.	**Need for Comprehensive Cybercrime Law**	57-67

PART II

Observation/Recommendations of the Committee	68-90

ANNEXURES

I.	Offences under the IT Act along with their penal actions	91-97
II.	Statistics observed on various Apps and Social Networking Sites	98-102

APPENDICES

I	Minutes of the 4th sitting of the Committee (2025-26) held on 9th June, 2025	103-106
II	Minutes of the 5th sitting of the Committee (2025-26) held on 9th June, 2025	107-109
III	Minutes of the 9th sitting of the Committee (2025-26) held on 22nd July, 2025	110-113
IV	Minutes of the 11th sitting of the Committee (2025-26) held on 19th August, 2025	114-116
V	Minutes of the 21st sitting of the Committee (2025-26) held on 17th March, 2026	117-118

COMPOSITION OF COMMITTEE ON THE EMPOWERMENT OF WOMEN (2025-26)

Lok Sabha

1. Dr. D. Purandeswari - **Chairperson**
2. Smt. Lovely Anand
3. Smt. D.K. Aruna
4. Smt. Harsimrat Kaur Badal
5. Smt. Shobhanaben Mahendrasinh Baraiya
6. Ms. Iqra Choudhary
7. Smt. Kriti Devi Debbarman
8. Km. Priyanka Satish Jarkiholi
9. Dr. Kadiyam Kavya
10. Smt. Jyotsna Charandas Mahant
11. Smt. Hema Malini
12. Smt. Mahima Kumari Mewar
13. Smt. Delkar Kalaben Mohanbhai
14. Km. Sudha R.
15. Smt. Satabdi Roy
16. Smt. Himadri Singh
17. Dr. Rani Srikumar
18. Smt. Smita Uday Wagh
19. Vacant
20. Vacant

Rajya Sabha

21. Dr. Sangeeta Balwant
22. Smt. Sagarika Ghose
23. Ms. Swati Maliwal
24. Smt. Mamata Mohanta
25. Smt. Sudha Murty
26. Smt. Maya Naroliya
27. Smt. Rajani Ashokrao Patil
28. Smt. Sunetra Ajit Pawar
29. Smt. Sadhna Singh
30. Dr. Kanimozhi NVN Somu

Secretariat

1. Smt. Jyochnamayi Sinha - Joint Secretary
2. Shri Sreekanth S. - Deputy Secretary
3. Shri Yogesh Verma - Committee Officer

INTRODUCTION

I, the Chairperson of the Committee on the Empowerment of Women having been authorized by the Committee to submit the Report on their behalf, present this **Fourth** Report of the Committee on the Empowerment of Women (2025-26) on the subject '**Cyber Crimes and Cyber Safety of Women'**

2. The Report is based on the inputs received from the Ministry of Home Affairs, Ministry of Electronics & Information Technology (MeitY), Cyber Peace Foundation, an NGO, Cyber Experts from CDAC and Social Media Intermediaries (Google & Meta) at the sittings held on 9th June, 2025, 22nd July, 2025 and 19th August, 2025.

3. The Committee also wish to express their gratitude to the representatives of Ministries Experts, and NGO for appearing before the Committee to tender evidence and furnishing the information desired by the Committee in connection with the issues relating to the subject.

4. The Report was considered and adopted by the Committee at the sitting of the Committee held on 17th March, 2026.

5. The Committee place on record their appreciation for the assistance rendered to them by officials of the Lok Sabha Secretariat attached to the Committee.

6. For facility of reference and convenience, the Observations and Recommendations of the Committee have been printed in bold letters in Part II of the Report.

New Delhi
17 March, 2026
26 Phalguna, 1947 (saka)

DR. D. PURANDESWARI
Chairperson
Committee on the Empowerment of Women

REPORT

PART I

NARRATION

1. Introductory

1.1. India's rapid digital transformation has greatly expanded access to technology but has simultaneously triggered a sharp rise in cybercrimes targeting women and children. Increased internet penetration, widespread smartphone use, and reliance on digital platforms have made cyberspace more vulnerable to misuse. Crimes such as cyberstalking, online harassment, sextortion, identity theft, non-consensual intimate imagery (NCII), child sexual exploitation material (CSEAM), and cyberbullying have grown at an alarming pace. The emergence of Generative AI has further intensified risks, enabling the creation of deepfake pornography and synthetic explicit content that severely compromise the dignity of women and minors while complicating detection, classification, and takedown processes. These developments highlight the urgent need for stronger legal, technological, and institutional safeguards.

1.2. The borderless, anonymous, and interconnected nature of cyberspace, coupled with technologies like AI, IoT, machine learning, and 5G, has increased the number of entry points for cyberattacks. Although the government has implemented policies such as the National Cyber Security Policy (2013), updated 2023 information security guidelines, the IT Act, and 24x7 CERT-In monitoring, cyber offences continue to rise. NCRB data from 2017–2022 shows cybercrimes against women increasing by nearly 239 percent, while cases involving children grew twentyfold. A significant rise during the COVID-19 pandemic reflected higher digital dependence. NCRP data further indicates more than 2.48 lakh complaints related to women and children between 2019 and April 2025, suggesting serious underreporting and the need for comprehensive interventions including legal reform, digital safety tools, parental controls, platform responsibility, and victim-friendly systems.

1.3. Cyber offences also have deep economic, psychological, and social impacts. Victims face extortion and blackmail, often through anonymous payment channels that hinder investigations. Emotional consequences include trauma, fear, anxiety, and stigma, especially in conservative settings where reputational harm can severely affect education, employment, and social relationships. Many victims avoid reporting crimes due to shame or fear of retaliation, strengthening offenders' impunity and weakening the cyber safety environment.

1.4. The complexity of cybercrimes is further driven by the use of encrypted apps, VPNs, cloud hosting, virtual numbers, spoofed identities, and fake SIMs. Offenders often operate anonymously, sometimes internationally, using dark web networks and untraceable technologies. Generative AI has made impersonation and sextortion more scalable. Low awareness of cyber laws, social stigma, and limited digital hygiene—especially among minors—make women and children particularly vulnerable.

1.5. India's legal and enforcement framework includes the IT Act, POCSO Act, and provisions of the Bhartiya Nyaya Sanhita, supported by mechanisms such as NCRP, I4C, SAHYOG, cyber forensic labs, and NCMEC alerts. Coordination across Ministries, police, and digital platforms is supported by systems like SAMANVAYA and victim-support services such as One Stop Centres. Awareness efforts include Cyber Jaagrookta Diwas, digital literacy campaigns, and tools like Cyber Swachhta Kendra and m-KAVACH.Despite progress, challenges remain, including delays in cooperation from global platforms, lack of fast-track mutual assistance frameworks, uneven cyber investigation capacity, and jurisdictional confusion. Enhancing automated jurisdiction mapping, strengthening forensic infrastructure, expanding specialized training, and enabling real-time inter-state data sharing are crucial. Ultimately, safeguarding women and children requires sustained technological investment, stronger platform accountability, international collaboration, and an empathetic victim-focused ecosystem.

2. Expanding Public Awareness & Community Outreach

2.1 Spread of public awareness is very important in preventing the occurrences of cybercrime especially against vulnerable sections of women and children. I4C has undertaken following public awareness measures in this regard:

Caller Tune Campaign: I4C is collaboration with the Department of Telecommunications (DoT) has launched a caller tune campaign with effect from 19.12.2024 for raising awareness about cybercrime and promoting the Cybercrime Helpline Number 1930 & NCRP portal. The caller tunes are also being broadcast in regional languages and being delivered 7-8 times a day by Telecom Service Providers (TSPs),

SMS Campaigns The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs (MHA), has been sending targeted Text and Voice SMS alerts to citizens across India (based on the Modus Operandi prevalent in the particular area) to warn them about various cyber fraud schemes and the tactics used by fraudsters. I4C, MHA in collaboration with OLA started on 30 January 2025, adding cybercrime awareness messages to every SMS sent by OLA to passengers

Newspaper Ads: I4C has undertaken publicity campaigns through newspaper ads on Digital Arrest, Investment Scams, Part Time Job, Cyber Slavery, Sextortion across the country. More than 13 News Papers Ads in Hindi and all regional languages in full page, half page, quarter page & skybus sizes has been published under this campaign.

Advertisements in Cinema Halls: Awareness videos has been played in Hindi and 10 regional languages across 1000 cinema halls across the country for 3 months. One PSA film featuring Bollywood Icon Sh Amitabh Bachchan regarding 'Awareness against Cybercrime' was screened in the cinema theatres of the country in the month of Feb-March 2025 with the help of Ministry of Information & Broadcasting.

TV Campaigns: News channels like India Today News and AajTak ran a special News bulletin on Digital Arrest on 28/10/2024. 72 TV channels, Hindi as well as regional, ran the awareness short videos in Hindi and 10 regional languages during December 2024 to February 2025. (9 spots daily).

Radio Campaigns A special programme was organized by Aakashvani, New Delhi on Digital Arrest on 28.10.2024. Radio Spots on Radio City 91.1 FM and 92.7 FM for a week from 28th March to 03rd April, 2024 went on air where RJs talked about Cyber Hygiene. Radio Spots on Radio Mirchi 98.3 FM for a week from 10th April to 16th April, 2024 went

on Air where RJ Sid talked about Cyber Hygiene. **Mann Ki Baat:** Hon'ble PM has spoken about Digital Arrest and educated the citizens of India during "Mann Ki Baat" episode on 27/10/2024.

Celebrity Endorsements: Bollywood Icon Sh. Amitabh Bachchan agreed to be a part of I4C publicity campaign on pro-bono basis for generating awareness against cybercrime. ShBachchan has featured in 4 videos of I4C made on 3 most prominent modus operandi of cybercrime, namely, Digital Arrest, Cyber Slavery and Investment Scam. The fourth video is a direct message to the citizens by Mr Bachchan promoting 1930, National Cybercrime Reporting Portal and Cyberdost social media handle of I4C, MHA. He also used his own widely popular social media handle to promote the cyber awareness videos of I4C. Apart from celebrity endorsements, I4C has also engaged social media influencers to spread awareness on cybercrime.

School Campaigns- I4C, MHA in collaboration with CBSE organized awareness campaigns on cybercrime through VC thereby educating more than 25,000 thousand teachers and students. I4C, Hygiene MHA imparted Cyber training to more than 2 lakh NCC, NSS & NYKS Students across the country. A 1930 Cyber Walkathon was organized by I4C in collaboration with Mount Olympus School in Sector 79, Gurugram, Haryana on 22.12. 2024. More than 1500 persons, including students, parents, and police officers, participated in this event.

Raahgiri Campaign: I4C participated in Raahgiri Function at F-Block Inner Circle, Connaught Place New Delhi on 27.10.2024 (7-10 am) and educated the citizens on various modus operandi of cybercriminals.

Campaign at IITF: Fair For creating mass awareness among citizens about cybercrime and Investment Scam, I4C, MHA established a stall at ITPO, Bharat Mandapam, New Delhi during the recently concluded India International Trade Fair w.e.f. 14- 27 Nov, 2024.

Delhi Metro Campaign: A 03 months announcement campaign was organised in Delhi Metro trains on Digital Arrest and other modus operandi used by cyber criminals to commit crime.

IRCTC website: The Indian Cyber Crime Coordination Centre (I4C) utilizes IRCTC's website to promote the Cyber Crime Helpline Number (1930) and the National Cyber Crime Reporting Portal (NCRP) at www.cybercrime.gov.in aiming to educate citizens about cyber safety and reporting mechanisms.

IPL Campaign: Publicity of Helpline Number 1930 and the National Cyber Crime Reporting Portal, along with awareness videos, was displayed during IPL 2025 at all the stadiums.

Digital Displays: Digital displays at 5 Airports and 171 railway stations across the country were installed for a month to spread awareness on cybercrime.

Engagement of Civil Society: The I4C, MHA collaborated with 6 Resident Welfare Associations (RWAs) across major cities (Delhi, Mumbai, Kolkata, Chennai, Bangalore, and Hyderabad), identifying 90 societies in these six metropolitan areas. Through this partnership, awareness among senior citizens, women, and other residents living in these societies about cyber hygiene has been spread.

Campaign during Kumbh Mela 2025: The I4C, MHA in collaboration with UP Government, CAPFs and other organisations undertook programs to create awareness about cybercrime, Cyber Crime Helpline Number 1930 and National Cyber Crime Reporting portal through Digital Displays, Hoardings, and Standees during the recently concluded MahaKumbhMela 2025 at Prayagraj.

Campaign during Suraj Kund Mela 2025: The I4C, MHA in collaboration with Haryana Police undertook programs to create awareness about cybercrime, CyberCrime Helpline Number 1930 and National Cyber Crime Reporting portal through Digital Displays, Hoardings, and Standees during the recently concluded during the Suraj Kund Mela 2025 at Faridabad Haryana.

Marathon 2025 I4C, MHA in collaboration with SBI organized Green Marathon 2025 on March 9, 2025 at the Central Secretariat Sports Ground in New Delhi. I4C, MHA set up a Cyber Help Desk and displayed awareness standees on cybercrime at various locations along the marathon route. I4C, MHA in collaboration with PNB organized Half Marathon named as Cyber Run 2025 on April 10, 2025 at the Jawaharlal Nehru Stadium in New Delhi.

Cyberdost Social Media Handle I4C also runs a popular social media handle Cyberdost available on 9 different platforms, where awareness videos based on latest modus operandi of cyber criminals along with information about 1930 and NCRP are posted on regular basis. Presently the handles have more than 17 lakh followers across the 9 platforms.

Daily Digest: Daily Digest carries a compilation of all news reports on cybercrime published in prominent newspapers. I4C, MHA has shared 610 Daily Digests shared from 2022 to April 2025 with concerned stakeholders and general public through National Cyber Crime Reporting Portal (NCRP) website https://cybercrime.gov.in/Webform/dailyDigest.aspx for generating awareness on the issues related to cybercrime.

Cyber JaagrooktaDiwas: States/UTs have been requested by MHA to organize 'Cyber JaagrooktaDiwas' on first Wednesday of every month on cyber hygiene and launch mass awareness in vernacular languages for all schools, colleges, Universities, Panchayati Raj Institutions and Municipalities by involving District Magistrates, Police authorities, Officers of Education Department, PRIs etc.

2.2 The Ministry of Electronics and Information Technology (MeitY) is implementing the 'Information Security Education and Awareness (ISEA) Project' for generating human resources in Information Security and creating general awareness on various aspects of cyber hygiene and cyber security among the masses. Details of various activities carried out under the said project are as under:

As a part of Awareness activities, so far 4240 awareness workshops on Information Security have been organized through direct/virtual mode across the country for school & colleges students, teachers, faculty, Government personnel, LEAs, general users, parents, women, CSCs, etc. covering 9.43 Lakhs participants. Out of these workshops, 48 awareness workshops on Information Security have been organized exclusively for women candidates covering 5,881 participants. In addition, 1,30,215 school teachers have been trained as master trainers in 57 training programs. Besides this, around 15 crores estimated beneficiaries have been covered through various activities in indirect mode.

In addition, awareness handbooks namely Information Security Awareness Handbook for Women, Cyber Margadarshak, Cyber Security Tips for Women, OnlineSafety Tips for Women at home, Women Rights against Cyber-crime and multilingual awareness material in the form of posters, brochures, short videos, etc. on cyber hygiene and cyber security aspects have been published and made available for download through www.isea.gov.in and https://staysafeonline.in/ and Emerging Cyber

Threats Against Women and Girls are available at https://www.staysafeonline.in/concept/emerging-cyber-threats-against-women-and-girls.

CERT-In conducts training/workshops on “cyber threats and countermeasures” especially for women for creating cyber security awareness. During the year 2024, a total of 1659 women officials were trained from Government Ministries/Departments.

To educate women users on Cyber security best practices, CERT-In released the "Cyber Security Handbook for Mahila Suraksha" on the occasion of International Women’s Day 2025. To ensure wider dissemination and outreach of the awareness booklet, the booklet was shared through websites of CERT-In, social media handles of CERT-In, MyGov and TransformingIndia. On International Women's Day 2025, around 1600 women officials from 30 States and Union Territories took part in the CERT-In's "Cybersecurity Awareness Sessions for Women Officials."

2.3 **Initiatives byDigital India Corporation(DIC)**

National Commission for Women (NCW) is carrying out following initiatives:

NCW 24*7 Women Helpline 14490 aims to provide a Digital Complaint Registration System for women affected by violence through referral (Linking with appropriate authority such as police, One Stop Centre, hospital) and providing information about women related government programmes across the country. This Women Helpline is being operated from the premises of the National Commission for Women, New Delhi. This is operational from July 2021.

Its main objectives are to provide Digital Complaint Registration System for women in distress through trained counsellors, to facilitate psychological counselling or referral to the appropriate agencies such as Police, Hospitals, District Legal Service Authority (DLSA), Protection Officer (PO) and One Stop Crisis Centre (OSC) and to provide information about the appropriate support services, government agencies, etc.

Digital India Corporation(DIC) has designed, developed and is maintaining this application (https://ncwwomenhelpline.ncw.gov.in/). The calling system is integrated with IVRS (Interactive Voice Response System) in this application. The portal has a list of police

centres, counsellors, lawyers, across India, who are used by call centre professionals to connect and forward or schedule the call.

NCW Women Safety Audit Platform is also made operational. The objective of the audit is to assess the level of safety experienced by women in public spaces and workspaces in the city based on a survey & focused group discussion (FGDs). Based on information gathered during the survey, the commission shall prepare a Women's security score card for the city. City Safety Score card has been generated for the tier-II 20 cities. Now this application is used for various Research Survey conducted by the Commission and renamed as NCW Research App.

NCW Her Legal Guide (Wen enabled and Mobile App) is also made operational. The App focuses on various rights and statutes pertaining to women in India. The App envisages to legally empower women with just a click. This mobile app can act as a new friend for women in difficult situations and will make them aware about their rights. It also contains details about the helplines pertaining to women. The Mobile Application is available both in English and Hindi. It was launched by Hon'ble Justice Dr. D.Y. Chandrachud on the occasion of Legal Services Day, 2023.

2.4. Further, regarding a large gap in reporting, despite the availability of the National Cyber Crime Reporting Portal (NCRP) and awareness campaigns MHA informed as under:-

"The NCRP has made reporting easy for victims of cybercrime. An Online Citizen Survey has been conducted by I4C to assess the effectiveness of the National Cybercrime Helpline 1930 and National Cyber Crime Reporting portal (NCRP) in capturing cybercrime incidents and to understand the level of public awareness about these mechanisms to report cybercrime. As per survey report, 83.42% of citizens (out of a total of 3849 responses) have heard about the National Cybercrime Reporting Portal (NCRP) and 76.10% of citizens were aware about the 1930 Cybercrime Helpline. The findings of this survey reveal a considerable success in spreading public awareness as a result of measures taken by I4C. **Going ahead, new measures will be taken to further make it easy to report such offences and attempts.**

2.5. In response to a question “With a vast majority of India’s population residing in rural areas. In villages, it is always a social concern to come out and tell their problems. What are the Ministry’s strategic plans to tailor cybercrime awareness campaigns specifically for rural women, schoolgirls, and digital naïve populations through local dialects and community platforms?” MHA furnished the following written reply :-

The Ministry of Home Affairs (MHA), through the Indian Cyber Crime Coordination Centre (I4C), is developing strategic outreach plans to ensure cybercrime awareness reaches rural and vulnerable populations, especially women, schoolgirls, and digitally naïve users. Recognizing the hesitation and social barriers in rural areas when it comes to reporting cybercrimes, the Ministry is promoting localized awareness campaigns using regional languages and local dialects. These efforts include community-based sessions, school campaigns, radio programs, folk performances, posters, and street plays in collaboration with local governance institutions, schools, and civil society organizations. NCC and NSS which have national reach, have been roped in by the MHA for educating the cadets and the volunteers about cyber safety. Sessions with NCERT and CBSE teachers are being conducted regularly to sensitise them about cybercrime especially those targeting women and children.

2.6. In regard to the possibility of launching a structured, nationwide **‘Cyber Safety Week’,** similar to ‘Road Safety Week’, involving Panchayati Raj Institutions, Self Help Groups, ASHA/Anganwadi workers, and school authorities to raise awareness about common cyber threats targeting women and children, MHA furnished the following reply:-

Cyber Jaagrookta Diwas: States/UTs have been requested by MHA to organize ‘Cyber Jaagrookta Diwas’ on first Wednesday of every month on cyber hygiene and launch mass awareness in vernacular languages for all schools, colleges, Universities, Panchayati Raj Institutions and Municipalities by involving District Magistrates, Police authorities, Officers of Education Department, PRIs etc. **Going ahead, it would be very useful to conduct such Cyber Safety Weeks.**

2.7. In a response to the question “How does the Ministry plan to integrate and institutionalize cyber hygiene education in school curriculums and rural digital literacy programs, especially under schemes like Digital India or Beti Bachao Beti Padhao? (ii)

Whether any data is available on the training being imparted for cyber security of women in the last ten years in the Centre and at State level? Please give details thereof. MHA informed as under:

'…… I4C, MHA in collaboration with CBSE organized awareness campaigns on cybercrime through VC thereby educating more than 25,000 thousand teachers and students, imparted Cyber Hygiene training to more than 2 lakh NCC, NSS & NYKS Students across the country, a 1930 Cyber Walkathon was organized by I4C in collaboration with Mount Olympus School in Sector 79, Gurugram, Haryana on 22.12.2024. More than 1500 persons, including students, parents, and police officers, participated in this event. States/UTs have been requested by MHA to organize 'Cyber Jaagrookta Diwas' on first Wednesday of every month on cyber hygiene and launch mass awareness in vernacular languages for all schools, colleges, Universities, Panchayati Raj Institutions and Municipalities by involving District Magistrates, Police authorities, Officers of Education Department, PRIs etc. The training regarding women's related issue entitling cybercrimes is being imparted under CCPWC scheme. Regular sessions with NCERT and CBSE teachers will continue to be conducted regularly to sensitise them about cybercrime especially those targeting women and children. States will be encouraged to conduct such training with the state education departments.'

2.8. Further, in a written reply to the question- With numerous awareness initiatives launched, how is the Ministry measuring their reach and impact, particularly among low-income groups and those with limited digital literacy, who may be more vulnerable to certain types of cybercrime? MHA has informed as under:-

To assess the reach and effectiveness of its extensive cyber awareness campaigns, particularly among vulnerable and digitally less literate populations, the Ministry of Home Affairs—through I4C—is adopting a multi-pronged evaluation approach. Under the CCPWC framework and subsequent initiatives, I4C has rolled out awareness programs using diverse and inclusive mediums such as regional language caller tunes, SMS alerts, cinema and radio campaigns, and grassroots engagement through NCC/NSS/NYKS students, school webinars, and events like Raahgiri and Kumbh Mela. These are targeted specifically to reach lower-income groups and rural populations with limited access to digital education.

To measure the impact, I4C is integrating data from various sources, including metrics from the National Cybercrime Reporting Portal (NCRP) and feedback mechanisms from public events and campaigns. The CyberDost social media handle, with over 17.67 lakh followers across platforms, also serves as a live feedback loop. Future plans include enhancing data collection tools on the NCRP dashboard to analyse the effectiveness of outreach by region and demographic and incorporating impact assessments as part of national review mechanisms. This evidence-based approach will help in refining strategies and ensuring that awareness efforts are inclusive, measurable, and adaptive to emerging threats.

Further, an Online Citizen Survey has been conducted by I4C to assess the effectiveness of the National Cybercrime Helpline 1930 in capturing cybercrime incidents and to understand the level of public awareness about the occurrence of cybercrime and the mechanisms put in place by I4C to report them. The feedback received through this survey would facilitate necessary changes in processes and policies around detection of cybercrime.

2.9. There has been an observation of "Low Legal Awareness" as a challenge. Are specific components of awareness campaigns focused on educating women about their legal rights, reporting procedures, and the protections available under the law? MHA, in response to the above question has submitted in a written reply: -

Yes, the Indian Cyber Crime Coordination Centre (I4C) has integrated specific components within its awareness campaigns to address the issue of low legal awareness among women. These campaigns focus on educating women about their legal rights, the reporting procedures available through the National Cybercrime Reporting Portal (NCRP) and the 1930 Cyber Helpline, and the protections provided under key laws such as the IT Act, POCSO Act, and Bhartiya Nayay Sanhita. I4C’s school campaigns, awareness drives with NCC/NSS/NYKS students, and field-level outreach programs are structured to ensure that women, especially from vulnerable and underserved communities, are informed about how to recognize, report, and respond to cybercrimes.

Further, I4C has embedded legal awareness messaging in its nationwide multi-channel campaigns—such as caller tune alerts, SMS broadcasts, radio and cinema ads,

and the CyberDost social media handle—which regularly disseminate information about cyber laws, reporting mechanisms, and victim assistance in regional languages. These efforts are designed to reach women in both urban and rural areas, including those with limited digital literacy. By making legal information accessible, relatable, and repeated across trusted platforms, I4C aims to empower women to assert their rights and take prompt action against cyber offences.

Extensive public awareness campaigns have been undertaken by I4C through various channels (caller tunes, SMS, media ads, social media, celebrity endorsements, school campaigns, etc.) to educate citizens about cybercrime and cyber hygiene, particularly targeting vulnerable groups. Initiatives like Digital Shakti, Cyber Rakshak, and Cyber Shiksha focus on building cyber safety awareness and skills among women and girls.

2.10. On MeitY's Information Security Education and Awareness (ISEA) Project, MeitY informed the Committee:-

As part of the ISEA project, general awareness on various aspects of cyber hygiene and cyber security (incl. cyber safety) is imparted through awareness workshops, quizzes, competitions for schools/colleges students, teachers, women, etc.; organizing training programs for school teachers in association with NCERT, CBSE and State Boards and dissemination of mass awareness multilingual resources in the form of handbooks, posters, short videos, etc. through https://staysafeonline.in/ and social media platforms. Awareness programs are adapted to the needs of the diverse users and literacy levels by tailoring content, delivery methods, and evaluating user feedback.

Repository of multilingual awareness resources presently covers 102 topics on cyber hygiene, cyber safety and cyber security, which are segregated for specific target groups such as women and children based on the age group, demographics, emerging cyber threats, etc. Content designed for Women emphasizes on protection against online harassment, cyberstalking, doxing, promoting safe use of social media, digital financial tools, privacy practices, strong password habits, and awareness of scams targeting women, such as job fraud and romance scams. The Content designed for Children

focusses on safe internet use, protection from online predators and cyberbullying, and fostering healthy screen habits.

The content is made available in the form of cyber safety/security daily tips (bilingual), short videos, reels, shorts, storyboards, and in downloadable formats (i.e. posters, advisories, newsletters, handbooks, etc.) to cater to the diverse needs and address literacy barriers across users. Content is disseminated through (i) Awareness Workshops & Training in schools, colleges, women's groups, etc. (b) Digital Platforms: e-learning portals, ISEA awareness portal (https://staysafeonline.in/), prominent social media platforms, and (c) Use of Traditional Media such as DD/AIR programs, street plays (nukkad natak), and posters to ensure outreach in low-internet rural areas. Additionally, engagements with schools, banks, community-based organizations, self-help groups, educators, and volunteers are carried-out for promotion of cyber hygiene and cyber security awareness at grassroot level.

3. Strengthening Investigation, Forensics & Law Enforcement Capacity

3.1 MeitY initiated a project "CyberShakti: Empowering Indian Women Government Officials in Cybersecurity" in October 2024 to develop women workforce in cybersecurity. The target is to train 1000 women employees from various State/UT Governments, Government organizations and PSUs through beginner level and advanced level courses. So far, 558 and 116 Women Government Officials participated in beginner level training in online mode and advanced level training programme in offline mode respectively. Two Webinars have been conducted to sensitize women government officials about the need of cyber-Security and their prospective role in this domain have been conducted. Total 477 participants joined the webinars.

'Police'& 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India and States/UTs are primarily responsible for dealing with cybercrimes against women. However, to strengthen the mechanism to deal with cybercrimes against women in a comprehensive and coordinated manner, the Central Government has taken coordinated actions to strengthen the capacity of States/UTs. Some of the steps taken in this regard are; awareness about cybercrimes, centralized facility to report cybercrimes 24X7 from anywhere, effective coordination, issuance of alerts/advisories; capacity

building/training of law enforcement personnel/ prosecutors/ judicial officers; improving cyber forensic facilities; etc. MHA is committed to provide a framework and ecosystem for effective coordination among the Law Enforcement and other agencies, to holistically deal with the cybercrimes against women in the country:-

CCPWC Scheme: CCPWC Scheme was launched in 2018 & was operational until 2024. Under this Scheme, MHA has provided financial assistance to the tune of Rs.131.60 crores to States/UTs for setting up of Cyber Forensic-cum-Training Labs, training of LEAs and hiring of Jr. Cyber Forensic Consultants. Cyber Forensic-cum-Training Laboratories have been commissioned in 33 States/UTs namely Andhra Pradesh, Arunachal Pradesh, Assam, Bihar, Chhattisgarh, Gujarat, Haryana, Himachal Pradesh, Kerala, Karnataka, Madhya Pradesh, Maharashtra, Mizoram, Odisha, Sikkim, Telangana, Uttarakhand, Uttar Pradesh, Goa, Meghalaya, Nagaland, Dadra and Nagar Haveli & Daman and Diu, Punjab, Tripura, Puducherry, Chandigarh, J&K, Rajasthan, West Bengal, Jharkhand, Manipur, Andaman & Nicobar Islands and Delhi.

Training curriculum has been prepared for LEA personnel, Public Prosecutors and Judicial officers for better handling of investigation and prosecution. States/UTs have been requested to organize training programmes. More than 24,600 LEA personnel, Public Prosecutors and Judicial officers have been provided training on cybercrime awareness, investigation, forensics etc. under CCPWC Scheme. Police Training Institutions in 36 States/UTs have been supported under this scheme for upgradation/creation of training facilities with special focus on cybercrime against Women & Children.

NCFL Scheme: National Cybercrime Forensic Laboratory (NCFL) has been set up in Dwaraka, New Delhi by the Union Ministry of Home Affairs, Government of India under the aegis of I4C. NCFL extends following services to the LEAs which are crucial in investigating crime against women and children:

Cybercrime Investigation Support: NCFL(I) helps LEAs with processing and analyzing digital evidence like computers, mobile phones, and encrypted data, which is crucial in cybercrime investigations.

Advanced Digital Forensic Services: It employs state-of-the-art tools for various types of digital forensics, such as mobile forensics, crypto forensics, and malware forensics, to uncover critical evidence that can aid in solving cybercrime cases.

Rapid & Targeted Analysis: NCFL(I) helps quick and efficient analysis of digital evidence to speed up the resolution of cybercrime cases.

Training & Capacity Building: It provides training programs to law enforcement personnel, ensuring they are equipped with the latest skills and tools in the ever-evolving field of cybercrime investigation.

Real-Time Investigation Assistance: In addition to remote support, NCFL(I) offers onsite assistance to handle crime scenes and analyze threats directly, ensuring a more hands-on and immediate response to ongoing investigations.

The NCFL includes units likes Memory Forensics Labs, Image Enhancement Lab, Network Forensics Lab, Malware Forensics Lab, Cryptocurrency Forensics Lab, Damaged Hard Disk and Advanced Mobile Forensics Lab.

Total 12,296 forensic cases attended at NCFL Dwarka till 31.05.2025.

3.2 Under the Indian Cyber Crime Coordination Centre (I4C), a dedicated vertical—National Cybercrime Threat Analytics Unit (NCTAU)—has been established to undertake systematic analysis of complaints received through the National Cybercrime Reporting Portal (NCRP). This unit is mandated to identify emerging modus operandi of cybercrimes and to conduct proactive cyber patrolling to collect Open Source Network Intelligence (OSNIT) related to potential suspects. Analytical reports generated by NCTAU are regularly disseminated to Law Enforcement Agencies (LEAs) across States/UTs to facilitate timely preventive and investigative actions.

Furthermore, the SAHYOG platform, developed by I4C, is currently being utilized to transmit takedown requests to Electronic Service Providers (ESPs) including social media Intermediaries, for removal of unlawful content. In the upcoming phase, the platform is proposed to be augmented with functionalities enabling LEAs to submit data requisition requests to ESPs in a structured and streamlined manner. This enhancement is aimed at

minimizing procedural delays and expediting lawful data access for investigation and prosecution of cybercrime cases.

3.3. In response to a question- 'It has been informed that there is an acute shortage of skilled manpower to deal with the new threats and vulnerabilities emerging in the cyber world. What are your views in this regard? How can this issue be addressed? What is the Plan of action to address this issue? Who is responsible for taking action in this regard? What specific capacity building initiatives have been undertaken by the Ministry of Home Affairs to train police personnel, cyber cells, and reporting officers in handling cybercrimes against women?' MHA has informed as under:-

While 'Police' and 'Public Order' fall under State jurisdiction, the Ministry of Home Affairs (MHA), the Indian Cyber Crime Coordination Centre (I4C), has taken several key steps to strengthen the capacity of States and Union Territories in dealing with cybercrimes against women. These initiatives aim to create a uniform and coordinated response system across the country.

I4C sponsored residential training programs from 1 to 10 days duration through various training institutions, State Police Academies, National Police Academies and institutions of national importance for LEAs of all states/UTs on the topics related to investigation of cybercrime and Digital Forensics, Cryptocurrency. Ransomware etc.

The Massive Open Online Courses (MOOC) platform, namely **'CyTrain'** portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cybercrime investigation, forensics, prosecution etc. along with certification. So far over 1.03 lakh persons have obtained certifications on this platform.

The Cyber Commando program aims to train Cyber Commandos from various police ranks across States, Union Territories, and Central Police Organizations, selecting candidates based on their expertise in computer networks and operating systems. Once trained, these commandos will act as a national resource within their respective organizations, specializing in areas like digital forensics, incident response, and ICT infrastructure security. 5000 such commandos are planned to be trained over 5 years. The first batch of trained cyber commandos are already deployed in the states/UTs.

Cyber Forensic Labs: Cyber Forensic Labs act as facilities for forensic analysis and investigation of Cybercrime through use of the latest digital technology to support investigations undertaken by Law Enforcement Agencies (LEAs). Following categories of Cyber Forensic Labs have been set up by I4C in collaboration with different stakeholders:-

a. National Cyber Forensic Laboratory (NCFL): National Cybercrime Forensic Laboratory (NCFL) has been setup in Dwaraka, New Delhi by Union Ministry of Home Affairs, Government of India under the aegis of I4C. Another NCFL is being set up at Assam in collaboration with the Assam police. It will be established at the Lachit Borphukan Police Academy in Dergaon, under a Memorandum of Understanding (MoU) between the Assam Police and the I4C. It will serve mainly the North – East Region.

b. Cyber Forensic Labs in States/UTs: CCPWC Scheme was launched in 2018 & was operational until 2024. Under this Scheme, MHA has provided financial assistance to the tune of Rs.131.60 crores to States/UTs for setting up of Cyber Forensic-cum-Training Labs, training of LEAs and hiring of Jr. Cyber Forensic Consultants. Cyber Forensic-cum-Training Laboratories have been commissioned in 33 States/UTs namely Andhra Pradesh, Arunachal Pradesh, Assam, Bihar, Chhattisgarh, Gujarat, Haryana, Himachal Pradesh, Kerala, Karnataka, Madhya Pradesh, Maharashtra, Mizoram, Odisha, Sikkim, Telangana, Uttarakhand, Uttar Pradesh, Goa, Meghalaya, Nagaland, Dadra and Nagar Haveli & Daman and Diu, Punjab, Tripura, Puducherry, Chandigarh, J&K, Rajasthan, West Bengal, Jharkhand, Manipur, Andaman & Nicobar Islands and Delhi. Training curriculum has been prepared for LEA personnel, Public Prosecutors and Judicial officers for better handling of investigation and prosecution. States/UTs have been requested to organize training programmes. More than 24,600 LEA personnel, Public Prosecutors and Judicial officers have been provided training on cybercrime awareness, investigation, forensics etc. under CCPWC Scheme. Police Training Institutions in 36 States/UTs have been supported under this scheme for upgradation/creation of training facilities with special focus on cybercrime against Women & Children.

Further, to regularly train and assist the States/UTs in cybercrime investigations, following programs have been launched by I4C:

a. **State Connec**t – I4C's Joint Cyber Crime Coordination Team (JCCT) undertakes a 'State Connect' program since 2024. It is undertaken both in offline and online mode. In the offline mode, a dedicated team of I4C experts visits States/Union Territories and conducts workshops with the senior police officers of various ranks of that State/UT. The workshops cover the details of initiatives undertaken by I4C, latest information on investigating complex cybercrime cases and an evaluation report on the State/UT's performance in handling cybercrime. The challenges faced by the State/UT are either clarified on the spot or feedback taken by I4C for follow-up action after the workshop. Till, 30.06.2025, I4C has conducted the state connect program with 29 states.

b. **Peer Learning Session**: Best practices, operational experience, challenges faced, and success stories are shared in the Peer Learning Sessions with LEAs from across the States/UTs of India every friday at 4:00 PM to learn from their peers in an online mode. These sessions are followed by questions and answers to make the discussions fruitful. In every Peer Learning Session, police officials from over 1000 locations spread across India participate. Till 30.04.2025, 115 Peer learning sessions have been organised.

c. **Thana Connect**: To ensure dissemination and use of I4C services by all police stations, I4C launched the online 'Thana Connect' program in February, 2025. It is conducted every Tuesday for one State/Union Territory. The concerned State/UT is required to ensure participation from each police station in its jurisdiction. Till 30.06.2025, 10,596 police personnel from twenty six States/UTs have been participated to tackle trends and operational challenges in cybercrime.

3.4 In what ways is the MHA facilitating the training and sensitization of prosecutors and judicial officers as part of a comprehensive approach to addressing cybercrimes against women? MHA, in a written reply to this question has submitted that- I4C through the National Cybercrime Training Center Vertical carries out Schemes and programs to train and sensitize prosecutors and judicial officers as part of a comprehensive approach to addressing cybercrimes as detailed under:

i. I4C sponsored residential training programs through various training institutions, State Police Academies, National Police Academies and institutions of national importance for LEAs of all states/UTs on the topics related to investigation of cybercrime

and Digital Forensics, Cryptocurrency investigations, Ransomware etc. Number of trainees (Judges/prosecutors) are as under:

Organisation/Official	**No. of Officers trained**
	Cumulative (till 30.06.2025)
Judicial Officers	891
Public Prosecutors	490

ii. The **Massive Open Online Courses (MOOC)** platform, namely 'CyTrain' portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cybercrime investigation, forensics, prosecution etc. along with certification. Number of registered trainees and certificates issued to Judges/prosecutors are as under:

Organisation	**Trainees Registered**	**Certificates issued**
	Cumulative (till 30.06.2025)	**Cumulative (till 30.06.2025)**
Judges/Prosecutors	397	90

iii. **Cyber Forensic Labs in States/UTs**: CCPWC Scheme was launched in 2018 & was operational until 2024. Under this Scheme, MHA has provided financial assistance to the tune of Rs.132.93 crores to States/UTs for setting up of Cyber Forensic-cum-Training Labs, training of LEAs, judicial officers, prosecutors and hiring of Jr. Cyber Forensic Consultants. Cyber Forensic-cum-Training Laboratories have been commissioned in 33 States/UTs namely Andhra Pradesh, Arunachal Pradesh, Assam, Bihar, Chhattisgarh, Gujarat, Haryana, Himachal Pradesh, Kerala, Karnataka, Madhya Pradesh, Maharashtra, Mizoram, Odisha, Sikkim, Telangana, Uttarakhand, Uttar Pradesh, Goa, Meghalaya, Nagaland, Dadra and Nagar Haveli & Daman and Diu, Punjab, Tripura, Puducherry, Chandigarh, J&K, Rajasthan, West Bengal, Jharkhand, Manipur, Andaman & Nicobar Islands and Delhi. Training curriculum has been prepared for LEA personnel, Public Prosecutors and Judicial officers for better handling of investigation and prosecution. States/UTs have been requested to organize training programmes. More than 24,600 LEA personnel, Public Prosecutors and Judicial officers have been provided training on cybercrime awareness, investigation, forensics etc. under CCPWC Scheme. Police

Training Institutions in States/UTs have been supported under this scheme for upgradation/creation of training facilities with special focus on cybercrime against Women & Children.

3.5. Further, MHA has submitted in a written reply to the question 'What are the future plans and strategic frameworks envisioned by the Ministry of Home Affairs to strengthen institutional and technological capacity among law enforcement and other stakeholders for tackling cybercrimes against women?

Augmentation of Cyber Forensic Facilities is one of the key components of this strategy to enhance capacities of LEAs through forensic tools, expert consultants, and advanced IT infrastructure to support police investigations. **'CyTrain' portal has been launched to helps in the capacity building of police officers/judicial officers through online course** on critical aspects of cybercrime investigation, forensics, prosecution etc. along with certification. Training curriculum has been prepared for Police personnel, Public Prosecutors and Judicial officers for better handling of investigation and prosecution. States/UTs have been requested to organize training programmes. More than 24,600 LEA personnel, Public Prosecutors and Judicial officers have been provided training under CCPWC Scheme. Physical training is also provided from time to time. I4C is making efforts for the capacity building of all pillars of criminal justice system i.e. LEAs, Forensic Examiners, Prosecutors and Judges for imparting training across the country. 'State Connect' programme has been started under I4C both in offline and online mode. In the offline mode, a dedicated team of I4C experts visits States/Union Territories and conducts workshops with the senior police officers of various ranks of that State/UT. So far, I4C has conducted the state connect program with 29 states. 'Thana Connect' programme has been launched under I4C in online mode to ensure dissemination and use of I4C services by all police stations. It is conducted every Tuesday for one State/Union Territory. So far, 10,596 police personnel from 26 States/UTs have been participated to tackle trends and operational challenges in cybercrime. Best practices, operational experience, challenges faced, and success stories are shared in the Peer Learning Sessions with LEAs from across the States/UTs of India every Friday at 4:00 PM to learn from their peers in an online mode. So far, 115 Peer learning session has been organised.

3.6 In a written submission, MHA has informed that in the evolving landscape of cybercrime, especially those targeting women and children, traditional investigative approaches are no longer sufficient. Fraudsters are increasingly leveraging advanced technologies, including artificial intelligence (AI), anonymization tools, and encrypted platforms to evade detection. Therefore, continuous and specialized training of law enforcement officials, prosecutors, and judicial officers is essential to equip them with the necessary skills to understand, trace, and prosecute such complex cyber offences effectively.

Beyond the quantitative metrics of officials trained, the Ministry **will be incorporating outcome-based indicators to assess the real-world impact of these capacity-building initiatives.** This includes tracking the increase in the **conversion rate of cybercrime complaints** into FIRs, the number of chargesheets filed, reduction in time taken to complete investigations, and the rate of convictions secured—particularly in cases involving women and children.

Further MHA informed that Cybercrime knows no boundaries—offenders can operate from any part of the country and target victims located in distant States or Union Territories. Traditional methods such as physically deputing officers to other jurisdictions for investigation are not only time-consuming but also operationally inefficient in handling the scale and complexity of cyber offences. To address this challenge, the Ministry of Home Affairs has developed the **SAMANVAYA platform** under the Indian Cyber Crime Coordination Centre (I4C). This platform facilitates real-time coordination between Law Enforcement Agencies (LEAs) across States/UTs, enabling secure digital sharing of suspect information including names, addresses, bank details, SIM/IMEI data, and more. Tools like Pratibimb and GIS-based mapping help visually connect data points for better analytical insights. Before the establishment of the JCCT, there was no common platform to facilitate interstate coordination in cybercrime investigations. The SAMANVAYA platform now enables better coordination among Law Enforcement Agencies (LEAs) across different States and Union Territories (UTs), with the following key features:

CIAR (Cybercrime Investigation Assistance Request): This feature allows for sending and receiving requests for assistance, including the execution of summons, service of

notices, address verification, and other investigative support. All States and UTs are actively utilizing this facility.

Techno-Legal Support: LEAs from various States and UTs can seek critical assistance from subject matter experts at I4C during the course of investigations. Majority of the States/UTs are utilising this facility.

3.7. The Ministry of Home Affairs, through I4C, is actively working to standardize and facilitate the adoption of effective tools like **Internet Crime Against Children Child On-line Protection System (ICACCOPS)** across all States and Union Territories to ensure a consistent and coordinated approach to tackling cybercrimes against women and children. I4C is in the process of formal collaboration with platforms such as ICACCOPS, which are integrated with international agencies like the International Centre for Missing & Exploited Children (ICMEC), to strengthen the detection and takedown of Child Sexual Exploitative and Abuse Material (CSEAM) nationwide. Once finalized, the platform will be rolled out uniformly across all States/UTs.

I4C has already provided access to the Cyber Tipline Case Management Tool (CMT) of NCMEC to all State/UT nodal officers and is disseminating tipline information to LEAs on a daily basis for prompt action. Additionally, training programs have been conducted in collaboration with NCMEC to build capacity among LEAs. These efforts collectively aim to institutionalize best practices and ensure a uniform, technology-enabled response to online crimes against vulnerable groups across the country.

3.8. MHA, in response to the question-What specific data is the Ministry collecting to identify potential bottlenecks, delays, or challenges within the prosecution and judicial process specifically for cybercrime cases against women and children, from filing of charge sheets to final judgments, has reiterated that Police and Public order are State subject and State LEAs have to take proactive measures to tackle cyber crime against women and children. The measures, inter-alia, includes registration of cases, filing of chargesheet, removal of content, awareness generation, capacity building, designation of fast track courts, establishment of forensic support system for LEAs.

3.9. Further, in regard to any concrete administrative or policy interventions being implemented to streamline the trial process for these sensitive cases, MHA submitted that

I4C, MHA has written to all states and UTs to set up fast track courts to tackle cybercrime cases. Once set up, these courts will expedite the trial of cybercrime cases including those pertaining to women and children.

4. SOP for investigation

4.1 The Ministry of Home Affairs, through the Indian Cyber Crime Coordination Centre (I4C), has established a comprehensive and citizen-friendly mechanism to report cybercrime cases across India. The key components of this mechanism are as follows:

i. **National Cybercrime Reporting Portal (NCRP)** – www.cybercrime.gov.in: This is a 24x7 online platform available in multiple languages that allows any individual, from anywhere in the country, to report cybercrime incidents. It has two dedicated reporting options:

- "Report Women/Child Related Crime" (can be reported anonymously)
- "Report Other Cybercrimes" (requires user details and OTP verification) Complaints are automatically routed to the concerned State/UT police based on technical identifiers such as IP address, mobile number, or victim's location.

ii. Cybercrime Helpline (1930): Citizens who fall victim to financial cyber frauds can call 1930, a toll-free number where specially trained call center agents assist the complainant in blocking the fraudulent transaction by immediately alerting banks and payment platforms through the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS).

iii. Offline Reporting at Police Stations: Victims can also lodge a cybercrime complaint at their nearest police station, where cyber nodal officers or designated cybercrime cells handle these cases. In many States, cybercrime cells at district and State levels have been established to support investigation.

iv. **Report and check suspect:** To enhance cyber safety measures in the country, the National Cybercrime Reporting Portal (NCRP) of I4C, MHA has recently introduced a new feature titled as ‘Report and Check Suspect’ on https://www.cybercrime.gov.in. This facility interacts with the citizens in two ways:

a. It provides citizens a search option to search I4C's repository of identifiers of cyber criminals through 'Suspect Search'. Now, citizens can inquire about the mobile numbers, e-mail Ids, account numbers, URLs and other identifiers for their possible linkages with the cyber criminals.

b. We intend to not only provide information to citizens but also make them a partner in prevention of cybercrime by pro-actively seeking information from them. For this purpose, a tab namely 'Report Suspect' has been created under 'Report and Check Suspect' to enable citizens to report suspicious website URLs, WhatsApp numbers/telegram handles, phone numbers, e-mail ids, SMS headers/numbers, deep fakes and social media URLs. This reported data will be used to ascertain potential cyber threats and neutralize them in time. Appropriate action will be taken by Law Enforcement Agencies only when the sufficient collaboration is made out from other sources in respect of information provided by the citizens. The citizens not only report suspicious identifiers to I4C but can also lodge complaints with Social Media Intermediaries against any objectionable online content activities.This multi-channel reporting and redressal system is designed to make cybercrime complaint registration accessible, responsive, and supportive to all citizens, particularly women and children.

4.2. In a written reply to the question 'Despite the availability of NCRP and the 1930 helpline, what challenges prevent women—especially in rural and semi, urban areas from reporting cybercrimes, MHA informed the Committee as under :-

Despite the availability of the NCRP portal and the 1930 helpline number, women in rural and semi-urban areas may be facing several challenges in reporting cybercrimes due to limited awareness about reporting mechanisms and lack of digital literacy. **Many women also lack access to mobile phone or the internet, making online reporting difficult. Additionally, language barriers and the absence of localized support systems would further discourage reporting.**

4.3. Major operational challenges faced by police stations, especially in Tier II/III cities and rural districts, in identifying and acting upon cases involving CSAM and online harassment of women:-

Police stations in Tier II/III cities and rural districts face several operational challenges in effectively identifying and responding to cases involving CSEAM and online harassment of women:

i **Lack of technical expertise:** Many local police personnel are not adequately trained in digital forensics, cyber laws, or online evidence handling, which makes it difficult to identify, preserve, and act upon digital offences.

ii **Limited cyber infrastructure:** Police stations often lack essential tools such as high-speed internet, forensic software, secure data storage, and access to real-time platforms like SAHYOG or cyber forensic labs, slowing down response time.

iii **Under-reporting and victim hesitation:** Victims, especially women in rural areas, are often reluctant to report cases of online harassment or CSEAM due to social stigma, fear of defamation, or lack of awareness about reporting mechanisms like cybercrime.gov.in.

iv **Jurisdictional confusion:** Officers sometimes face uncertainty in handling complaints involving content shared from unknown or foreign IPs, especially on encrypted platforms or anonymous accounts. This is worsened by limited exposure to cross-jurisdiction coordination protocols.

v **Delays in data access from platforms:** Obtaining user data or takedown support from social media and messaging platforms is often slow, particularly for smaller districts without dedicated cyber cells or liaison officers.

vi **Shortage of manpower and specialized units:** Many rural police stations operate with limited staff who are already burdened with multiple responsibilities, leaving little capacity to pursue time-sensitive and technically complex cybercrime investigations.

vii Lack of victim-sensitive protocols: In many areas, police handling of cyber offences against women lacks empathy, privacy, or gender-sensitization, discouraging victims from pursuing cases further.

4.4. Further, in regard to formulation of a nationally applicable Standard Operating Procedure (SOP) for timely reporting, investigation, evidence collection, and takedown requests for cybercrimes targeting women and children, MHA has informed that the Ministry of Home Affairs, through the Indian Cyber Crime Coordination Centre (I4C), **is in the process of formulating a nationally applicable Standard Operating Procedure**

(SOP) to guide police and investigative agencies in the timely reporting, investigation, digital evidence collection, and takedown of harmful content in cases involving cybercrimes against women and children. The SOP aims to bring uniformity in handling such sensitive cases across States and Union Territories, especially for offences like sextortion, online stalking, impersonation, deepfakes, and CSEAM.

5. Leveraging Technological Advancements to enhance Cyber Security Frameworks

5.1. Proactive Monitoring Tool (PMT):

CDAC Mumbai has developed a Proactive Monitoring Tool (PMT) based on machine learning to proactively identify and filter Child Sexual Exploitative Abuse Material (CSEAM) content. The scope of work for the PMT includes the development of a scalable proxy network infrastructure to continuously crawl the web for CSA and Rape/Gang Rape (RGR) content without being blocked by websites. It also involves software capable of classifying crawled content as CSA, assigning a content severity score, and extracting information such as the number of individuals depicted and their estimated ages. Additionally, a robust image hashing module has been created to store and catalog relevant content from crawled data, forming a comprehensive repository or knowledge base. The tool further includes components to classify images and videos related to RGR and a centralized dashboard for system management, configuration, and regular statistical reporting.

At present, this tool is being utilized to analyze incoming Tipline reports to determine whether they contain CSEAM content. This aids in the swift identification and assessment of harmful material, enhancing the ability of law enforcement and relevant agencies to respond promptly and effectively.

SAHYOG: The Sahyog Portal is an online platform developed to facilitate the issuance of notices under Section 79(3)(b) of the Information Technology Act, 2000, by the appropriate government or its authorized agencies to IT intermediaries. Its primary objective is to ensure the prompt removal or disabling of access to information, data, or communication links used for unlawful activities, thereby promoting a safer and more secure cyberspace in India. By bringing together all authorized agencies—including

Central Law Enforcement Agencies (8), State agencies (28), and UT agencies (6)—along with IT intermediaries (66), Internet Service Providers, and Virtual Asset Service Providers (34) on a single platform, the portal enables coordinated and timely action against illegal or unlawful online content. So far, a total of 199 notices have been issued involving 1,412 URLs, out of which 940 have been taken down. Many of these URLs might be containing objectionable online content against women and children.

5.2. In this connection, whether MeitY is considering amending the IT Rules to mandate deployment of AI-based cyberbullying detection modules on all major social media platforms operating in India, similar to the PMT model for CSAM, MeitY in a written submission has informed that the Government is committed to leveraging emerging technologies like AI for public good across key sectors, while remaining vigilant about their misuse, particularly in the form of misinformation and deepfakes. The IT Act, 2000 does not differentiate between information generated through AI or other technologies and that created by users directly. To ensure that the Internet remains Open, Safe, Trusted, and Accountable, MeitY has notified and amended the IT Rules, 2021, which impose legal obligations on intermediaries, including social media platforms. These include taking reasonable efforts including their expeditious action towards removal of unlawful content under Rule 3(1)(b) and compliance within 36 hours upon receipt of court orders or government notices under Rule 3(1)(d), thereby ensuring platform accountability and user safety.

Under Rule 4(4) of the IT Rules, 2021, SSMIs are already required to deploy technology-based measures to proactively identify specific harmful content. Further, through a series of advisories issued on 26.12.2023, 15.03.2024, and 03.09.2024, MeitY has reiterated intermediaries' legal obligations under Rule 3(1)(b) and emphasized the use of technological measures like AI responsibly, including content labelling, user awareness, and mechanisms for user reporting. These advisories aim to strengthen platform accountability and protect users, especially from AI-enabled harms, while reminding intermediaries that non-compliance may result in the loss of exemption from the liability for third party information/content as provided under section 79 of the IT Act and legal consequences.

5.3 Further, in response to a question-What steps has MeitY taken to evaluate or implement large language model-based (LLM) AI tools that detect gender-targeted harassment, trolling, or threats in regional languages and dialects across digital platforms, MeitY has informed as under-

'The matter is related to cybercrime, which pertains to Ministry of Home Affairs (MHA) and hence MHA is in better position to reply'

5.4. In regard to provisions which are in place to facilitate mandatory disclosure of identity-linked metadata by intermediaries, when AI systems flag suspicious accounts or content related to cyber harassment, MeitY submitted that Intermediaries are required under Rule 3(1)(j) of the IT Rules, 2021 to provide identity-linked information or assistance to lawfully authorised government agencies within 72 hours for investigation or cyber security purposes. Additionally, Rule 4(2) mandates Significant Social Media Intermediaries (SSMIs) offering messaging services to enable identification of the first originator of a message upon valid legal orders under Section 69 of the IT Act. Under Rule 4(4), SSMIs must deploy technology-based tools to proactively detect harmful content, including CSAM, and notify users attempting to access such flagged information. Under Rule 7 of the IT Rules, 202, non-compliance with these provisions may lead to loss of exemption from the liability for third party information/content as provided under section 79 of the IT Act and legal consequences. Further, MeitY advisories dated 26.12.2023 and 15.03.2024, among other things, direct intermediaries to embed permanent metadata identifiers in AI-generated content like deepfakes to ensure traceability.

5.5. Further, in a written reply of the question- Is MeitY developing any APP/Software to enable the cyber fraudsters to not get access to photographs and videos which are personal in nature to protect against cyber crimes, MeitY has informed to the Committee-

'The cybercrime/cyber-fraud is dealt by Ministry of Home Affairs (MHA) and hence, MHA is in better position to reply'

6. Budget Allocation for Research & Development

6.1. In a written communication MHA informed the Committee- 'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. The

States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs. The efforts of the States for equipping and modernizing their police forces has been supplemented under the scheme of "Assistance to States & UTs for Modernization of Police" {erstwhile scheme of Modernization of State Police Forces (MPF)}. Under the scheme, central assistance is provided to all the State/UT Governments for procurement of weapon; equipment for Information Technology, Communication, Training, etc. Construction of Police stations is also allowed to all States and UTs. An amount of Rs. 205.6175 crore has been released to all the State/UT for Modernization of Police" under Police Modernization Scheme during the last three years.

6.2. The Ministry of Home Affairs has released financial assistance to the tune of Rs. 132.93 crore under the 'Cyber Crime Prevention against Women and Children (CCPWC)' Scheme, to the States/UTs up to 31.03.2024 for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of LEAs' personnel, public prosecutors and judicial officers. Under the Nirbhaya Fund scheme, an amount of Rs. 97.99 crore was allocated to all States/UTs for strengthening DNA and Cyber/Digital Forensics facilities. All States/UTs have reported 100% utilisation of the allocated funds also developed DNA and Cyber Division.

6.3. In response to a question regarding list of organisations which undertake R&D in cyber security in our country and seeking information whether the funding to these organisations have been adequate enough. If no, the reasons thereof and the remedial steps taken thereon, MeitY has informed as under-

"MeitY invites proposals for R&D in cyber security from academic and research institutes on current and prospectives topics to develop tools and technologies for funding. These proposals are evaluated by a Working Group chaired by an experienced academic Professor. After recommendation of Working Group, proposals are processed for approval of the competent authority. Organisations which are being funded for R&D projects in cyber security by MeitY are IITs, NITs, Other academic institutes and CDAC Centres.

Funds are adequately provided as per the project objectives and deliverables proposed by the project implementing agency/organisation.

Further, MeitY is funding academic and research institutes to undertake research and development to develop tools and technologies in cyber security. The thrust areas for R&D in cyber security include but not limited to embedded systems and IoT security, cyber forensics, mobile device security, threat intelligence and AI/ML based threat modeling, network and system security, industrial security, detection & mitigation of malware, risk assessment & mitigation, and security issues in emerging technologies such as AI, IoT, Cloud computing, quantum computing etc.

Organisations under MeitY or associated with MeitY that have currently undertaken R&D projects in cyber security are C-DAC (C-DAC Kolkata, C-DAC Hyderabad, C-DAC PATNA, C-DAC Thiruvanthapuram, C-DAC Bangalore, C-DAC Chennai, C-DAC New Delhi, C-DAC Noida), NIELIT Kohima and ERNET Chennai.

6.4 Further, in regard to the total budgetary allocation under MeitY in FY 2025–26 for supporting R&D projects focused on cybercrime detection and prevention technologies, particularly those addressing cyber threats against women, MeitY submitted that the total budgetary allocation under MeitY in FY 2025–26 for supporting Cyber Security Projects is Rs. 782 Cr from which R&D projects are funded. However, there is no separate fund focused on cybercrime detection and prevention technologies, particularly those addressing cyber threats against women.

6.5. Further in a written submission, MeitY has also informed that there is no separate budget allocation to support cyber forensic labs and Examiner of Electronic Evidence under Section 79A of the IT Act. The Notification of Cyber Forensic Labs as Examiner of Electronic Evidence under Section 79A of the IT Act is one of the activities of MeitY and MeitY has not sanctioned any grant-in-aid in FY 2025-26 or in the past to develop deepfake detection, anti-stalking or AI-based alert systems for women's online safety.

7. Role of Social Media Intermediaries in Ensuring Online Safety for Women

7.1 Meity has informed about the various provisions of the IT Rules, 2021 that focus on enhanced safety of women and children include inter alia the following:

i. Prohibiting transmission of unlawful information violative of Rule 3(1)(b) of the IT Rules, 2021:

- Rule 3(1)(b) of the IT Rules, 2021 prohibits eleven types of content on the Indian Internet available on the intermediary platform. Intermediaries are required to ensure that their users do not use their platforms for sharing or transmitting content that violates Rule 3(1)(b) and other laws and that their terms of use expressly restrict use of eleven types of unlawful information which inter-alia include the following.

- Rule 3(1)(b)(ii): Information that is obscene, pornographic, invasive of another's privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, or any information that is relating promoting hate speech etc. [Obscenity/ Hate speech/ Harassment]

- Rule 3(1)(b)(v): Information that deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates misinformation, patently false information, untrue or misleading in nature. [Misinformation/ Deepfakes]

- Rule 3(1)(b)(vi): Information that impersonates another person. [Impersonation/ Deepfakes]

- Rule 3(1)(b)(xi): Information that violates any law for the time being in force. [E.g., Indecent Representation of Women (Prohibition Act), 1986; Bharatiya Nyaya Sanhita, 2023, etc.]

ii. Immediate termination of user account engaged in unlawful activity against violation of Rule 3(1)(c) of the IT Rules, 2021:

Rule 3(1)(c) of the IT Rules, 2021 mandates all intermediaries including social media intermediaries that all users must be clearly informed periodically including through the terms of services and user agreements of the intermediary or platforms about the consequence of dealing with the unlawful information on its platform, including disabling of access to or removal of non-compliant information, immediate termination of access or usage rights of the user to their user account, as the case may be, and punishment under applicable law.

iii. Time-bound removal or takedown of unlawful information under Rule 3(1)(d) of the IT Rules, 2021:

Rule 3(1)(d) of the IT Rules 2021 mandates the platforms to ensure expeditious action, well within the timeframes stipulated under the IT Rules, 2021 (as early as possible but not later than 3 hours), to remove or disable access to information/content that violates the aforesaid provisions of the IT Rules, 2021, upon receipt of court orders or reasoned intimation from the Appropriate Government or its authorised agency.

iv. Providing information & assistance to Law Enforcement Agencies (LEAs):

Rule 3(1)(j) of the IT Rules, 2021 mandates the intermediaries to provide information under their control or possession, or assistance well within the timeframes stipulated under the IT Rules, 2021 (as soon as possible but not later than 72 hours) to the Government agency which is lawfully authorized for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents.

v. Time-bound Grievance Redressal Mechanism under Rule 3(2) of the IT Rules, 2021:

Rule 3(2) of the IT Rules 2021 mandates the intermediaries to ensure expeditious action, well within the timeframes stipulated under the IT Rules, 2021 (not later than 36 hours), to resolve complaints of violation of the rules in relation to select prohibited information under Rule 3(1)(b) which are either heinous or serious in nature and, in case of a complaint by an individual or her/his authorized representative, remove within 2 hours any content which prima facie exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct (i.e. breach of physical privacy and circulation of revenge pornography) or which is in the nature of impersonation or an artificially morphed images (i.e. deepfakes) of such individual.

vi. Enhanced Grievance Redressal through appealing mechanism under Rule 3A – Establishing Grievance Appellate Committees (GAC):

The Government has also established GAC under Rule 3A of the IT Rules, 2021 to allow users and victims to appeal online on www.gac.gov.in against decisions taken by the Grievance Officers of intermediaries in case they are dissatisfied with the decision of the Grievance Officer in case of legal violations including obscenity, vulgarity, misinformation and deepfakes or where the Grievance Officers fails to redress the grievances from users or victims or an individual or any person on his behalf within the timelines prescribed under the IT Rules, 2021.

vii. Deployment of automated tools under Rule 4(4) of the IT Rules, 2021 to proactively identify and remove unlawful information and curb their virality:

Rule 4(4) of the IT Rules, 2021 requires SSMI to endeavour deployment of automated tools or other 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 Rule 3(1)(d) of the IT Rules, 2021 in accordance with the clause. Rule 4(4) also requires that the SSMI shall display a notice to any user attempting to access any information included under this sub-rule stating that such information has been identified by the intermediary under the categories referred to in the sub-rule. This would help mitigating the concerns of virality happened through social media platforms.

viii. Appointment of designated officers based in India and publishing physical address to be in India by SSMI under Rule 4(1) of the IT Rules, 2021 to assist in enforcement of rules & laws of the land:

Rules 4(1) and 4(5) of the IT Rules, 2021 require SSMI to appoint a Chief Compliance Officer, a Resident Grievance Officer and a nodal contact person, all to be residents in India; and have a physical contact address to be in India so as to

make them accountable for speedy law enforcement and compliance with the IT Act and rules made thereunder.

ix. Loss of safe harbour against failure to comply by the intermediaries:

Rule 7 of the IT Rules, 2021 provides that in case of failure of the intermediaries to observe the legal obligations as provided in the IT Rules, 2021, they lose their safe harbour protection under Section 79 of the IT Act and shall be liable for consequential action or prosecution as provided under any extant law.

7.2 In regard to modal SOPs for intermediaries (e.g., social media platforms, ISPs) regarding timely content removal, metadata sharing, and cooperation with LEAs in cases of cybercrimes against women, Meity submitted that the formulation and enforcement of Standard Operating Procedures (SOPs) for intermediaries such as social media platforms and internet service providers falls primarily under the domain of the Ministry of Electronics and Information Technology (MeitY), as per the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. However, to support timely action in cases of cybercrimes against women, the Ministry of Home Affairs, through the Indian Cyber Crime Coordination Centre (I4C), has developed the SAHYOG portal. This is based on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. This platform enables law enforcement agencies across States and Union Territories to send structured unlawful content removal notices and data access requests to social media intermediaries in a secure and time-bound manner. In case the takedown requests are not complied with by the IT Intermediaries within a time specified under the IT Act and rules framed thereunder, LEA's retain the right to lodge FIRs against the IT Intermediaries.

7.3 In regard to the number of complaints received on Sahyog Portal, MHA informed that portal does not receive complaints from citizens. It processes takedown requests/notices received from LEAs under Section 79(3)b of the IT Act read with Rule 3(1)(d) . A total of 16484 online links/illegal contents/apps/websites have been taken down (till 31.07.2025) through the Sahyog portal. Noncompliance to Section 79(3)b of IT Act entails loss of Safe Harbour for the IT Intermediary and LEAs are free to act accordingly. No action against IT Intermediaries have been initiated by MHA so far.

7.4. Further, in response to a question regarding developing their own Indian platform like StopNCII.org, MHA assured to examine the recommendation in consultation with stakeholders.

7.5. Further, MHA has informed that as on 30th June 2025, I4C has forwarded a total of 1,41,206 URLs to intermediaries for the removal of unlawful content and accounts, and the intermediaries have acted upon them accordingly. I4C, MHA is proactively monitoring compliance by intermediaries with removal notices issued under Section 79(3)(b) of the Information Technology Act, 2000, ensuring timely action—within 36 hours, or 24 hours in cases involving CSAM (Child Sexual Abuse Material). Under Section 69A of IT Act, Meity considers blocking requests only from notified Nodal Officers of different organizations. All requests are examined by an Inter-Ministerial Committee and recommended for blocking action. In addition, a review committee regarding review of blocking directions issued by MeitY under Section 69A of the IT Act, 2000.

7.6 In a written submission, MHA submitted the data of complaints received in the categories related to Women and Children on NCRP is as under:

Category	Sub-Category	2019	2020	2021	2022	2023	2024	2025 (Till 31.05.2025)
CSAM/CSEM/RGR (Anonymous + Report &Track)	(i) Child Pornography (CP)-Child Sexual Abuse Material (CSEAM)	188	2019	2109	3062	2957	6079	2938
	(ii)Rape/Gang Rape (RGR)-Sexually Abusive Content	180	2184	27945	30574	12129	4273	2981
	(iii)Sexually Obscene material	943	9606	12251	16341	14322	21990	12094
	(iv)Sexually Explicit Act	782	8379	9743	12247	10658	16133	7395
TOTAL		**2093**	**22188**	**52048**	**62224**	**40066**	**48475**	**25408**

7.7 At present, Social Media Intermediaries (SMIs) report Child Sexual Abuse Material (CSAM) to the National Center for Missing and Exploited Children (NCMEC), a U.S.-based non-profit that operates a global cyber tipline. These reports are received by the

designated Nodal Officer at I4C, who is authorised to access them securely. I4C uses these reports to identify actionable complaints and, based on jurisdiction (victim or suspect location), distributes them to the concerned State/UT Law Enforcement Agencies (LEAs). LEAs have been onboarded to the Cyber Tipline Management Tool (CMT) maintained by NCMEC, enabling them to directly receive and access these reports. Before distribution, the reports are filtered through the Proactive Monitoring Tool (PMT) to remove false positives, and further analysis is conducted by the Online Cybercrime against Women and Children (OCWC) team at I4C. This team flags habitual offenders, prepares detailed case summaries, and shares them with respective LEAs for focused action.

As per the Supreme Court's direction in the *Just Rights for Children Alliance* case, intermediaries are now expected to report CSAM not only to NCMEC but also directly to Indian LEAs.

7.8 In a written reply to the question- What actions has the Ministry taken in cases where intermediaries failed to comply with takedown notices or refused to cooperate under Section 79(3)(b) of the IT Act? Have any intermediaries lost their "safe harbour" protection so far due to non-compliance? MHA has informed that I4C, MHA is proactively monitoring compliance by intermediaries with removal notices issued under Section 79(3)(b) of the Information Technology Act, 2000, ensuring timely action—within 36 hours, or 24 hours in cases involving CSAM (Child Sexual Abuse Material). In cases of non-compliance or delayed compliance within the specified timeframe, I4C engages with the intermediary's nodal officer and convenes meetings to address the issue.

7.9 In regard to any study undertaken worldwide as to what all powers do Government have over intermediaries and where is our legal system lacking in that? MHA has submitted tha**t** I4C has not undertaken any study worldwide in this regard, however, the Government exercises regulatory powers over intermediaries under various provisions of the Information Technology Act, 2000 and associated rules, mainly:

i. **Section 69A of the IT Act**, **2000** – Empowers the Government to direct intermediaries to block access to information in the interest of sovereignty, integrity of India, security of the State, public order, or to prevent incitement to any cognizable offence. Non-compliance may lead to penal consequences.

ii. **Section 79(3) of the IT Act –** Grants conditional "safe harbour" to intermediaries, which can be lifted if they fail to comply with Government directions or do not act on unlawful content after receiving actual knowledge or notification by the appropriate authority.

iii. **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** –Mandate intermediaries to publish terms of use and privacy policies and require grievance redressal mechanisms to be established. Further, the IT Rule 2021, impose obligations to remove unlawful content within stipulated timelines upon receiving actual knowledge or being notified by agency of appropriate government. Additionally, Significant Social Media Intermediaries (SSMIs) have further obligations like appointing chief compliance officers, nodal contact person, grievance officers.

Further, the Indian legal system provides a comprehensive and balanced framework to regulate intermediaries through the Information Technology Act, 2000, the IT Rules, 2021, and the strengthened provisions of the new criminal laws, 2023.

7.10 Further, the existing mechanism to control the fraudulent cases on Matrimonial websites, the Ministry of Home Affairs, through the Indian Cyber Crime Coordination Centre (I4C), has enabled systems for effective reporting and investigation of cyber frauds on matrimonial websites. Victims can report such incidents through the National Cybercrime Reporting Portal (www.cybercrime.gov.in), where complaints are routed to the appropriate State or UT police based on digital identifiers.

7.11 To identify trends and evolving fraud tactics, the Threat Analysis Unit (TAU) at I4C regularly monitors the portal for emerging modus operandi used in cases involving impersonation, emotional manipulation, and financial exploitation of women on matrimonial platforms. This intelligence is shared with concerned law enforcement agencies for targeted action. Awareness efforts are also conducted to educate users, particularly women, about safe practices while interacting on such platforms. These steps help ensure stronger preventive mechanisms and improved law enforcement response to such offences. Being IT Intermediaries such platforms are expected to exercise due diligence about the content hosted on their platform in accordance with Rule 3(1)a of the IT Intermediary Guidelines, 2021.

7.12 In a written submission, removal of harmful content related to women and to ensure swift justice, Google Inc. has informed that Google proactively works with Law

Enforcement Agencies (LEA) to assess threats and to counter attempts to deceive, harm, or take advantage of people using the platforms. Google maintains regular communication channels with law enforcement, as communication with law enforcement, industry partners, and government agencies is a key component of efforts to keep users safe. Information from industry peers and law enforcement help in YouTube's efforts to ensure the integrity of the platform and act swiftly in response to crises or when abuse that may threaten public safety or the integrity of democratic processes is detected. Interactions with law enforcement include the following:

i. Google regularly engages with Indian LEAs to ensure that it is able to explain the various processes and procedures followed by it in responding to requests from LEAs. In addition,

ii. Google takes valuable feedback to further improve upon or streamline its existing processes.

iii. Google has held workshops with various LEAs including the cybercrime cells in various cities in India. Google representatives have presented at seminars and workshops held by various agencies, including the National Police Academy, CBI and the MHA. These sessions are designed to equip LEA to report content more accurately and to ensure that proper processes are followed to ensure expeditious review and action. Further, senior officers and specialists from the legal investigations team of Google have visited law enforcement officers in various states and central investigative agencies such as the CBI to address their concerns and to explain existing policies and the approach taken in responding to their requests.

iv. Google also partnered with the Data Security Council of India and Cyber Peace Foundation to train law enforcement agencies across India on cybercrime investigations. With a view to expedite review of requests for removal of unlawful content received from government authorities and law enforcement agencies, Google has made available a dedicated webform that enables bulk reporting of unlawful content. This is a dedicated channel created for use only by law enforcement and other government agencies empowered to send requests for content removal in India, so that the relevant support team can review the matter and action as per the applicable policies.

7.13. X (Formerly Twitter) partners with StopNCII, a global initiative aimed at preventing the non-consensual sharing of intimate images through hash matching technology. This partnership provides access to StopNCII's hashes to detect and prevent the spread of NCII on our platform. In addition to users being able to report NCII directly to X to get it removed, users can also create hashes of their own images on a separate website provided by StopNCII, which are then shared with participating platforms which can then detect, block, and remove matching content to proactively prevent abuse. (X reply through Meity)

7.14 In written submission, Meta has informed that they have strict rules against content or behavior that exploits people, including sharing or threatening to share someone's intimate images via sextortion. We encourage anyone who sees content they think breaks our rules to report it—and they have a dedicated reporting option to use if someone is sharing private images. When we become aware of this content, we work to take action. They have specialized teams working on combating sextortion. They have identified patterns associated with this behavior, and built automated systems that detect and remove these accounts at scale. They also have dedicated teams that investigate and remove these criminals and report them to authorities, including law enforcement and NCMEC, when appropriate. They work with partners, like NCMEC and the International Justice Mission, to help train law enforcement around the world to identify, investigate and respond to these types of cases. They recognise the critical role of law enforcement agencies ("LEAs") in keeping the public safe, and are wholly committed to cooperating with Indian authorities. We carefully review, validate and respond to LEA requests based on applicable law and policy and share actionable information with Indian LEAs when called upon.

Further, Meta responds to data disclosure requests received from various LEAs across India through the Law Enforcement Online Request System ("LEORS"), available at www.facebook.com/records. LEORS serves as an essential bridge between Meta and LEAs by allowing LEAs to submit, track, and follow up on their requests, and receive corresponding data. Once data is produced, LEORS allows the authorised LEA that has submitted the request to download data, ensuring that it reaches authorized law enforcement personnel through a secure process. Meta also provides LEAs with publicly

available guidelines (available at https://about.meta.com/actions/safety/audiences/law/guidelines). These guidelines specify the required form of the requests and how to submit the requests.

Meta works towards complying with all legally valid data requests in accordance with its policies within 72 hours of receipt, including under circumstances where the alleged perpetrator is anonymous or uses a fake account. When Meta receives an LEA request for information associated with an account located outside India, it reviews and complies with valid requests as per applicable law and its policies where the LEA has established a nexus between the identified user and India – i.e., the account has a connection to criminal activity that directly affects India.

Meta also reports potential suicide and self-harm cases to Indian LEAs. Meta uses a combination of machine learning and user reports to detect posts or live videos that may indicate someone is at risk of suicide or self-harm. Systems flag potentially concerning content for human review, allowing Meta to intervene through partnerships it has created with LEAs. For example, Uttar Pradesh has reported that Meta enabled it to save more than 1,200 lives since January 2024.

Moreover, Meta's alerts have enabled police to respond with speed, and in some instances within 9 minutes (see, e.g., https://x.com/Uppolice/status/1954931348038430963 and https://timesofindia.indiatimes.com/city/lucknow/alert-from-meta-helps-up-cops-save-life-of-a-youth-trying-to-hang-self/articleshow/123150560.cms). Meta works closely and collaborates with various Indian authorities. For example:

● Meta works and collaborates with the Indian Cyber Crime Coordination Center ("I4C"), an agency under the Ministry of Home Affairs, to address cyber crimes. Meta remains committed to working with I4C to ensure the safety of its users, including complying with takedown requests issued by I4C under Section 79(3)(b) of the IT Act.

● In cooperation with the Ministry of Home Affairs, Meta has met with various LEAs to share best practices for obtaining information from Meta for their investigations. Meta also conducted a training session for law enforcement officers of the National Investigation

Agency in Delhi and Gujarat, and with State Law Enforcement in Karnataka and West Bengal.

● Meta helped coordinate a national training workshop on Child Safety Investigations in partnership with NCMEC and I4C in June 2024.

● Meta conducts regular training with both central and state LEAs to explain its policies, programs, tools, and processes on how to request information from Meta during their investigations, consistent with published information for LEAs on Meta's website. At a meeting held on 4 December 2024 between Delhi Police and intermediaries, pursuant to the Hon'ble Delhi High Court's order dated November 13, 2024 in Shabana v. Govt. of NCT of Delhi & Ors., Meta provided a comprehensive demonstration of the LEORS and explained its standard operating procedure for handling LEA requests for user data. With respect to statistics concerning grievances submitted to Meta, Meta provides statistics concerning the reports it receives through its Indian grievance mechanism each month in its India Monthly Report, available for download at https://transparency.meta.com/reports/regulatory-transparency-reports/, consistent with its obligations under the IT Rules. Meta's monthly reports break down such statistics by category, including, for example, "Content showing me in nudity/partial nudity or in a sexual act", "Bullying or Harassment", and "Inappropriate or Abusive Content".

7.15 In response to the following observation of the Committee-

(i) Online harassment, trolling and identity theft Abuse, threats, fake profiles and identity theft have become common on social media. KYC should be made mandatory on all social media platforms and a quick complaint redressal mechanism should be established.

(ii) Deepfakes, mod photos, and revenge porn AI-based technology is used to distort the image of women and blackmail them and harass them. The government should make a law to prevent deepfakes, implement a safety filter on social media and set up a fast-track cyber court for such cases.

(iii) Control over dating and gaming apps Women and girls are lured into the trap through tempting offers, fake rewards and chatting. There should be strict monitoring on these

apps, age verification should be mandatory and only licensed companies should be allowed.

MeitY has stated as under:-

The Ministry of Electronics & Information Technology (MeitY) has taken a note of these developments and has been undertaking regular consultations with various stakeholders including the Ministries/Departments/Commissions as well as the intermediary platforms/social media platforms and the industry bodies to implement the various provisions of the Information Technology Act, 2000 ("IT Act") and the rules made thereunder along with regular monitoring of compliances made by the intermediary platforms. Simultaneously, MeitY regularly examines the existing statutory provisions and need for strengthening the legal framework, as applicable.

7.16 As regards the existing statutory provisions, MeitY would like to emphasize about the provisions under the IT Act and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021") along with other criminal laws such as the Bharatiya Nyaya Sanhita 2023 ("BNS"), The Indecent Representation of Women (Prohibition Act), 1986, The Young Persons (Harmful Publication) Act, 1956, The Protection of Children from Sexual Offences Act, 2012 ("POCSO") and any other extant laws to regulate and monitor obscene, indecent, vulgar and slanderous content in digital and social media platforms. An elaborate description is being provided below for more clarity for the kind perusal of the Committee on Empowerment of Women (COMWOMEN).

(I) Information Technology Act, 2000 (IT Act)

The Indian cyberspace is primarily regulated through the IT Act and the rules thereunder. As the principal legislation regulating digital platforms and online activities, the IT Act provides the legal foundation for ensuring accountability of intermediaries and safeguarding users from a range of cyber offences. There are 18 sections under the IT Act which cover various forms of cyber offences, out of which 6 offences are non-bailable and 12 offences are bailable.

The IT Act provides for punishment against various offences considered as cybercrimes such as identity theft, cheating by personation, violation of privacy, publishing/transmitting material that is obscene/ containing sexually explicit act, etc., depicting children in

sexually explicit act/transmitting/ browsing child sexual abuse material, cyber terrorism, non- compliance with the direction for blocking access of information by public on certain grounds like public order, national security, etc.

To counter the criminal offences in the nature of obscenity and sexually explicit content using a computer resource that includes any social media platform, sections 67, 67A and 67B of the IT Act provide punishment for publishing or transmitting material that is obscene, containing sexually explicit act, etc., and depicting children in sexually explicit act, etc. in electronic form, respectively. Any offence under section 67 is punishable with imprisonment up to three years and with fine up to five lakh rupees on first conviction and five years and with fine up to ten lakh rupees on subsequent conviction and is a cognizable offence, whereas, offences under sections 67A and 67B are punishable with imprisonment up to five years and with fine up to ten lakh rupees on first conviction and seven years and with fine up to ten lakh rupees on subsequent conviction and are cognizable offences. Section 66E of the IT Act provides punishment for violation of privacy that prescribes that the intentional capture, publishing, and/or transmission of the image of the private area of any person without his or her consent, shall be a punishable offence with imprisonment up to three years or with fine up to two lakh rupees or both.

Further, for the purpose of defining offences, the IT Act and the rules made thereunder do not distinguish between any information that is synthetically generated using Artificial Intelligence ("AI") tools or any other technology and those which are generated by users themselves. Therefore, where any information falls within the scope of sections 66E, 67, 67A and 67B or any other sections of the IT Act dealing with cyber offences related to unlawful information, any person/user may make complaint before the police or/and report a grievance to the Grievance Officer of the concerned intermediary on whose platform such unlawful information is being made available to the public. Upon receipt of such request, the police may investigate the matter and initiate prosecution. In the case of an Appropriate Government Order, Court order or grievance, the intermediary is required to act expeditiously and in any case within the timelines prescribed under the IT Rules, 2021. The intermediaries are also required to make reasonable efforts by themselves, and to cause their users to not host, display, upload, modify, publish, transmit, store, update or share any information which are categorised as unlawful, in violation of the extant laws.

Regarding restriction of online content which are unlawful in nature (that includes information that is obscene, pornographic, invasive of another's privacy), the IT Act provides for following two routes:

i. Section 69A (power of issuing blocking direction): Further, section 69A of the IT Act provides power to the Central Government to issue directions for blocking for access of information through any computer resource if it is necessary or expedient to do so in the interest of sovereignty and integrity, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above. Based on the request from various nodal officers appointed in various organisations, the Designated Officer in MeitY issues directions for blocking for access of information online under section 69A of the Information Technology (IT) Act, 2000. MeitY follows the due process as provided in the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. Therefore, any unlawful information which is against the interest of sovereignty and integrity, defence of India, security of the State, friendly relations with foreign States or public order or incites to the commission of any cognizable offence relating to above, can be ordered for blocking for access under section 69A.

ii. **Section 79 (Intermediary regulation):** Section 79 of the IT Act regulates all intermediaries including social media intermediaries and ensures that the intermediaries—

a. Observe the due diligence obligations & guidelines as prescribed by the Central Government,

b. Ensure that they do not conspire or abet or aid in the commission of an unlawful act, otherwise they shall be unable to claim exemption from liability under section 79(1) of the IT Act

c. expeditiously remove any information that is being used to commit an unlawful act, upon receiving a court order, or on being notified by the appropriate Government or its agency.

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

To protect users in India and the Indian internet at large from the emerging harms emanating from the misuse of technologies including AI and to ensure accountability towards law of the land, MeitY in exercise of the rule-making powers given under sections 69A, 79 read with section 87 of the IT Act and after extensive public consultations with relevant stakeholders, has notified the IT Rules, 2021 on 25.02.2021 which was subsequently amended on 28.10.2022 , 6.4.2023, 22.10.2025 and 10.02.2026

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. The Rules also provide code of ethics, procedures and safeguards in relation to Digital Media to be followed by publishers of news & current affairs and also online curated content providers. The IT Rules, 2021 have two segments:

i. Intermediary Guidelines (Part-II of the Rules, except rule 5*) administered by MeitY and Appropriate Government

ii. Digital Media Ethics Code (Part-III of the Rules) administered by the Ministry of Information & Broadcasting ("MIB") in line with the distribution of subjects under the Government of India (Allocation of Business Rules), 1961 ("AOBR").

* Rule 5 in Part-II is related to due diligence to be observed by an intermediary in relation to news and current affairs content made available on their platform by such publishers and shall be administered by MIB, Govt. of India.

The IT Rules, 2021 have objective of enhancing online safety of users, particularly women & children by empowering them to exercise their rights towards safety, trust and modesty by enabling them to report grievances against various online harms and offences which are violative of any extant law and seek time-bound redressal from the intermediaries including social media intermediaries concerned whose computer resources are misused for hosting, publishing or sharing, uploading, etc. The IT Rules, 2021 may be accessed at the following link: https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_151780

7324077&type=rule&filename=information_technology_(intermediary_guidelines_and_digital_media_ethics_code)_rules,_2021_(updated_06.04.2023)-.pdf

(III) Regulation of Intermediaries under the IT Rules, 2021

Rule 3(1)(b) of the IT Rules, 2021 casts specific due diligence obligations on intermediaries, including social media intermediaries to make reasonable efforts by themselves and to cause the users of their computer resource to not host, store, transmit, display or publish, etc. any such information that is categorised as unlawful under the IT Rules, 2021 and violative of any law for the time being in force. Such unlawful information comprises any information that, among other things, is obscene, pornographic, paedophilic, invasive of another's privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, or promoting enmity between different groups on the grounds of religion or caste with the intent to incite violence, or harmful to child or that is relating or encouraging money laundering or gambling, or that is misinformation, patently false information, untrue or misleading in nature, or that threatens the unity, integrity, defence, security or sovereignty of India, public order, or that violates any law for the time being in force (that includes POCSO, BNS, etc.). Therefore, where any information falls within the categories mentioned in Rule 3(1)(b) of the IT Rules, 2021, any user may make a request to the Grievance Officer of the concerned intermediary on whose platform such unlawful information is made available to the public. While making reasonable efforts, intermediaries are required to ensure their accountability that includes their expeditious action towards removal of the unlawful information categorised under the IT Rules, 2021 or on the basis of grievances received against any such unlawful information within the timelines prescribed under Rule 3(2) of the IT Rules, 2021. In case of failure of the intermediaries to observe the legal obligations as provided in the IT Rules, 2021, they shall be liable for consequential action or prosecution as provided under any law for the time being in force.

Various provisions of the IT Rules, 2021 that focus on enhanced safety of women and children include inter alia the following:

a. Prohibiting transmission of unlawful information violative of Rule 3(1)(b) of the IT Rules, 2021:

Rule 3(1)(b) of the IT Rules, 2021 restricts eleven types of content on the Indian Internet available on the intermediary platform. Intermediaries are required to ensure that their

users do not use their platforms for sharing or transmitting content that violates Rule 3(1)(b) and other laws and that their terms of use expressly restrict use of eleven types of unlawful information which inter-alia include the following.

• Rule 3(1)(b)(ii): Information that is obscene, pornographic, invasive of another's privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, or any information that is relating or encouraging money laundering, or promoting hate speech etc. [Obscenity/ Hate speech/ Harassment/ money laundering]

• Rule 3(1)(b)(iii): Information that is harmful to child [child safety]

• Rule 3(1)(b)(v): Information that deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates misinformation, patently false information, untrue or misleading in nature. [Misinformation/ Deepfakes]

•Rule 3(1)(b)(vi): Information that impersonates another person. [Impersonation/Deepfakes]

• Rule 3(1)(b)(vii): Information that threatens the unity, integrity, defence, security or sovereignty of India, public order, etc.

• Rule 3(1)(b)(xi): Information that violates any laws for the time being in force (such as, BNS, POCSO, etc.).

b. Immediate termination of user account engaged in unlawful activity against violation of Rule 3(1)(c) of the IT Rules, 2021:

Rule 3(1)(c) of the IT Rules, 2021 mandates all intermediaries including social media intermediaries that all users must be clearly informed periodically including through the terms of services and user agreements of the intermediary or platforms about the consequence of dealing with the unlawful information on its platform, including disabling of access to or removal of non-compliant information, immediate termination of access or usage rights of the user to their user account, as the case may be, and punishment under applicable law.

c. Time-bound removal of or disabling access to unlawful information under Rule 3(1)(d) of the IT Rules, 2021:

Rule 3(1)(d) of the IT Rules 2021 mandates the platforms to ensure expeditious action, well within the timeframes stipulated under the IT Rules, 2021 (as early as possible but

not later than 3 hours), to remove or disable access to information/content that violates the aforesaid provisions of the IT Rules, 2021, upon receipt of court orders or reasoned intimation from the Appropriate Government or its authorised agency.

d. Providing information & assistance to Law Enforcement Agencies (LEAs):

Under Rule 3(1)(j) of the IT Rules, 2021, an intermediary is required to provide information under its control or possession, or assistance well within the timeframes stipulated under the IT Rules, 2021 (as soon as possible but not later than 72 hours) to the Government agency which is lawfully authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents.

e. Respecting Constitutional rights:

Under Rule 3(1)(n) of the IT Rules, 2021, an intermediary shall respect all the rights accorded to the citizens under the Constitution, including in the Articles 14, 19 and 21.

f. Time-bound Grievance Redressal Mechanism under Rule 3(2) of the IT Rules, 2021:

Rule 3(2) of the IT Rules 2021 mandates the intermediaries to ensure expeditious action, well within the timeframes stipulated under the IT Rules, 2021 (not later than 36 hours), to resolve complaints of violation of the rules in relation to select prohibited information under Rule 3(1)(b) which are either heinous or serious in nature and, in case of a complaint by an individual or her/his authorised representative, remove within 2 hours any content which prima facie exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct (i.e. breach of physical privacy and circulation of revenge pornography) or which is in the nature of impersonation or an artificially morphed images (i.e. deepfakes) of such individual.

g. Enhanced Grievance Redressal through appealing mechanism under Rule 3A –

Establishing Grievance Appellate Committees (GAC): The Government has also established GAC under Rule 3A of the IT Rules, 2021 to allow users and victims to appeal

online on www.gac.gov.in against decisions taken by the Grievance Officers of intermediaries in case they are dissatisfied with the decision of the Grievance Officer in case of legal violations including obscenity, vulgarity, misinformation and deepfakes or where the Grievance Officers fails to redress the grievances from users or victims or an individual or any person on his behalf within the timelines prescribed under the IT Rules, 2021.

h. Enabling traceability of the first originator of unlawful information in India on specific grounds upon receipt of lawful order under Rule 4(2) of the IT Rules, 2021:

Rule 4(2) of the IT Rules 2021 prescribes that the significant social media intermediaries (SSMI) (i.e., social media intermediaries having 50 lakhs or above registered user base in India) shall cooperate with Law Enforcement Agencies (LEA) for prevention, detection, investigation, prosecution or punishment by enabling identification of the first originator of information related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material (CSAM).

i. Deployment of automated tools under Rule 4(4) of the IT Rules, 2021 to proactively identify and remove unlawful information and curb their virality:

Rule 4(4) of the IT Rules, 2021 requires SSMI to endeavour deployment of automated tools or other 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 Rule 3(1)(d) of the IT Rules, 2021 in accordance with the clause. Rule 4(4) also requires that the SSMI shall display a notice to any user attempting to access any information included under this sub-rule stating that such information has been identified by the intermediary under the categories referred to in the sub-rule.

j. Appointment of designated officers based in India and publishing physical address to be in India by SSMI under Rule 4(1) of the IT Rules, 2021 to assist in enforcement of rules & laws of the land: Rules 4(1) and 4(5) of the IT Rules, 2021 require SSMI to appoint a

Chief Compliance Officer, a Resident Grievance Officer and a nodal contact person, all to be residents in India; and have a physical contact address to be in India so as to make them accountable for speedy law enforcement and compliance with the IT Act and rules made thereunder.

k. A significant social media intermediary is also required to enable users who register for their services from India, or use their services in India, to voluntarily verify their accounts by using any appropriate mechanism, including the active Indian mobile number of such users, and where any user voluntarily verifies their account, such user shall be provided with a demonstrable and visible mark of verification, which shall be visible to all users of the service

l. Rule 7 of the IT Rules, 2021 provides that in case of failure of the intermediaries to observe the legal obligations as provided in the IT Rules, 2021, the provisions of section 79(1) of the IT Act shall not be applicable to such intermediaries (i.e., the intermediaries shall be liable for that information, data, or communication link made available or hosted by him under section 79 of the IT Act) and shall be liable for consequential action or prosecution as provided under any law for the time being in force.

IT Rules, 2021– Timelines for intermediaries:

Sl. No.	Obligation on Intermediaries	Timelines	Prescribed under Rule
1.	Acknowledgement of grievance	Within 24 hrs	Rule 3(2)(a)
2.	Removal of information/ link relating to unlawful information under Rule 3(1)(b) [except sub-clauses (i), (iv) and (xi)] against complaint	Within 36 hrs	Rule 3(2)(a)(i)- 1st proviso
3.	Response to Grievance [for any matter other than Rule 3(2)(a)(i)-1st proviso]	Within 7 days	Rule 3(2)(a)(i)
4.	**Removal/ disabling of content which exposes the private area of individual or any impersonated content including artificially morphed images (e.g. deepfakes) against complaint**	**Within 2 hrs**	Rule 3(2)(b)
5.	**Content removal on receipt of court order or reasoned**	**As early as possible but not**	Rule 3(1)(d)

	intimation from Appropriate Government or its agency	**later than 3 hours**	
6.	**Provide information under control or possession of intermediary concerned, or assistance to the authorised Government agency**	**Within 72 hours of the receipt of an order**	Rule 3(1)(j)
7.	Preservation of information and associated records relating to removal/ disabling of access to such information	For 180 days or as may be required	Rule 3(1)(g)
8.	Retaining user's registration information after cancellation or withdrawal of his registration	For 180 days	Rule 3(1)(h)

7.17 **Steps taken by the Government for Grievance Appellate Committee (GAC)**

To ensure that Internet in India is Open, Safe and Trusted and Accountable, the Central Government after extensive public consultations with relevant stakeholders has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021") on 25.02.2021 which was subsequently amended 28.10.2022 and 6.4.2023.

The IT Rules, 2021 cast specific legal obligations on intermediaries, including social media intermediaries and platforms, to ensure their accountability towards safe & trusted Internet including their expeditious action towards removal of the prohibited information under Rule 3(1)(b) including online safety of users, particularly women & children.

In case of failure of the intermediaries to observe the legal obligations as provided in the IT Rules, 2021, they lose their safe harbour protection under section 79 of the IT Act and shall be liable for consequential action or prosecution as provided under any law for the time being in force.

The Rule 3A of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provides for the establishment of Grievance Appellate Committee with its composition and empowers it for reviewing and adjudicating grievances ensuring fair and transparent resolution of appeals. As per the rule, the composition of each GAC consists of a chairperson and two whole time members to be

appointed by the Central Government, of which one is to be an ex-officio and two are to be independent members. GAC function as adjudicatory body as its authority is derived from the amended IT Rules, 2021.

Subsequently, MeitY established three Grievance Appellate Committees (work distributed on the basis of classification of the information covered under clause (b) of sub-rule (1) and clause (b) of sub-rule (2) of rule (3) of the IT Rules) comprising of 1 chairman and 2 members for a period of three years alongwith secretariat staff comprising of Manager, Assistant Managers and Legal officer to support the work. Year wise appeals statistics is as under:

S. No.	Head	2023	2024	2025	Total
1	Appeal Received	374	1927	1715	4016
2	Disposed	249	1176	618	2043
3	Under process	0	0	291	291
4	Rejected*	125	751	806	1682

*Rejected appeals are those which do not fall within the purview of the Grievance Appellate Committee (GAC). Such appeals are reviewed and appropriately responded to, informing the appellant to approach the relevant forum or appropriate authority for redressal of their grievance.

8. Inter-Ministerial and Inter-State Coordination

8.1. The broad framework of allocation of work to various Ministries related to Cyber Security

The Ministry of Electronics and Information Technology is the nodal Ministry for electronics and information technology and deals with the Information Technology Act. ~~and~~ The Information Technology Act provides provisions for some of the cyber-related crimes, and also deals with the issues of cyber security. In the year 2024 vide gazette notification dated on 27th September 2024, the Government of India (Allocation of Business) Rules were amended, and the subjects related to the cyber security, as in the IT Act, was allocated to the Ministry of Electronics and Information Technology. The

matters related to telecom networks were allotted to the Department of Telecommunication. The matters related to cyber-crime have been allocated to the Ministry of Home Affairs, and the overall coordination and strategic direction for cyber security is with the National Security Council Secretariat. This is the broad framework of allocation of work to various Ministries. Further investigation and their trial in the courts is facilitated by the law enforcement agencies. Usually, the State Police or the other Police agencies will carry out this activity.

8.2 In response to the question, How the Government ensures proper synergy in dealing with cyber security coordination with law enforcement agencies? MHA submitted that I4C is primarily a coordination agency and has set up coordination mechanisms through various channels. Some of them are as follows:

JCCT: I4C has established 7 JCCT (Joint Cybercrime Coordination Team) across country which covers all States/UTs. LEA Nodal Officer from each State/UT, who deals in cybercrime and cyber security, is the part of JCCT. Contact details including Emails and Phone Numbers are available to connect with them in any matter pertaining to that State/UT.

Cyber Commandos: I4C is imparting special training through technical institutes to the selected officers from LEAs across the country to enhance their capabilities to perform cyber security related duties. Their data base is available with I4C and they can be contacted in case of any cyber security issue arises in any State/UT.

SAMANVAYA: SAMANVAYA platform provides several functionalities which can help in coordination; Crime and Criminal Infrastructure Mapping through Pratibimb, Cybercrime Inter -State (Police Station 2 Police Station) Assistance Request, Banking Data and CCTV Footage Requests, SIM and Device Blocking, Repository of Cybercriminal Interrogation Reports, Interstate crime Linkage Analysis, Threat Intelligence Sharing and others.

Informal Channels: WhatsApp group of LEAs are also available through which information is shared .

CYMAC: Ministry of Home Affairs (MHA) has formed CyMAC (Cyber Multi Agency Centre) under the MAC (Multi Agency Centre) platform on 22.01.2025 with the objective to effectively address cybersecurity threats, cyber espionage, misuse of emerging

technologies against national security and similar concerns. The stakeholders onboarded on CyMAC are: Intelligence Bureau, Indian Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), National Informatics Centre (NIC), Indian Cyber Crime Coordination Centre (I4C), Ministry of Communications (DoT), etc. CyMAC has been formed to streamline efforts by coordinating the gathering & dissemination of intelligence to prevent, detect and disrupt cyber threat/incidents, analyse cyber threat / incidents for attribution of attacks and assist in responding to incidents by suggesting mitigation strategies and recovery processes.

9. International Issues & Cooperation

9.1 The field of cybercrime knows no boundaries and at times victims are targeted from across the national borders. Understanding the nature of cybercrime, I4C MHA has led the Indian delegation to the UN Convention against Cybercrime. This convention has been adopted by the UN General Assembly and is likely to be signed by various countries in 2025. This will provide a global framework for cooperation in the area of cybercrime. The Convention includes provisions for:

a) Enhancing international cooperation

b) Protecting personal data and privacy

c) Promoting public awareness and education

d) Technical assistance to countries that lack adequate infrastructure

e) Addressing illegal interception, money laundering, hacking, and online child sexual abuse material.

Once ratified, the Convention will present a robust structure to resolve issues originating from across the national borders.

9.2 Further, in response to the question- *What are the major challenges currently faced by Indian law enforcement agencies in investigating and prosecuting cases of cybercrimes against women that originate from or involve foreign jurisdictions (e.g., sextortion, CSAM hosting, social media impersonation)? Whether there is a smooth mechanism of coordination between the Ministry of External Affairs and the Home Ministry to resolve the cases?* MHA submitted that - Indian law enforcement agencies face several critical challenges in investigating and prosecuting cybercrimes against women that

involve foreign jurisdictions as many of the IT Intermediaries offering services in India are located abroad with no physical presence in the country. These include:

Delayed access to data: Obtaining user data, IP logs, and evidence from global social media companies or hosting providers is often delayed, especially when the servers are located outside India. Many intermediaries respond only to requests routed through Mutual Legal Assistance Treaties (MLATs), which can take several months.

Jurisdictional limitations: Law enforcement has limited legal authority to act against perpetrators, servers, or platforms that are not physically or legally based in India. This weakens the ability to prosecute offenders in a timely manner.

Anonymity tools: Offenders commonly use VPNs, anonymisers, and dark web platforms to conceal their identities and locations, making traceability and attribution of online abuse (such as sextortion or CSEAM hosting) technically complex and time-consuming.

Non-cooperative platforms: Some foreign platforms are not fully compliant with Indian takedown or data access requests and may deny requests unless routed through formal diplomatic or MLAT channels.

Lack of real-time cooperation frameworks: There is currently no fast- track global mechanism that enables real-time cooperation between Indian LEAs and foreign digital platforms or governments, especially for emergency cases involving online sexual exploitation or impersonation.

Inter-ministerial coordination between MHA and MEA is ensured through various committees, high-level meetings and routine correspondence. Interpol channels through CBI are currently being used by various LEAs.

10. Counselling and Rehabilitation of Cyber Victims

10.1 Currently, the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs primarily focuses on strengthening technical, investigative, and forensic capabilities to combat cybercrime, including crimes targeting women and children. However, providing dedicated psycho-social support and legal aid services to victims is not within the mandate of I4C or the Ministry of Home Affairs.

The responsibility for victim support services, including psychological counselling, rehabilitation, and legal aid, largely falls under the Ministry of Women and Child Development (MWCD). MWCD supports various schemes such as One Stop Centres (OSCs), which offer integrated services including legal aid, medical assistance, counselling, and temporary shelter for women affected by violence, including cyber harassment. These centres, operational across all States/UTs, are designed to provide immediate support and are linked to the Women Helpline (181). For children, the Childline (1098) and provisions under the Juvenile Justice Act and POCSO Act enable intervention in cases involving online exploitation.

To enhance awareness and accessibility, potential victims are reached through awareness campaigns, school and college outreach programs, and government portals such as cybercrime.gov.in, where complaints can be submitted directly. While these services are institutionally available, inter-ministerial coordination remains essential to ensure that victims of cybercrime are seamlessly referred from enforcement agencies to appropriate support and rehabilitation services. Strengthening this linkage is an important area for future policy integration.

10.2 Key initiatives to support victims and enhance justice delivery as advocated by NGO presented before the Committee on 09.06.2025

i. Create a Cyber Survivor Compensation Fund dedicated to providing financial aid for survivors of cybercrimes, covering costs related to emotional trauma, reputational damage, and legal expenses.

ii. Develop uniform, nationwide protocols for the collection, preservation, and presentation of digital evidence to improve prosecution success rates and judicial efficiency.

iii. Provide accessible counseling and legal aid services tailored to the needs of women victims of cybercrime to support emotional recovery and informed legal action.

iv. Encourage collaboration between law enforcement, judiciary, and technology experts to continuously update best practices for victim support and evidence handling in cybercrime cases.

v. Cyber Rehabilitation - Partner with civil society and health institutions to provide

vi. psychosocial counselling, vocational training, and digital upskilling.

vii. Establish regional Cyber Rehabilitation Centers to support reintegration and empowerment.

11. Need For Comprehensive Cybercrime Law

11.1 Indian Legal Framework

The main legal provisions related to Cybercrime against Women and Children are as below:

a) BhartiyaNayay Samhita, 2023

- Sections 74, 75, 77, 78, 79: Deal with sexual harassment, voyeurism, and stalking, with varying degrees of punishment.
- Section 356: Deals with defamation, including online defamation.
- Section 351: Deals with criminal intimidation through anonymous communication.

b) **The Information Technology Act, 2000** includes provisions to address cybercrimes against women and children:

- Section 66C: Addresses identity theft, with penalties of up to three years in prison and fines.
- Section 66E: Covers privacy violations through unauthorized capturing or transmitting images, punishable by up to three years in prison or fines.
- Section 67 and 67A: Deal with the transmission of obscene and sexually explicit content, imposing imprisonment and fines for offenders

c) Sec 67B -Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form. **Protection of Children from Sexual Offences Act, 2012 (POCSO)**: Section 11, 12, 13, 14, 15, 16, 19, 20 of the Protection of Children from Sexual Offences Act, 2012 (POCSO) includes provisions to address cybercrimes against women and children.

d) The Indecent Representation of Women (Prohibition) Act, 1986.

11.2 Various Directions for Actions to Address Online Crimes Against Women and Children

I. National Human Rights Commission (NHRC) of India a statutory body responsible for the protection and promotion of human rights issued an advisory in 2023 on the

Protection of the Rights of Children against Production, Distribution and Consumption of Child Sexual Abuse Material (CSAM) where in it emphasised on the need for a framework for preventing and combating the production, distribution, and consumption of CSAM, safeguarding the rights and dignity of children in line with constitutional and international obligations. The key recommendations of NHRC included;

a. Legal Challenges and Addressing the Gaps:

i. Terminology Update: Replace Child Pornography' with 'Child Sexual Abuse Material' (CSAM) and define 'sexually explicit';
ii. Intermediary Definition: Include VPN, VPS, and Cloud Service Providers in the definition;
iii. Harmonization of Laws: Explore bilateral agreements for consistent enforcement across jurisdictions;
iv. International Treaty: Pursue adoption of UN draft convention on 'Countering the use of information and communications technologies for criminal purposes';
v. Enhancing Punishment: Re-evaluate punishment severity for CSAM offenses;
vi. Certificate under Indian Evidence Act: Re-evaluate the requirement for certificates in CSAM cases.

b. Monitoring and Regulating Intermediaries:

i. Use of Technology: Mandate intermediaries to deploy algorithms for proactive CSAM detection;
ii. CSAM-Specific Policy: Require intermediaries to develop and publicize CSAM- specific policies;
iii. Removal Timeframe: Ensure prompt removal of CSAM within 6 hours;
iv. Partnerships: Facilitate real-time information sharing among intermediaries;
v. Information-Sharing: Direct intermediaries to share CSAM content information with authorities;
vi. Pop-Up Messages: Implement pop-up warming messages for CSAM-related searches;

vii. Availability of Records: Ensure ISPs maintain detailed records and provide data to law enforcement;

viii. KYC Norms: Ensure compliance with KYC norms for subscribers;

ix. Domain Registration: Mandate KYC compliance for domain registration;

x. Quarantining Posts: Require mandatory quarantining of posts for CSAM detection.

c. Detection, Investigation, and Monitoring of CSAM:

xi. Specialized Police Units: Establish specialized state and central police units for CSAM investigation;

xii. Nodal Point: Central police unit to act as a nodal point for collaboration and coordination;

xiii. Database: Create a national database of CSAM and expand existing databases;

xiv. Use of Technology: Utilize technological methods for offender identification and victim alert;

xv. Forensic Investigators: Increase the number of forensic investigators proficient in handling CSAM cases;

xvi. General Consent to CBI: Simplify the process for CBI investigation consent.

d. Capacity Building, Sensitization, Awareness, and Victim Support:

xvii. Training Courses: Develop training courses for LEAs, prosecutors, and judges;

xviii. Awareness Programs: Conduct awareness programmes for parents, children, and educators;

xix. Cyber Curriculum: Incorporate cyber safety education into school curriculums;

xx. Psycho-Social Support: Provide support services and rehabilitation opportunities for CSAM survivors;

xxi. Vernacular Language Lexicon: Translate cybersecurity terminology and CSAM search terms into vernacular languages;

xxii. SMS Alerts: Implement recurring SMS alerts cautioning users about CSAM.

II. Hon’ble Supreme Court of India’s judgement in Just Rights for Children Alliance case:

The Supreme Court of India delivered a landmark judgment on September 23, 2024, in the case of Just Rights for Children Alliance &Anr. v. S. Harish & Ors. (Criminal Appeal Nos. 2161–2162 of 2024), significantly strengthening the legal framework against “Child Sexual Exploitative and Abuse Material” (CSEAM) in the digital realm. The case originated from an appeal by the Just Rights for Children Alliance, a coalition of NGOs dedicated to child protection, challenging a Madras High Court decision that had quashed criminal proceedings against S. Harish. The High Court had ruled that mere possession or viewing of child pornography did not constitute an offence under Section 67B of the Information Technology (IT) Act, 2000, or Section 15(1) of the Protection of Children from Sexual Offences (POCSO) Act, 2012.

The Supreme Court overturned the High Court's decision, holding that the **mere possession, downloading, or viewing** of child sexual exploitation material (CSEM) is a punishable offence under both **Section 15 of the POCSO Act** and **Section 67B of the IT Act**, regardless of intent to distribute or publish.

The judgment clarified that online platforms and intermediaries are obligated under **Section 79 of the IT Act** and under **Rule 11** of the **POCSO Rules 2020** to exercise due diligence, promptly remove CSEAM, and report such content to Indian authorities. Reporting solely to international bodies does not absolve them of these responsibilities. The directions of the Hon’ble Court to the intermediaries are elucidated below;

1. The intermediaries should be made more accountable for CSEAM content on their platforms.
2. They should mandatorily flag such content and take efforts on pulling down such content - proactively as well as on the information given by LEAs.
3. They should report CSEAM content to local LEAs, Special Juvenile Police Unit (SJPUs), Cyber Crime portal (Rule 11 of POCSO Rule 2020) for taking necessary enforcement action.

4. The report to local LEAs, SJPUs, Cyber Crime portal shall include the details of the device in which such pornographic content was noticed and the suspected device from which such content was received.

11.3 The word intermediary has been defined in Section 2(1)(w) of the Information Technology Act 2000. Section 79 of the Act provides an exemption from liabilities if intermediaries have adopted proper due diligence while performing their activities. This is broadly called the **"safe harbour" provision.** However, this provision cannot be invoked if adequate due diligence with Child Sexual Exploitative & Abusive Material on their page is not put in the accountability bracket.

11.4 Presently, the social media intermediaries are reporting the CSEAM contents to the National Centre for Missing & Exploited Children (NCMEC), an American NGO. NCRB (now I4C) has signed an MOU with NCMEC for sharing the cyber tip-lines (CSEAM content shared by the intermediaries linked to Indian Geography), and the same is being shared with the concerned State/UT authorities through NCRP for action. The Hon'ble court has acknowledged the MOU between NCRB and NCMEC. However, the court has observed 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."* This is best explained as intermediaries taking the easy path of only flagging such content, thereby reaching NCMEC and not taking the timely onus of reporting this content to local LEAs, who can ensure immediate action/enforcement. The Rule 11 of the POCSO Rule 2020, read as follows:

***Rule 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 materialincluding 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 endeavours to create widespread awareness about the procedures of making such reports from time to time.

11.5 The Hon'ble Court categorically stated that "**due diligence includes not only removal of child pornographic content but also making an immediate report of such content to the concerned police units/cybercrime portal in the manner specified under the POCSO Act and the Rules thereunder**". The judgement re-emphasised on the criminality of non-reporting by stakeholders.

Thus, Sections 19 & 20 of the POCSO Act 1912, Rule 11 of the POCSO Rule 2020 and the directions of the Hon'ble Supreme Court, obligate the Intermediaries to report, remove CSEAM and also hand over the necessary material, including the source from which CSEAM material has originated, to the SJPU or local police or cyber-crime portal (cybercrime.gov.in).

11.6 Various provisions of the IT Rules, 2021 that focus on enhanced safety of women and children include inter alia the following:

i. Prohibiting transmission of unlawful information violative of Rule 3(1)(b) of the IT Rules, 2021:

- Rule 3(1)(b) of the IT Rules, 2021 prohibits eleven types of content on the Indian Internet available on the intermediary platform. Intermediaries

are required to ensure that their users do not use their platforms for sharing or transmitting content that violates Rule 3(1)(b) and other laws and that their terms of use expressly restrict use of eleven types of unlawful information which inter-alia include the following.

- Rule 3(1)(b)(ii): Information that is obscene, pornographic, invasive of another's privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, or any information that is relating promoting hate speech etc. [Obscenity/ Hate speech/ Harassment]
- Rule 3(1)(b)(v): Information that deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates misinformation, patently false information, untrue or misleading in nature. [Misinformation/ Deepfakes]
- Rule 3(1)(b)(vi): Information that impersonates another person. [Impersonation/ Deepfakes]
- Rule 3(1)(b)(xi): Information that violates any law for the time being in force. [E.g., Indecent Representation of Women (Prohibition Act), 1986; Bharatiya Nyaya Sanhita, 2023, etc.]

ii. Immediate termination of user account engaged in unlawful activity against violation of Rule 3(1)(c) of the IT Rules, 2021:

Rule 3(1)(c) of the IT Rules, 2021 mandates all intermediaries including social media intermediaries that all users must be clearly informed periodically including through the terms of services and user agreements of the intermediary or platforms about the consequence of dealing with the unlawful information on its platform, including disabling of access to or removal of non-compliant information, immediate termination of access or usage rights of the user to their user account, as the case may be, and punishment under applicable law.

iii. Time-bound removal or takedown of unlawful information under Rule 3(1)(d) of the IT Rules, 2021:

Rule 3(1)(d) of the IT Rules 2021 mandates the platforms to ensure expeditious action, well within the timeframes stipulated under the IT Rules,

2021 (as early as possible but not later than 36 hours), to remove or disable access to information/content that violates the aforesaid provisions of the IT Rules, 2021, upon receipt of court orders or notice from the Appropriate Government or its authorised agency or upon receipt of complaint made by the impersonated individual or person authorised by him in this behalf (within 24 hours).

iv. Providing information & assistance to Law Enforcement Agencies (LEAs):

Rule 3(1)(j) of the IT Rules, 2021 mandates the intermediaries to provide information under their control or possession, or assistance well within the timeframes stipulated under the IT Rules, 2021 (as soon as possible but not later than 72 hours) to the Government agency which is lawfully authorized for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents.

v. Time-bound Grievance Redressal Mechanism under Rule 3(2) of the IT Rules, 2021:

Rule 3(2) of the IT Rules 2021 mandates the intermediaries to ensure expeditious action, well within the timeframes stipulated under the IT Rules, 2021 (not later than 72 hours), to resolve complaints of violation of the rules in relation to select prohibited information under Rule 3(1)(b) which are either heinous or serious in nature and, in case of a complaint by an individual or her/his authorized representative, remove within 24 hours any content which prima facie exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct (i.e. breach of physical privacy and circulation of revenge pornography) or which is in the nature of impersonation or an artificially morphed images (i.e. deepfakes) of such individual.

vi. **Enhanced Grievance Redressal through appealing mechanism under Rule 3A – Establishing Grievance Appellate Committees (GAC):**

The Government has also established GAC under Rule 3A of the IT Rules, 2021 to allow users and victims to appeal online on www.gac.gov.in against decisions taken by the Grievance Officers of intermediaries in case they are dissatisfied with the decision of the Grievance Officer in case of legal violations including obscenity, vulgarity, misinformation and deepfakes or where the Grievance Officers fails to redress the grievances from users or victims or an individual or any person on his behalf within the timelines prescribed under the IT Rules, 2021.

vii. **Deployment of automated tools under Rule 4(4) of the IT Rules, 2021 to proactively identify and remove unlawful information and curb their virality:**

Rule 4(4) of the IT Rules, 2021 requires SSMI to endeavour deployment of automated tools or other 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 Rule 3(1)(d) of the IT Rules, 2021 in accordance with the clause. Rule 4(4) also requires that the SSMI shall display a notice to any user attempting to access any information included under this sub-rule stating that such information has been identified by the intermediary under the categories referred to in the sub-rule. This would help mitigating the concerns of viralty happened through social media platforms.

viii. **Appointment of designated officers based in India and publishing physical address to be in India by SSMI under Rule 4(1) of the IT Rules, 2021 to assist in enforcement of rules & laws of the land:**

Rules 4(1) and 4(5) of the IT Rules, 2021 require SSMI to appoint a Chief Compliance Officer, a Resident Grievance Officer and a nodal contact person, all to be residents in India; and have a physical contact address to be in India so as to make them accountable for speedy law enforcement and compliance with the IT Act and rules made thereunder.

ix. Loss of safe harbour against failure to comply by the intermediaries:

Rule 7 of the IT Rules, 2021 provides that in case of failure of the intermediaries to observe the legal obligations as provided in the IT Rules, 2021, they lose their safe harbour protection under Section 79 of the IT Act and shall be liable for consequential action or prosecution as provided under any extant law.

11.7 In response to the question- 'In view of overlapping and outdated legal provisions, does the MHA plan to initiate or support the formulation of a unified and comprehensive cybercrime legislation addressing gender-specific harms in the digital space?' MHA in a written statement submitted that-

Cybercrimes, including gender-specific harms, are presently addressed through existing laws such as the Information Technology Act, 2000, BNS 2023, and other special legislations like the POCSO Act, 2012 and the Indecent Representation of Women (Prohibition) Act, 1986. Subject of "Issues related to Cybercrime" was allocated to MHA in AoBR in September 2024. **While there is no current proposal from I4C, MHA, for a unified cybercrime legislation, the Ministry of Home Affairs, is continuously assessing legal and policy gaps and supporting capacity building and inter-agency coordination to address emerging cyber threats, including those targeting women.**

11.8 Further, MHA submitted that the existing legal framework is anchored in the Information Technology Act, 2000, along with evolving rules like the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Coupled with provisions under the new criminal laws 2023, the framework addresses a wide range of cyber offences. However, recognizing the dynamic nature of technology and emerging threats, the Government continuously reviews the law for alignment with global best practices. The Ministry of Home Affairs, through mechanisms like the I4C, regularly suggests procedural improvements, enhanced coordination mechanisms, and capacity-building initiatives rather than structural changes to the IT Act itself. This reflects a proactive approach, ensuring the legal regime remains both effective and responsive without immediate need for major legislative overhaul. Further, under Section 78 of the IT Act, 2000, the power to investigate cyber offences currently vests with police officers not below the rank of

Inspector. However, given the increasing volume and complexity of cybercrime cases, the Ministry has proposed a critical amendment to delegate investigative powers to Sub-Inspectors, thereby enhancing responsiveness and efficiency in law enforcement. This proposal aligns with the broader objective of improving access to justice and expediting cybercrime investigations across jurisdictions. Subject of “Issues related to Cybercrime” was allocated to MHA in AoBR in September 2024. New legislations may be considered at an appropriate time.

PART-II

Observations/Recommendations

1. Introductory

India's rapid digital expansion has undeniably improved connectivity and access but has simultaneously exposed women and children to escalating cyber risks. The Committee note with concern that the proliferation of smartphones, social media usage, online payments, and digital dependency has by default created a landscape where cyber offences such as cyberstalking, sextortion, impersonation, financial fraud, child sexual exploitation, and non-consensual intimate imagery are rising at an alarming pace. NCRB data reflecting a nearly 239 percent increase in cybercrimes against women and multi-fold rise in cases involving children between 2017 and 2022 underscores the seriousness of the situation. The Committee perceive that the exponential surge in complaints recorded on the National Cybercrime Reporting Portal (NCRP) indicates growing awareness as well as institutional action but there are cases of under-reporting driven by fear, stigma, and limited digital literacy, particularly among young girls, rural women, and socio-economically vulnerable groups.

The Committee observe that new-generation technologies such as Generative AI, IoT devices, machine learning, and 5G, while leapfrogging ease of life, have created sophisticated avenues for exploitation as well. Deepfake pornography, synthetic explicit content, and AI-enabled impersonation have greatly complicated detection, takedown, and forensic tracking. Offenders increasingly leverage encrypted platforms, VPNs, cloud servers, spoofed identities, virtual numbers, and dark web infrastructure, making attribution and investigation more challenging. These rapidly evolving technological complexities always outpace regulatory, investigative, and institutional capacities and pose compelling challenges.

While it is encouraging to note that the Government has introduced frameworks under the IT Act, POCSO Act, Bhartiya Nyaya Sanhita, and cyber security mechanisms such as CERT-In, I4C, cyber forensic labs, SAMANVAYA, SAHYOG, and the NCRP, gaps persist in enforcement capability, coordinated responses, and platform accountability. The Committee find that delays in data

sharing by global digital platforms, absence of rapid cross-border cooperation mechanisms, and jurisdictional ambiguity frequently impede timely investigations and victim relief. The uneven capacities of State Police Units, shortage of trained cyber investigators, lack of real-time inter-state data sharing, and inadequate forensic infrastructure further weaken India's cybercrime response, particularly in cases involving vulnerable groups.

The Committee observe that the social and psychological consequences of cyber offences remain severe. Victims, especially women and minors, endure trauma, humiliation, fear of reputational damage, and prolonged distress. In many conservative communities, stigma acts as a daunting barrier that prevents victims from reporting offences. This silence perpetuates impunity and discourages systemic redress. The Committee are concerned that despite multiple public awareness initiatives such as Cyber Jaagrookta Diwas, digital literacy campaigns, teacher training, and the Cyber Swachhta Kendra, awareness levels on safe digital practices, legal protections, and reporting mechanisms remain critically low.

In light of these challenges, the Committee recommend strengthening India's cyber safety architecture through multi-layered interventions. Firstly, awareness programmes must move beyond campaign-based outreach to sustained, institutionalised community engagement. Frontline workers such as ASHA and Anganwadi workers, Self-Help Groups, Teachers, and youth volunteers should be trained as "Cyber Safety Ambassadors" with region-specific content in local languages. Awareness on deepfakes, sextortion, safe digital financial practices, and reporting mechanisms must be widely disseminated. Schools should integrate age-appropriate cyber hygiene and cyber rights modules into their curricula. The whole process should be designed as an organic one able to respond to the rapidly evolving environment of the cyberspace.

Secondly, the Committee recommend substantial enhancement of investigative and forensic capabilities, including expanding cyber forensic labs, strengthening real-time inter-State data exchange, and establishing automated jurisdiction-mapping tools. Police personnel require specialised and continuous training on AI-enabled crimes, deepfake detection, digital evidence handling, and victim-sensitive approaches. Dedicated units for crimes involving women and

children must be empowered with technical resources and rapid response protocols.

Thirdly, digital platforms, particularly social media, messaging, and hosting services must be held to higher accountability standards. The Committee recommend fast-tracked data-sharing frameworks, stricter and shorter compliance timelines, mandatory deployment of AI-driven detection tools, and transparent reporting of child safety and women's safety measures.

In addition to above, the Committee recommend that the Ministry may introduce age-appropriate regulations and calibrated usage limits on social media platforms to safeguard children and adolescents from adverse psychological impacts and safety-by-design standards to ensure responsible digital engagement and protect the mental wellbeing of young users.

Further, the Committee also emphasise the need for a victim-centric response system, including integrated helplines, psychological counselling, legal assistance, and faster redressal mechanisms. Stronger international cooperation agreements, improved public–private collaboration, and sustained investment in emerging technologies are indispensable for a future-ready cyber safety ecosystem that protects India's women and children effectively.

2. Expanding Public Awareness & Community Outreach

The Committee observe that despite a wide range of campaigns undertaken by the Ministry of Home Affairs (MHA) through I4C and the Ministry of Electronics and Information Technology (MeitY), cyber safety awareness among women, children and the general public remains inadequate, particularly in rural and low-digital-literacy areas. The Committee are concerned that most initiatives continue to be episodic and campaign-driven rather than institutionalized, resulting in limited recall, inconsistent penetration, and low levels of legal understanding among victims. The Committee note that women often hesitate to report cases due to stigma, lack of knowledge about the Cybercrime Helpline 1930 and the NCRP portal, and the absence of user-friendly, multilingual support. In view of these gaps, the Committee recommend that both MHA and MeitY jointly design a sustained, community-anchored national cyber safety awareness programme with dedicated

outreach through schools, colleges, Panchayati Raj Institutions, SHGs, Anganwadi and ASHA networks, CSCs and civil society organisations. Only then the psychological barriers, especially the stigmatic aspect, be breached when awareness is dovetailed with sensitivity. Awareness material covering cyber hygiene, safe digital practices, protection from online frauds, stalking, sextortion, deepfakes, and legal rights should be produced in all major Indian languages and local dialects using relatable case studies. The Committee further recommend that a structured "National Cyber Safety Week" be observed annually and that all government offices, police stations, and public-facing institutions prominently display information on 1930 and NCRP. The Committee emphasises the need for simple, accessible, audio-visual legal literacy tools, mandatory school-level cyber hygiene modules, and involvement of teachers and trained local volunteers as "Cyber Safety Ambassadors". Quizzes and simple competitions with rewards may also be designed to attract attention to the subject. The Committee expect both Ministries to put in place mechanisms for continuous monitoring, district-wise impact assessment, and feedback loops to ensure that awareness efforts ultimately translate into increased reporting, timely redressal, and enhanced digital safety for women and children.

3. Strengthening Investigation, Forensics & Law Enforcement Capacity

The Committee recognise that both MHA and MeitY have undertaken substantial initiatives such as Cyber Shakti, CyTrain, CCPWC, NCFL, State Connect, Thana Connect, Cyber Commandos, and Peer Learning Sessions to enhance the preparedness of law enforcement agencies, prosecutors, and judicial officers. However, the Committee observe that these interventions, though important, remain fragmented, uneven across States and are insufficient in scope to meet the rapidly expanding nature of cybercrimes against women. The sharp increase in cases involving various cyber offences and cross-jurisdictional digital offences demands a far more advanced, sustained and technology-driven capacity-building ecosystem.

The Committee highlight that while 24,600 personnel have been trained under CCPWC and over one lakh certificates issued under CyTrain, such figures

do not necessarily seem to translate into improved investigation outcomes. Multiple States continue to report acute shortages of skilled cyber investigators, digital forensic analysts, and prosecutors with techno-legal expertise. Training participation also remains highly variable among States/UTs, with several frontline police stations still struggling to understand digital evidence preservation, metadata extraction, VPN tracing, darknet investigations, and handling of sensitive crimes involving women. The Committee therefore stress the necessity of standardizing training quality, ensuring mandatory participation, and linking cyber-skilling to career progression across all ranks. Further, the Committee also strongly feel that along with training, sensitisation of investigative personnel about the unique situations encountered by cybercrime victims, women, to be specific, should also be given importance.

The Committee also note that forensic capacity remains a major bottleneck. Although NCFL in Delhi and the upcoming NCFL in Assam provide world-class facilities, most States lack adequate tools and manpower for deepfake detection, image enhancement, and advanced mobile forensics. With over 12,000 forensic cases handled at NCFL, the Committee are concerned that delays may worsen as case volumes grow. Accordingly, the Committee recommend the rapid establishment of additional regional forensic units, mobile cyber forensic vans, and dedicated cyber forensic consultants in every State to support swift and high-quality investigation of crimes against women. The State Governments also may be offered assistance when in need.

Further, though initiatives such as State Connect, Thana Connect, Peer Learning Sessions, and SAMANVAYA have improved coordination, the Committee finds that these platforms must be institutionalized so that every police station and district unit routinely uses them. Several States are yet to fully adopt advanced tools such as ICACCOPS, CyberTipline Case Management, OSNIT analytics, and GIS-based suspect tracking. The Committee recommends mandatory onboarding of all States/UTs, regular audits of utilization, and targeted retraining for districts demonstrating low performance.

In view of the submissions, the Committee recommends that the Ministry of Home Affairs urgently develop a National Cyber Capacity-Building Framework for women-related cybercrimes, outlining uniform standards for training content, minimum hours of annual training, certification norms, and mandatory skills for police, prosecutors, and judicial officers. The Committee also recommends the creation of a centralized repository of case studies, SOPs, investigation checklists, deepfake identification tools, and legal guidance notes accessible to all police stations through CyTrain or I4C dashboards. Continuous, modular, and specialization-oriented training, rather than one-time workshops, must be adopted to keep pace with evolving technologies.

The Committee further recommend that CyberShakti be significantly scaled up by MeitY with a dedicated vertical for training women police officers, cyber cell personnel, and women officials from social welfare departments who often interact with victims. Specialized modules on digital stalking, NCII takedown processes, safe evidence preservation, and AI-based harms should be added. The Committee emphasize that CyberShakti must transition from an introductory sensitization programme to a sustained and intensive capacity-building mechanism producing women cyber-security professionals across States/UTs.

The Committee also take note the absence of adequately trained techno-legal prosecutors and the limited exposure of judicial officers to digital evidence. In this regard. the Committee emphasize that unless prosecutors and judges understand the complexities of deepfakes, digital chain of custody, metadata, server logs, cryptocurrency trails, and international cooperation procedures, justice delivery will remain slow. The Committee therefore recommend establishing specialised prosecution units for cybercrimes against women and creating dedicated training calendars for judicial academies in collaboration with I4C. Fast-track courts dealing with women-related cybercrimes must have judges specifically trained in digital evidence and online harms. Recognizing the crucial role of prosecutors and judicial officers in delivering timely justice, the Committee recommend that MHA and State Governments jointly ensure the posting of techno-legal prosecutors in cyber cells

and women-related cybercrime units. Dedicated training calendars for judicial academies must be created in collaboration with I4C, ensuring exposure to latest trends in cyber crime. Fast-track courts for cybercrimes against women must be staffed with trained judges familiar with digital evidence complexities. The possibility of securing help of cyber professionals for the investigators, prosecutors and the Judges may also be explored.

Through these capacity-focused interventions standardized training, expanded forensic capability, institutionalized coordination, and specialized techno-legal expertise, the Committee believe that the investigative and enforcement ecosystem can be significantly strengthened, thereby improving cyber safety outcomes for women across India.

4. SOP for investigation

The Committee observe that despite the establishment of a multi-channel reporting mechanism through the National Cybercrime Reporting Portal (NCRP), the 1930 helpline, offline police stations, reporting by women remains much less than satisfactory, particularly in rural and semi-urban areas. The Committee have repeatedly highlighted during the process of examination of the subject that awareness gaps, language barriers, lack of digital literacy, hesitation due to stigma, and fear of insensitive police handling continue to deter women from lodging complaints. In this context, the Committee note that frontline police stations in Tier II/III towns and rural districts face persistent challenges in identifying, registering, and responding to cyber offences, especially those involving deepfakes, CSAM, morphing, sextortion, and online stalking. In light of these concerns, the Committee recommend that the Ministry of Home Affairs adopt a victim-centric, simplified, and uniform SOP that focuses on accessibility, confidentiality, and immediate support for women and children. Such SOPs formulated by the MHA may be shared with the States as well.

Further, the Committee find it compelling that many women are unaware of NCRP or 1930 and that digital illiteracy and limited mobile/internet access severely restrict reporting. The Committee, therefore recommend that the SOP include

provisions for assisted reporting, wherein Anganwadi centres, One Stop Centres, women helplines (181), Mahila Police Volunteers, Panchayat digital kiosks, and CSCs are designated as official assisted-reporting points. These centres must be equipped to file NCRP complaints on behalf of victims confidentially. The Committee further recommend that the portal and helpline be made available in all Schedule VIII languages, with simple interface features, audio-based guidance, and visual icons to support first-time digital users.

Another aspect that grips the attention of the Committee is the serious operational difficulties faced by police stations, as highlighted in their deliberations, particularly the lack of technical expertise, poor infrastructure, jurisdictional confusion, delays in data access from platforms, shortage of manpower, and absence of victim-sensitive approaches. Keeping this in view, the Committee recommend that the SOP clearly define minimum technical requirements for every police station, including stable high-speed internet, secure evidence storage devices, access to Sahyog, ICACCOPS, NCMEC Tipline case management tools, and OSNIT dashboards. The Committee also stresses the need for mandatory training for Station House Officers and Investigating Officers on handling sensitive digital evidence, explaining victim rights, documenting cybercrimes involving deepfakes, and applying appropriate legal sections without delay.

An important matter brought to the fore by Members is that police often hesitate to register women-related cybercrimes due to technical unfamiliarity or jurisdictional confusion. The SOP must, therefore, explicitly mandate same-day registration of complaints involving NCII, deepfake pornography, stalking, impersonation, and CSAM, irrespective of territorial jurisdiction. Such cases must be immediately categorised as "urgent" and escalated to district cyber cells. The Committee also find it imperative that the SOP prescribe a standard 24-hour timeline for initiating takedown requests through SAHYOG, especially in cases where continued online availability exacerbates harm to the woman.

The Committee also emphasise that frontline police personnel must adopt a victim-sensitive approach. The SOP should include detailed guidance on ensuring privacy during complaint intake, preventing secondary victimisation, and providing quality psychological support. Dedicated women officers or specifically trained personnel must handle these cases. In this direction, the Committee recommend that each police station maintain a confidential counselling and support protocol, including referrals to OSCs, cyber counsellors, and NGOs specialising in women's digital safety.

Clearly spelt out coordination workflows between district cyber cells, State cyber nodal officers, I4C's analytical units, and NCFLs are critical in ensuring that delays do not arise due to procedural ambiguity. The SOP shall provide for this.

The Committee appreciate the Ministry's ongoing work on a national SOP and recommend that the final version integrates clear timelines, checklists, and automated workflows to avoid subjective interpretation. In particular, the SOP should include standard formats for FIRs, evidence intake forms, platform communication templates, victim consent forms, and guidelines for interacting with intermediaries. The Committee also want that the SOP incorporate a public-facing simplified version, explaining key steps for women, parents, and guardians.

The Committee are of the firm opinion that ensuring accountability is pivotal in rendering any SOP effective. Hence, the SOP must mandate periodic compliance audits, district-wise performance dashboards, and reporting of pendency, takedown timelines, and prosecution progress for cybercrimes against women. The Committee also recommend the creation of a grievance escalation route for victims when police stations fail to act in accordance with the SOP.

Through these comprehensive SOP-focused recommendations centred on accessibility, mandatory procedures, technological readiness, and victim sensitivity, the Committee are of the considered belief that reporting, investigation, and redressal of cybercrimes against women can become significantly more timely, transparent, and effective across all regions of the country.

5. Leveraging Technological Advancements to enhance Cyber Security Frameworks

The Committee observe that the rapid expansion of the digital ecosystem has been accompanied by a corresponding rise in cybercrimes targeting women, including online harassment, cyberstalking, deepfake misuse, identity theft, circulation of non-consensual intimate imagery, and financial fraud. While recognising the efforts of the Ministry of Home Affairs (MHA) and the Ministry of Electronics & Information Technology (MeitY) through important technological interventions such as the Proactive Monitoring Tool (PMT), the National Cybercrime Reporting Portal, and the Sahyog platform for rapid takedowns, the Committee are of the considered view that far more robust, responsive, and coordinated technological upgradation is required to ensure meaningful cyber-safety for women across the country. Cybercrimes today are not only faster, more complex, and more anonymous, but also deeply consequential for the mental, emotional, and physical well-being of women. Hence, technological solutions must be strengthened, scaled, and oriented specifically towards prevention, early detection, rapid response, and long-term resilience.

The Committee recommend that MeitY and MHA jointly enhance and deploy advanced AI-driven tools such as the Proactive Monitoring Tool (PMT) for detecting Child Sexual Exploitative Abuse Material (CSEAM), Rape/Gang-Rape content, deepfakes, and morphed imagery affecting women. PMT-like capabilities such as ML-based classification, severity scoring, age estimation, and secure image-hash repositories should be expanded to cover broader forms of gendered cybercrimes. The Committee further recommend that this enhanced tool be integrated with the National Cybercrime Reporting Portal and law-enforcement workflows to ensure real-time alerts, faster assessment of incoming reports, and immediate initiation of takedown and investigation procedures.

With respect to content removal, the Committee acknowledge the utility of the SAHYOG Portal but desire for strengthening its operational scope. All major and emerging Intermediaries, including social media companies, messaging

services, cloud platforms, dating apps, and Virtual Asset Service Providers, must be mandated to integrate their systems with Sahyog for seamless, time-bound compliance. Given the recurring delays and lack of accountability from certain Intermediaries, the Committee recommend that MeitY establish A clearly enforceable timelines, automated compliance dashboards, and financial or legal penalties for non-compliance in the removal of harmful content affecting women and children. Further, the Committee find that frequent misuse of deepfake technology demands a specialised and unified "Central Deepfake Detection Infrastructure" under MeitY to support States, police units, and courts with rapid verification.

The Committee also reckon a need for serious upscaling of the technical capacity of cybercrime units at the ground level. Many district-level cyber cells remain understaffed, rely on outdated tools, and face significant delays in evidence extraction, digital forensics, and cross-platform coordination. The Committee therefore recommend urgent augmentation of manpower, modern forensic tools, cyber-intelligence platforms, and continuous technical training. Given the shortage of skilled personnel, the Committee strongly recommend for creation of a national "Cyber Volunteer–Warrior Programme" to onboard trained youth, cybersecurity graduates, and ethical-hacking talent as paid, certified contributors supporting cyber police units. This will also create a steady talent pipeline for the future. Private Sector companies may also be encouraged/incentivised to contribute towards this programme.

The Committee further want that technological reforms be complemented by a responsive, coordinated governance framework. MHA and MeitY must jointly establish a unified Cyber Safety Coordination Mechanism for Women, enabling seamless data-sharing, cross-platform action, and policy coherence across NCRP, Sahyog, PMT, Grievance Appellate Committees, and authorised agencies under the IT Act. Regular audits, performance dashboards, and gender-segregated reporting of cybercrimes should also be institutionalised. The Committee firmly believe that an integrated, technology-driven, and victim-centric cyber-safety architecture is a

sine qua non for securing the digital dignity, privacy, and safety of women across India.

6. Budget Allocation for Research & Development

The Committee find that although cybercrimes targeting women have grown exponentially manifesting in forms such as cyberstalking, online harassment, deepfakes, identity theft, non-consensual intimate imagery (NCII), and gender-based online violence, the present financial and institutional ecosystem for Research and Development (R&D) in cybercrime prevention and cyber safety of women remains inadequate and fragmented. While the Ministry of Home Affairs (MHA) supplements State/UT efforts by funding police modernization, cyber forensic capacity and CCPWC initiatives, these monetary allocations are neither proportionate to the rising complexity of technology-enabled crimes nor specifically oriented towards women-centric cyber threats. The Committee note that upto 31 March 2024, only ₹132.93 crore has been released under CCPWC for capacity building and ₹97.99 crore under Nirbhaya Fund for DNA and cyber/digital forensics, with the States/UTs utilising 100 % of the funds. But it is significant to note that these expenditures has been largely for two infrastructure-driven initiatives and not directed towards advanced research in AI-enabled threat detection, cyber forensics innovation, or predictive tools for crimes against women.

Similarly, in case of MeitY, despite a substantial cybersecurity budget of ₹782 crore in FY 2025–26, there is no dedicated funding stream for R&D on cybercrime detection and prevention technologies specifically aimed at safeguarding women, nor is there any earmarked allocation for developing deepfake detection, anti-stalking tools, automated threat-intelligence systems, proactive monitoring technologies, or AI-based alert systems which could protect women online. Further, The Committee note with alarm that there is no separate allocation for notified cyber forensic labs or Examiner of Electronic Evidence (Section 79A), especially keeping in perspective the evidence placed before the Committee regarding delays in investigation, lack of technical manpower, under-equipped cyber cells, and the urgent need for modern forensic capabilities capable of

handling AI-driven crimes. The Committee also note in this connection the concerns raised by experts and civil society organisations regarding the acute under-reporting of cybercrimes due to stigma, lack of digital literacy, inadequate victim support systems, and the limited ability of law enforcement agencies to detect, triage and investigate sophisticated cyber offences against women. It is evident that such systemic gaps can only be bridged through sustained investment in indigenous R&D, technological innovation, and the development of specialised tools tailored to the unique cyber vulnerabilities of women.

In view of the above, the Committee strongly recommend that the Government may create a Dedicated Women-Centric Cyber Safety R&D Fund within MeitY and MHA with clearly defined objectives, deliverables, and measurable outputs. This fund must exclusively support the development of advanced tools such as automated deepfake detection engines, AI-based content-scanning systems for early identification of non-consensual imagery, predictive behaviour-profiling tools for cyberstalking, multilingual cyber-safety AI chatbots, secure reporting technologies, and real-time threat-intelligence systems integrated with NCRP and I4C. The Committee further recommend for earmarking a fixed percentage of the existing Cyber Security Project Budget for women-focused R&D and mandating annual reporting on outcomes. This may also be in tune with the gender budgeting initiative of the Government.

Further, MeitY may expand R&D support beyond IITs, NITs and C-DAC to include start-ups, women-led tech innovators, academic consortia and cyber-forensic researchers working on gender-specific digital harms. Additionally, the Committee also strongly favours a separate financial window for strengthening and accrediting cyber-forensic labs under Section 79A, with funding for advanced tools, specialised training, and AI-assisted evidence examination. The Committee recommend that MHA and MeitY jointly create a multi-year roadmap to scale R&D investment, fill critical technology gaps, promote indigenous innovation, and ensure that India develops cutting-edge, proactive and globally benchmarked technological capabilities to secure women in the digital ecosystem.

7. Role of Social Media Intermediaries in Ensuring Online Safety for Women

The Committee observe that the rapid expansion of digital platforms has brought unprecedented opportunities for communication, expression and economic engagement for women, but has simultaneously exposed them to serious online harms including cyber-stalking, impersonation, deepfakes, sextortion, dissemination of intimate images, targeted harassment, trolling, threats, and exploitation through dating, gaming and matrimonial apps. While the Information Technology Act, 2000 and the IT Rules, 2021 provide a comprehensive due-diligence framework for Intermediaries, the enforcement on ground remains inconsistent, leaving women especially highly vulnerable. In view of the increasing complexity of cyber-enabled crimes and the serious psychological, social and economic impact on women, the Committee recommend that the regulatory architecture, accountability mechanisms and cooperation protocols with intermediaries may urgently be strengthened.

Further, the Committee find essential and hence recommend that all social media intermediaries and digital platforms must ensure strict compliance with Rule 3(1)(b) of the IT Rules, 2021 by proactively preventing the hosting and transmission of unlawful content, including obscene material, sexually explicit acts, morphed images, deepfakes, hate speech and gender-based harassment. The terms of service of all platforms must clearly specify these prohibitions in simple language accessible to users. Intermediaries must be directed to strengthen their internal monitoring frameworks to detect and disrupt emerging patterns of abuse, particularly against women and children.

The Committee note with concern that delays in the removal of harmful and unlawful online content continue to pose a serious threat to user safety and dignity. While acknowledging recent improvements in reducing takedown timelines under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Committee recommend that intermediaries strictly adhere to the prescribed timelines and in view of technological advancements and real-time monitoring capabilities, adopt upgraded rapid-response systems to enable

near-immediate action. Content involving intimate image abuse, impersonation, CSAM/CSEAM, and malicious deepfakes should be accorded the highest priority and removed at the earliest upon detection or reporting. To go further, the Committee recommend that MeitY conduct periodic audits of major platforms to assess compliance with these timelines and impose penalties or initiate proceedings under Rule 7 wherever compliance gaps are observed.

To strengthen accountability, the Committee recommend that the Chief Compliance Officer, Resident Grievance Officer and Nodal Officer appointed under Rule 4(1) must be made personally responsible for delays or negligence in responding to government orders or user complaints related to women's online safety. Their contact details, including physical address in India, must remain prominently available on all apps and websites.

Further, given the exponential increase in deepfakes and AI-generated sexually explicit content targeting women, the Committee recommend that intermediaries deploy advanced AI-based automated tools, as envisaged under Rule 4(4), to proactively detect, prevent re-uploading, and curb the virality of unlawful content. Such tools must include hash-matching, image-forensics, predictive monitoring and behavioural analysis for early identification of offenders. The Committee further recommend that Meity/MHA bring specific rules on deepfake governance, mandating safety filters, watermarking of AI-generated content, real-time detection systems, and severe penalties for non-compliance.

In addition to this, the Committee strongly recommend that mandatory KYC-based verification be introduced across all social media, dating and gaming platforms to curb the menace of fake profiles, impersonation and anonymous harassment. Platforms must carry out periodic re-verification and maintain high-risk flags for accounts repeatedly reported for abuse. Strict licensing norms and age-verification protocols must be established for dating and gaming apps, with penalties for platforms that fail to protect women and minors from fraudulent or coercive practices.

The Committee acknowledge and appreciate the SAHYOG Portal developed by I4C for secure, structured and time-bound communication with intermediaries. However, the Committee recommend for further strengthening of this mechanism by ensuring uniform standard operating procedures (SOPs) for all intermediaries on content removal, metadata sharing, cooperation with LEAs, and emergency response protocols. The Committee also recommend that the Government explore the creation of an Indian equivalent of StopNCII.org to empower women to hash and register their intimate images for automatic blocking across platforms.

Further, given the large volume of complaints relating to sextortion, intimate image abuse and CSAM, the Committee is strongly in favour of the I4C and State LEAs being provided with enhanced technical resources, training and analytics tools, and that intermediaries must facilitate seamless access to actionable information within the 72-hour limit under Rule 3(1)(j). The Committee also recommend creation of special cyber units within police forces, supported by digital forensic capability, to fast-track investigations in offences against women.

Recognising that many women face difficulty navigating platform-specific grievance mechanisms, the Committee recommends for strengthening of the Grievance Appellate Committees (GAC), including enhanced public awareness, simplified filing procedures, and transparent reporting on appeals related to gender-based harm, deepfakes and privacy violations.

The Committee further recommends that MeitY should examine gaps in the present legal framework, particularly concerning AI-generated content, non-consensual image sharing, online impersonation and cross-border platforms, and consider amendments to ensure greater accountability of intermediaries, including loss of safe harbour in cases of repeated non-compliance.

8. Inter-Ministerial and Inter-State Coordination

The Committee learn that cybercrimes against women have grown in volume, complexity, and severity, necessitating a far stronger, unified, and technology-driven coordination mechanism among all Ministries, States and specialised agencies to respond. While the Government has clarified the broad allocation of responsibilities—MeitY handling matters under the IT Act and social media intermediaries; the Department of Telecommunications overseeing telecom networks; the Ministry of Home Affairs responsible for cyber-crime investigation and the National Security Council Secretariat providing overarching strategic direction, the Committee find that the present coordination architecture remains disaggregated resulting in delayed investigations, information-sharing gaps and inconsistent enforcement of legal provisions, ultimately affecting women's safety online. The Committee want to highlight that the complexity of offences such as deepfake morphing, cyberstalking, identity theft, sextortion, impersonation, online radicalisation, and exploitation through dating and gaming apps demands far tighter inter-ministerial and inter-state synergy than what currently exists.

The Committee laud the initiatives taken by the Indian Cyber Crime Coordination Centre (I4C) such as the establishment of seven Joint Cyber Crime Coordination Teams (JCCTs), deployment of Cyber Commandos, operation of inter-state coordination through the SAMANVAYA platform, and the creation of CyMAC to improve real-time intelligence exchange across multiple agencies. However, the Committee observe that despite these structures, States continue to face difficulties in securing timely cooperation from social media intermediaries, obtaining critical metadata for investigation, and achieving rapid content takedown, especially in cases involving women. The Committee find it worrying that delays of even hours allow morphed images and defamatory content to go viral, resulting in irreparable trauma for victims. The Committee therefore recommend the establishment of a Unified National Cyber Coordination Grid with a specific architecture for women's Safety, integrating all Ministries, State Police Forces, CERT-In, NCIIPC, DoT, Cyber Forensic Labs, JCCTs, and social media

intermediaries onto a common, real-time, monitored communication loop for immediate response in women-related cyber-crime cases.

The Committee further recommend that MeitY, MHA, DoT, and NSCS jointly develop Standard Operating Procedures (SOPs) for inter-ministerial coordination, clearly specifying timelines, accountability points, and escalation pathways for urgent takedown orders, cross-border content reporting, access to digital evidence, device and SIM blocking, and emergency victim assistance. These SOPs must be binding on all intermediaries, State Police, and central agencies. The Committee also want to firmly emphasise that grievance redressal, including proceedings before Grievance Officers, GACs, and LEAs, must not function in silos but in a synchronised manner to ensure that women receive timely protection and justice.

The Committee note that while platforms like SAHYOG and SAMANVAYA are valuable, their usage across States is uneven, and many officials lack the training or technological familiarity to fully utilise these tools. The Committee therefore recommend a mandatory, centralised training programme for State cyber units, women-related crime cells, district-level supervisory officers, and techno-legal personnel, enabling uniform usage of I4C platforms, digital evidence procedures, cyber-forensic tools, and cross-state coordination mechanisms. Special emphasis shall be placed on cases involving deepfakes, impersonation, intimate-image abuse, and online harassment of women, where rapid digital forensics and real-time inter-agency communication are critical.

The Committee also stress upon for an uniform integration of AI-based alerts into the SAHYOG and JCCT ecosystems so that actionable intelligence reach States immediately rather than through disarrayed channels such as informal WhatsApp groups, which lack traceability and accountability.

For the sake of coordinated response, the Committee recommend the creation of State-wise Cyber Coordination Control Rooms for Women's Safety,

integrated with NCRP, 1930 helpline, and I4C systems, enabling rapid triaging of complaints and immediate escalation to social media intermediaries. To make it more effective, monthly coordination meetings must be mandated between MeitY, MHA, DoT, NSCS, and the States to review outstanding takedown requests, cross-border cooperation challenges, non-compliance by intermediaries, and deficiencies in State cyber units.

The Committee are also of the emphatically in favour of enhancing accountability among social media intermediaries by setting up a Central Compliance Review Board jointly operated by MeitY and MHA to evaluate platform-wise adherence to deadlines, responsiveness to State Police, and proactive removal of harmful content. Persistent non-compliance should attract penalties, loss of safe-harbour protection, and in extreme cases, blocking orders.

9. International Issues & Cooperation

The Committee comprehend that cybercrimes targeting women have acquired a distinctly transnational character, with perpetrators frequently operating from outside India and exploiting differences in jurisdiction, anonymity tools, and slow international cooperation channels. The Committee note in this regard that India's active participation in the drafting of the UN Convention against Cybercrime, soon to be opened for signatures, marks an important global step in addressing cross-border cybercrimes. While the Convention includes provisions for enhanced cooperation, privacy protection, public awareness, technical assistance and action against offenses such as hacking, money laundering and online child sexual abuse material, the Committee are of the view that its effectiveness will depend on the creation of robust, time-bound and enforceable mechanisms for real-time cooperation, especially in cases involving women and children.

The Committee learn as highlighted by the MHA that Indian law enforcement agencies face significant barriers when foreign jurisdictions or offshore-based intermediaries are involved. Delays in access to essential data such as user

information, transaction logs or IP details, often arise because many global platforms respond only through Mutual Legal Assistance Treaty (MLAT) mechanisms, which take several months. When digital evidence is ephemeral and crimes such as sextortion, deepfake circulation, CSAM hosting or impersonation cause immediate harm, such delays severely undermine purposeful investigations. The Committee find it worrisome that foreign platforms often fail to comply promptly with takedown requests, even in cases involving women, thereby prolonging victim distress and enabling further dissemination of harmful content.

The Committee recognise that offenders increasingly use VPNs, anonymisers, dark-web forums and cross-border payment channels to evade detection. These trends, highlighted during the Committee's interactions with experts and technical agencies, intrinsically necessitate deeper global cooperation not only for investigation but for intelligence-sharing, forensic attribution, and preventive monitoring as well.

In light of the above, the Committee recommend that the Government proactively leverage the UN Convention to establish fast-track, time-bound, cross-border assistance protocols, particularly for cases involving cybercrimes against women. India should pursue and negotiate bilateral or multilateral rapid-response agreements with countries that host major digital platforms or data centres, ensuring quicker preservation, sharing and takedown of content related to sexual exploitation, deepfakes, impersonation or financial extortion. The Committee further recommend the establishment of 24×7 cyber liaison officers in key Indian Missions abroad to coordinate with foreign authorities, expedite requests, and monitor platform-level responsiveness.

The Committee also strongly advocate that India advocate global obligations on digital intermediaries irrespective of their physical presence, to cooperate with lawful requests within defined timelines particularly in cases involving harm to women. Mechanisms for platform accountability, escalation channels for emergency assistance, and penalties for non-compliance should be formalised

under domestic law and reinforced through international agreements. The Committee further recommend scaling up of India's engagement in international cyber intelligence networks, expanding use of Interpol channels, and strengthening the capacity of I4C to serve as India's nodal point for international anti-cybercrime coordination.

10. Counselling and Rehabilitation of Cyber Victims

The Committee observe that while steady progress is being made in strengthening technical and investigative frameworks to address cybercrimes, robust systems for counselling, effective psychosocial support and rehabilitation of women victims of cyber offences remain inadequate and inconsistently accessible across States/UTs. The Committee note that women are subjected to online harassment, morphing, sextortion, identity theft, and circulation of intimate images thereby often experience severe emotional distress, social stigma, reputational harm, and economic hardship. To address these challenges, the Committee recommend the establishment of a comprehensive, coordinated and victim-centred framework that bridges existing institutional gaps in coordination with I4C, State Police, NCRP, and the Ministry of Women and Child Development (MWCD). The framework should ensure that every cyber victim particularly women who reports a complaint is automatically connected to the nearest One Stop Centre (OSC) or other MWCD-supported services for psychological counselling, legal aid, and rehabilitation with strict safeguards for confidentiality. These OSCs, Women Helpline (181), and Childline (1098) may also be strengthened with cyber-specialised counsellors and trained staff to deal with trauma arising from online abuse.

The Committee also recommend the creation of Dedicated Cyber Counselling Units within OSCs and district police cyber cells, staffed with psychologists trained in digital-trauma counselling. These units should function in close collaboration with civil society organisations, mental health institutions, and cyber-safety experts. To ensure continuity of care, the Committee want the establishment of Regional Cyber Rehabilitation Centres, offering long-term psychosocial support, digital-literacy rebuilding, vocational training, and

reintegration support for women whose livelihoods or education have been disrupted due to cyber victimisation.

Recognising the financial burden faced by many victims in seeking legal remedies, digital forensic services, and therapy, the Committee recommend that the Government establish a Cyber Survivor Compensation Fund, with clearly defined eligibility criteria, to support victims of severe cyber offences, including sextortion, identity theft, online blackmail, and circulation of private images. This fund should operate on the lines of victim-compensation schemes under existing criminal laws but tailored specifically for cybercrimes against women and children.

11. Need for Comprehensive Cybercrime Law

The Committee comprehend that cyber offences impacting women and children are presently addressed through multiple statutes, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the POCSO Act, 2012, and the Indecent Representation of Women (Prohibition) Act, 1986, supplemented by subordinate legislation such as the IT Rules, 2021. These provisions collectively cover a wide spectrum of offences—ranging from identity theft, voyeurism, stalking, defamation, deepfakes, and online harassment to Child Sexual Exploitative and Abuse Material (CSEAM), However, their dispersed nature often results in overlapping mandates, interpretational ambiguities, uneven enforcement, and procedural delays. Witnesses before the Committee have repeatedly underscored that victims, particularly women and children, face difficulty in navigating this complex legal maze, which contributes to under-reporting, delayed relief, and secondary victimisation.

The Committee further see that technological advancements such as encrypted platforms, anonymisation tools, artificial intelligence, and deepfake technologies have significantly altered the character of cyber offences. The law, however, remains largely offence-specific and incident-driven, rather than victim-centric and future-ready. Although recent judicial interventions, notably the landmark judgment of the Hon'ble Supreme Court in Just Rights for Children Alliance, have strengthened accountability of Intermediaries and clarified the

criminality of possession and non-reporting of CSEAM, the Committee are of the considered view that sustained reliance on judicial interpretation alone cannot be a substitute for a coherent legal framework.

The Committee acknowledge the efforts of the Government in strengthening Intermediary accountability through the IT Rules, 2021, expanding reporting mechanisms via the National Cyber Crime Reporting Portal, and enhancing coordination through I4C. However, evidence placed before the Committee highlight persistent gulfs in uniform enforcement across States, limited technical capacity at the cutting edge of investigation, lack of statutory backing for victim-centric services such as effective psychological counselling and rehabilitation, and inadequate integration of prevention, detection, investigation, prosecution and victim support within a single legal architecture. In this backdrop, the Committee hold the opinion that the absence of a consolidated law weakens India's ability to respond effectively to cross-border cyber offences and to harmonise domestic law with emerging international norms and treaties.

In view of the above, the Committee recommend that the Government may initiate a structured and time-bound examination towards the formulation of a comprehensive and gender-sensitive cybercrime legislation. Such a law should consolidate substantive offences relating to women and children, clearly delineate responsibilities and liabilities of Intermediaries and Service Providers, statutorily mandate victim support and rehabilitation mechanisms, strengthen reporting and evidence-handling procedures, and provide a uniform investigative framework with graded powers for law enforcement officers.

The Committee are of the firm belief that a comprehensive cybercrime law, complementing and harmonising existing statutes rather than abruptly replacing them, would significantly enhance legal certainty, enforcement efficiency, victim confidence and may also prove as deterrence. Such a legislative initiative would reflect a proactive, rights-based, and future-oriented approach, reaffirming the State's commitment to safeguarding the dignity, safety, and constitutional rights of women in the digital ecosystem.

New Delhi
17 March, 2026
26 Phalguna, 1947 (saka)

DR. D. PURANDESWARI
Chairperson
Committee on the Empowerment of Women

Annexure-I

1 Offences under the IT Act along with their penal actions

There are 18 sections which provide various types of cyber offences, out of which 12 such offences are bailable. The details are placed below–

Sr. No.	Section No.	Cyber Offence	Punishment	Bailable/ Cognizable
1	65	Tampering with computer source documents.	Imprisonment up to 3 years or fine up to 2 lakhs or both	Bailable, Cognizable
2	66	Computer related offences: Punishment for doing dishonestly or fraudulently any act cited in section 43 directly or causing any person to do so, such as unauthorised access to or use of, introducing virus to, damages to, disruption of, denial of access to, assistance to access to, wrongful charges to another person's account by tampering with, destroying, deletion or alteration of any information in, computer resource or stealing/ concealing/ destroying any computer source code.	Imprisonment up to 3 years or fine up to 5 lakh or both.	Bailable, Cognizable
3	66B	Punishment for dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years or fine up to 1 lakh or both.	Bailable, Cognizable
4	66C	Punishment for identity theft, i.e., making use of	Imprisonment up to 3 years or fine up to 1 lakh or both.	Bailable, Cognizable
5	66D	Punishment for cheating by personation by using computer resource	Imprisonment up to 3 years and fine up to 1 lakh.	Bailable, Cognizable
6	66E	Punishment for violation of privacy.	Imprisonment up to 3 years or fine up to 2 lakh or both	Bailable, Cognizable
7	66F	Punishment for cyber terrorism	Imprisonment which may extend to life.	Non-Bailable, Cognizable

Sr. No.	Section No.	Cyber Offence	Punishment	Bailable/ Cognizable
8	67	Punishment for publishing or transmitting obscene material in electronic form	1st Conviction – Imprisonment up to 3 years and fine up to 5 lakh. 2nd Conviction – Imprisonment up to 5 years and fine up to 10 lakh	Bailable, Cognizable
9	67A	Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form	1st Conviction – Imprisonment up to 5 years and fine up to 10 lakh. 2nd Conviction – Imprisonment up to 7 years and fine up to 10 lakh.	Non-Bailable, Cognizable
10	67B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	1st Conviction – Imprisonment up to 5 years and fine up to 10 lakh. 2nd Conviction – Imprisonment up to 7 years and fine up to 10 lakh.	Non-Bailable, Cognizable
11	69	Power to issue directions for interception or monitoring or decryption of any information through any computer resource (*punishment to intermediary who fails to assist the agency*)	Imprisonment up to 7 years and fine	Non-Bailable, Cognizable
12	69A	Power to issue directions for blocking for public access of any information through any computer resource. (*punishment to intermediary who fails to comply with such Government direction*)	Imprisonment up to 7 years and fine	Non-Bailable, Cognizable
13	69B	Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security. (*punishment to intermediary who intentionally or*	Imprisonment up to 1 year or fine up to 1 crore or both	Bailable, Non-Cognizable

Sr. No.	Section No.	Cyber Offence	Punishment	Bailable/ Cognizable
		knowingly contravenes by not providing technical assistance)		
14	70	Critical Information Infrastructure (CII)/ Protected system: *Punishment to any person who secures access or attempts to secure access to any computer resources relating to CII and declared as protected system*	Imprisonment up to 10 years and fine	Non-Bailable, Cognizable
15	70B	CERT-In: Indian Computer Emergency Response Team (CERT-In) to serve as national agency for incident response. (*punishment to any service provider, intermediaries, datacentres, etc., who fails to provide the information called for or comply with the direction issued by the CERT-In*)	Imprisonment up to 1 year or fine up to 1 crore or both	Bailable, Non-Cognizable
16	71	Punishment for misrepresentation to Controller of Certifying Authorities (CCA) or Certifying Authorities	Imprisonment up to 2 years or fine up to 1 lakh or both	Bailable, Non-Cognizable
17	73	Punishment for publishing electronic signature Certificate false in certain particulars	Imprisonment up to 2 years or fine up to 1 lakh or both	Bailable, Non-Cognizable
18	74	Punishment for publication of electronic signature certificate for fraudulent purpose	Imprisonment up to 2 years or fine up to 1 lakh or both	Bailable, Non-Cognizable

Non-Bailable offences under the IT Act (06 nos.):

Sr. No.	Section No.	Cyber Offence	Punishment	Bailable/ Cognizable
1	66F	Punishment for cyber terrorism	Imprisonment which may extend to life.	Non-Bailable, Cognizable
2	67A	Punishment for publishing or transmitting of material containing	1st Conviction – Imprisonment up to 5 years and fine up to 10 lakh.	Non-Bailable, Cognizable

Sr. No.	Section No.	Cyber Offence	Punishment	Bailable/ Cognizable
		sexually explicit act, etc., in electronic form	2nd Conviction – Imprisonment up to 7 years and fine up to 10 lakh	
3	67B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	1st Conviction – Imprisonment up to 5 years and fine up to 10 lakh. 2nd Conviction – Imprisonment up to 7 years and fine up to 10 lakh.	Non-Bailable, Cognizable
4	69	Power to issue directions for interception or monitoring or decryption of any information through any computer resource (*punishment to intermediary who fails to assist the agency*)	Imprisonment up to 7 years and fine	Non-Bailable, Cognizable
5	69A	Power to issue directions for blocking for public access of any information through any computer resource. (*punishment to intermediary who fails to comply with such Government direction*)	Imprisonment up to 7 years and fine	Non-Bailable, Cognizable
6	70	Critical Information Infrastructure (CII)/ Protected system: *Punishment to any person who secures access or attempts to secure access to any computer*	Imprisonment up to 10 years and fine	Non-Bailable, Cognizable

Sr. No.	Section No.	Cyber Offence	Punishment	Bailable/ Cognizable
		resources relating to CII and declared as protected system		

Bailable offences under the IT Act (12 nos.):

Sr. No.	Section No.	Cyber Offence	Punishment	Bailable/ Cognizable
1	65	Tampering with computer source documents.	Imprisonment up to 3 years or fine up to 2 lakhs or both	Bailable, Cognizable
2	66	Computer related offences: Punishment for doing dishonestly or fraudulently any act cited in section 43 directly or causing any person to do so, such as unauthorised access to or use of, introducing virus to, damages to, disruption of, denial of access to, assistance to access to, wrongful charges to another person's account by tampering with, destroying, deletion or alteration of any information in, computer resource or stealing/ concealing/ destroying any computer source code.	Imprisonment up to 3 years or fine up to 5 lakh or both.	Bailable, Cognizable
3	66B	Punishment for dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years or fine up to 1 lakh or both.	Bailable, Cognizable
4	66C	Punishment for identity theft, i.e., making use of	Imprisonment up to 3 years or fine up to 1 lakh or both.	Bailable, Cognizable

5	66D	Punishment for cheating by personation by using computer resource	Imprisonment up to 3 years and fine up to 1 lakh.	Bailable, Cognizable
6	66E	Punishment for violation of privacy.	Imprisonment up to 3 years or fine up to 2 lakh or both	Bailable, Cognizable
7	67	Punishment for publishing or transmitting obscene material in electronic form	1st Conviction – Imprisonment up to 3 years and fine up to 5 lakh. 2nd Conviction – Imprisonment up to 5 years and fine up to 10 lakh	Bailable, Cognizable
8	69B	Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security. (*punishment to intermediary who intentionally or knowingly contravenes by not providing technical assistance*)	Imprisonment up to 1 year or fine up to 1 crore or both	Bailable, Non-Cognizable
9	70B	CERT-In: Indian Computer Emergency Response Team (CERT-In) to serve as national agency for incident response. (*punishment to any service provider, intermediaries, datacentres, etc., who fails to provide the information called for or comply with the direction issued by the CERT-In*)	Imprisonment up to 1 year or fine up to 1 crore or both	Bailable, Non-Cognizable
10	71	Punishment for misrepresentation to Controller of Certifying Authorities (CCA) or Certifying Authorities	Imprisonment up to 2 years or fine up to 1 lakh or both	Bailable, Non-Cognizable

11	73	Punishment for publishing electronic signature Certificate false in certain particulars	Imprisonment up to 2 years or fine up to 1 lakh or both	Bailable, Non-Cognizable
12	74	Punishment for publication of electronic signature certificate for fraudulent purpose	Imprisonment up to 2 years or fine up to 1 lakh or both	Bailable, Non-Cognizable

Annexure-II

Statistics observed on various Apps and Social Networking Sites are given below:

A. SNAPCHAT

1. [1]**Statistics on Grievances Reported and actions taken thereon by Snapchat for the month of February, 2025:**

Sr. No.	Category	Total Content & Account Reports	Total Enforcements	Total unique accounts enforced
1.	Sexual Content	60,965	15,031	12,306
2.	Child Sexual Exploitation	21,466	6,816	6,019
3.	Harassment and Bullying	67,571	29,261	23,508
4.	Impersonation	17,410	111	108

2. **Statistics on Proactive Monitoring by Snapchat for the month of February, 2025**

Sr. No.	Category	Total Content & Account Reports	Total unique accounts enforced
1.	Sexual Content	19,284	9,036
2.	Child Sexual Exploitation	3,082	1,394
3.	Harassment and Bullying	31	23
4.	Impersonation	1	1

3. [2]**Statistics on Grievances Reported and actions taken thereon by Snapchat for the month of March, 2025:**

[1] **Source:** https://values.snap.com/privacy/transparency/india-02-2025
[2] **Source:** https://values.snap.com/privacy/transparency/india-03-2025

Sr. No.	Category	Total Content & Account Reports	Total Enforcements	Total unique accounts enforced
1.	Sexual Content	70,340	15,878	13,024
2.	Child Sexual Exploitation	25,610	7,771	6,797
3.	Harassment and Bullying	77,715	31,966	25,917
4.	Impersonation	21,118	142	142

4. Statistics on Proactive Monitoring by Snapchat for the month of March, 2025

Sr. No.	Category	Total Content & Account Reports	Total unique accounts enforced
1.	Sexual Content	19,745	9,472
2.	Child Sexual Exploitation	3,115	1,470
3.	Harassment and Bullying	38	35
4.	Impersonation	0	0

B. FACEBOOK

1. [3]Statistics on grievances and actions taken thereon by Facebook for the month of March, 2025:

Sr. No.	Category	Content Actioned	Proactive Rate

[3] https://transparency.meta.com/sr/india-monthly-report-Apr30-2025

1.	Adult Nudity and Sexual Nudity	2.0M	97.2%
2.	Bullying and Harassment	51.8K	63.2%
3.	Child Endangerment – Nudity and Physical Abuse	132.1K	99.3%
4.	Child Endangerment- Sexual Exploitation	88.4K	98.0%

2. [4]Statistics on grievances and actions taken thereon by Facebook for the month of April, 2025:

Sr. No.	Category	Content Actioned	Proactive Rate
1.	Adult Nudity and Sexual Nudity	1.6M	98.2%
2.	Bullying and Harassment	39.4K	65.8%
3.	Child Endangerment – Nudity and Physical Abuse	142.4K	99.2%
4.	Child Endangerment- Sexual Exploitation	161.7K	98.7%

C. INSTAGRAM

1. [5]Statistics on grievances and actions taken thereon by Instagram for the month of March, 2025:

[4] https://transparency.meta.com/sr/india-monthly-report-May31-2025
[5] https://transparency.meta.com/sr/india-monthly-report-Apr30-2025

Sr. No.	Category	Content Actioned	Proactive Rate
1.	Adult Nudity and Sexual Nudity	936.4K	98.0%
2.	Bullying and Harassment	439.4K	94.3%
3.	Child Endangerment – Nudity and Physical Abuse	166.5K	98.5%
4.	Child Endangerment- Sexual Exploitation	166.5K	98.5%

2. [6]Statistics on grievances and actions taken thereon by Instagram for the month of April, 2025:

Sr. No.	Category	Content Actioned	Proactive Rate
1.	Adult Nudity and Sexual Nudity	1.6M	98.2%
2.	Bullying and Harassment	39.4K	65.8%
3.	Child Endangerment – Nudity and Physical Abuse	142.4K	99.2%
4.	Child Endangerment- Sexual Exploitation	161.7K	98.7%

D. "X"

[6] https://transparency.meta.com/sr/india-monthly-report-May31-2025

1. [7]**Statistics on Grievances Reported and actions taken thereon by X for the period of April 26, 2024 through to May 25, 2025:**

Sr. No.	Category	Total Number of Grievances	Total Number of URLs Actioned
1.	Abuse / Harassment	280	40
2.	Child Sexual Exploitation	11	1
3.	Impersonation	20	2
4.	Sensitive Adult Content	355	83

2. **Statistics on Proactive Monitoring by X for the period of April 26, 2024 through to May 25, 2025**

Sr. No.	Category	Total Accounts Suspended
1.	Child Sexual Exploitation	227,474

[7] https://transparency.x.com/content/dam/transparency-twitter/country-reports/india/India-ITR-June-2025.pdf

Appendix-I

COMMITTEE ON THE EMPOWERMENT OF WOMEN (2025-2026)

MINUTES OF THE FOURTH SITTING OF THE COMMITTEE HELD ON WEDNESDAY, 09th JUNE, 2025

The Committee sat from 1100 hrs. to 1330 hrs. in Committee Room No. '01', Ground Floor, Block - A, Extension Parliament House Annexe, New Delhi.

PRESENT

Dr. D. Purandeswari - **Chairperson**

MEMBERS

LOK SABHA

1. Smt. Lovely Anand
2. Smt. D. K. Aruna
3. Ms. Iqra Choudhary
4. Smt. Kriti Devi Debbarman
5. Dr. Kadiyam Kavya
6. Smt. Jyotsna Charandas Mahant
7. Smt. Mahima Kumari Mewar
8. Km. Sudha R.
9. Smt. Himadri Singh
10. Dr. Rani Srikumar

RAJYA SABHA

11. Smt. Sagarika Ghose
12. Ms. Swati Maliwal
13. Smt. Rajani Ashokrao Patil
14. Smt. Sunetra Ajit Pawar
15. Smt. Sadhna Singh

SECRETARIAT

1. Smt Jyochnamayi Sinha - Joint Secretary
2. Smt. Neena Juneja - Director
3. Ms. Rachna Saxena - Deputy Secretary

Representatives of the Ministry of Electronics and Information Technology

1. Shri Bhuvnesh Kumar - CEO, UIDAI
2. Smt. Savita Utreja- - Scientist G and Group Coordinator

Representatives of the Ministry of Home Affairs

1. Shri Rakesh Kumar Pandey - Joint Secretary
2. Shri Rajesh Kumar - CEO, I4C

At the outset, the Chairperson welcomed the Members to the sitting of the Committee convened for briefing by the Representatives of the Ministry of Electronics and Information Technology and the Ministry of Home Affairs on the subject - 'Cyber Crimes & Cyber Safety of Women'. Thereafter, a PPT was made by JS(J) explaining the agenda of the sitting and the issues pertaining to Cyber Crimes & Cyber Safety of Women.

(The witnesses were then called in)

2. The Chairperson, then welcomed the Representatives of the Ministry of Electronics and Information Technology and the Ministry of Home Affairs to the sitting and in her welcome remarks, *inter-alia* raised issues that directly impacts the safety, dignity, and freedom of women in the digital world. She emphasized that Cyber-crimes against women have taken various alarming forms, from online stalking and identity theft to cyber bullying and the circulation of morphed images through use of deepfake technology. She appreciated the efforts made by the Ministry of Electronics and Information Technology and the Ministry of Home Affairs in addressing this issue. Initiatives such as the National Cyber Crime Reporting Portal (NCRP) under Indian Cyber Crime Coordination Centre (I4C), Proactive Monitoring Tool (PMT) by CDAC, Sahyog Portal to facilitate the issuance of Notices under IT Act, the launch of digital literacy campaigns, spreading public awareness and support for helpline services etc. are commendable and much needed. She further highlighted that often legal remedies are available, but the mechanisms for enforcement are weak or inaccessible, particularly for women in rural or marginalized communities. She impressed upon the need for greater awareness and sensitization on this important issue among all stakeholders.

3. Thereafter, Chairperson requested Ministries to brief the Committee Members on the legal safeguards, measures taken for creating awareness, the challenges they face in effective implementation of the laws and other significant gaps in implementation of cyber security measures.

4. The Chairperson also drew the attention of the witnesses to Direction 55 of the Directions by the Speaker regarding confidentiality of the proceedings and asked to present their PPT after introducing themselves.

5. After deliberations, the Committee raised the following important issues during the sitting:

(i) Widening the training and awareness drives regarding cybercrimes especially in rural areas, integration of cyber safety in schools.

(ii) To fix accountability of intermediaries and expeditious action.

(iii) Onboarding of IT intermediaries onto the Sahyog Portal for immediate action of reporting of CSEAM content.

(iv) Effective implementation of existing Indian legal framework for cyber crime against women eg. Bhartiya Nyay Samita, 2023, IT Act, 2000, POSCO Act, 2012, Indecent Representation of Women (Prohibition) Act, 1986 and others.

(v) Challenges of International cooperation on Cyber Crime.

(vi) AI & Tech-enabled identification to detect and flag CSEAM content (Child Sexual Exploitative and Abuse Material) automatically.

(vii) Observing Cyber Safety Week for mass awareness.

(viii) Collaboration with 3rd party organization & NGOs for intelligence and outreach on cybercrimes against women and children.

(ix) Provision of counselling, rehabilitation and social integration of women cyber victims.

(x) Capacity building of Police staff, Cyber Cells across the States.

(xi) Budget allocation for R&D and capacity building for Cyber Security.

(xii) Call for a new comprehensive Act to address various aspects of cybercrime and harassment against women.

(xiii) Overhauling of reporting mechanism and standardization of procedure for taking effective actions.

6. The Representatives of both the Ministries replied to the queries/clarifications sought by the Members on the subject and noted the suggestions given by the Committee. The Chairperson further requested them to furnish the written replies to those queries/clarifications which could not be clarified/replied to during the sitting.

7. The Chairperson then thanked the representatives of the Ministries for appearing before the Committee and furnishing valuable information on the subject.

(The witnesses then withdrew)

8. A verbatim record of the sitting of the Committee has been kept.

The Committee then adjourned.

Appendix-II

COMMITTEE ON THE EMPOWERMENT OF WOMEN (2025-2026)

MINUTES OF THE FIFTH SITTING OF THE COMMITTEE HELD ON WEDNESDAY, 09th JUNE, 2025

The Committee sat from 1430 hrs. to 1600 hrs. in Committee Room No. '01', Ground Floor, Block - A, Extension Parliament House Annexe, New Delhi

PRESENT

Dr. D. Purandeswari - **Chairperson**

MEMBERS

LOK SABHA

1. Smt. Lovely Anand
2. Smt. D. K. Aruna
3. Ms. Iqra Choudhary
4. Smt. Kriti Devi Debbarman
5. Dr. Kadiyam Kavya
6. Smt. Jyotsna Charandas Mahant
7. Smt. Mahima Kumari Mewar
8. Km. Sudha R.
9. Smt. Himadri Singh
10. Dr. Rani Srikumar

RAJYA SABHA

11. Smt. Sagarika Ghose
12. Ms. Swati Maliwal
13. Smt. Rajani Ashokrao Patil
14. Smt. Sunetra Ajit Pawar
15. Smt. Sadhna Singh

SECRETARIAT

1. Smt Jyochnamayi Sinha - Joint Secretary
2. Smt. Neena Juneja - Director
3. Ms. Rachna Saxena - Deputy Secretary

CDAC, NOIDA

1. Smt. Rekha Saraswat - Scientist –E

CYBER PEACE FOUNDATION

1. Major Vineet Kumar - Founder & Global President

At the outset, the Chairperson welcomed Smt. Rekha Saraswat, Scientist-E from CDAC (MEITY), and Major Vineet Kumar, Founder and Global President of Cyber Peace Foundation and requested them to apprise the Committee on the technical aspects in preventing and addressing cyber-crimes against women and existing measures. Further, commending the Foundation's significant grassroots work in promoting cyber safety, aiding victims of online abuse, conducting workshops, and supporting law enforcement, the Chairperson emphasized the importance of field-based insights that may help the Committee to understand on-ground challenges and system's loopholes, especially in the context of rising cyber threats against women.

2. Thereafter, the Chairperson drew the attention of the witnesses to Direction 55 of the Directions by the Speaker regarding confidentiality of the proceedings and asked to present their PPT after introducing themselves.

3. During the interaction, Smt. Rekha Saraswat *inter-alia* briefed the Committee on the various aspects of cybercrimes against women and available legal remedies. She raised several critical concerns, notably the lack of technical capabilities and tools within law

enforcement agencies (LEAs) leading to delays in addressing cybercrimes, Under-reporting that remains a persistent issue due to fear of stigma, victim blaming, and reputational damage.

4. Major Vineet Kumar, the Cyber Peace Foundation emphasized that cybercrimes against women are becoming more complex and damaging, with legislation struggling to keep up with rapid technological changes. The fragmented legal framework and weak accountability of intermediary platforms under existing IT rules were also flagged by the Foundation.

5. Further, the Cyber Peace Foundation proposed several key interventions like creating specialized cyber units for crimes against women, gender-sensitive and forensics training for police, developing survivor support systems, and enacting a comprehensive cybercrime law with clear definitions and inclusive protections, establish a Cyber Victim Compensation Fund, fast-track courts, standardized digital evidence protocols, and regional cyber rehabilitation centers, Integration of gender-sensitive digital safety education into curricula, improving platform transparency via AI tools, and enhancing international cooperation through expedited protocols and updated treaties .These measures aim to provide holistic support, ensure effective justice, and foster safer digital spaces for women.

6. The Expert and NGO replied to the queries of Members on the subject. Thereafter, the Chairperson thanked the expert and representatives from NGO for furnishing their valuable information and expertise on the subject.

(The witnesses then withdrew)

7. A verbatim record of the sitting of the Committee has been kept.

The Committee then adjourned

Appendix-III

COMMITTEE ON EMPOWERMENT OF WOMEN (2025-2026)

MINUTES OF THE NINTH SITTING OF THE COMMITTEE HELD ON TUESDAY, 22nd JULY, 2025

The Committee sat from 1500 hrs. to 1700 hrs. in Committee Room No. '01', Ground Floor, Block - A, Extension Parliament House Annexe, New Delhi.

PRESENT

Dr. D. Purandeswari - **Chairperson**

MEMBERS

LOK SABHA

1. Smt. Lovely Anand
2. Smt. D. K. Aruna
3. Ms. Iqra Choudhary
4. Smt. Jyotsna Charandas Mahant
5. Smt. Hema Malini
6. Smt. Mahima Kumari Mewar
7. Smt. Delkar Kalaben Mohanbhai
8. Smt. Satabdi Roy
9. Smt. Himadri Singh

RAJYA SABHA

10. Ms. Swati Maliwal
11. Smt. Mamata Mohanta
12. Smt. Sudha Murty
13. Smt. Maya Naroliya

14. Smt. Rajani Ashokrao Patil

SECRETARIAT

1. Smt Jyochnamayi Sinha - Joint Secretary
2. Smt. Neena Juneja - Director
3. Shri Sreekanth S. - Deputy Secretary

Representatives of the Ministry of Electronics and Information Technology

1. Shri S. Krishnan - Secretary
2. Shri Amitesh Kumar Sinha - Additional Secretary
3. Smt. Savita Utreja - Scientist G and Group Coordinator

Representatives of the Ministry of Home Affairs

1. Shri Rakesh Kumar Pandey - Joint Secretary
2. Shri Rajesh Kumar - CEO, I4C

At the outset, the Chairperson welcomed the Members to the sitting of the Committee convened for oral evidence of the Representatives of the Ministry of Electronics and Information Technology and the Ministry of Home Affairs on the subject - 'Cyber Crimes & Cyber Safety of Women'

(The witnesses were then called in)

2. After welcoming the representatives from the above-mentioned Ministries, the Chairperson expressed concern over the delay in furnishing written replies by the Ministry of Home Affairs (MHA) and seeking 12 weeks of extension of time to furnish those replies. She also highlighted the repeated last-minute exemption requests by the Home Secretary, stressing the need for seriousness, timeliness, and respect for the Committee's mandate on women's welfare.

3. The Chairperson , then reiterated the Committee's discussion held on 9th June, 2025 with MHA, MeitY and interaction with Cyber experts from CDAC and Cyber Peace foundation that mainly focused on scaling up cybercrime awareness and training, especially in rural areas, integrating cyber safety into school curricula, ensuring intermediary accountability, and strengthening the implementation of legal frameworks like the Bhartiya Nyay Sanhita, IT Act, and POCSO Act, along with addressing challenges in international cooperation for investigations. Key points also included AI-driven detection of exploitative content, observing Cyber Safety Week, and collaborating with NGOs for intelligence and outreach. Emphasis was placed on counselling, rehabilitation, and social reintegration of women victims, and capacity building of police and cyber cells across States. The CDAC expert highlighted under-reporting of cybercrimes due to stigma, fear, and limited law enforcement capabilities, stressing the need for victim-sensitive, tech-enabled redressal systems. The Cyber Peace Foundation echoed concerns on fragmented laws and weak platform accountability, proposing specialized cyber units, gender-sensitive training, a Cyber Victim Compensation Fund, fast-track courts, regional rehabilitation centers, standardized digital evidence protocols, a comprehensive cybercrime law, improved AI-driven platform transparency, and use of technology to block fraudsters instantly. These deliberations underline the urgent need for a coordinated, inclusive, and technology-driven approach to protect women's digital dignity and security in India.

4. After deliberations, the Committee *inter-alia* raised the following additional issues during the sitting:-

(i) Ensuring accountability of all Intermediaries: Current takedown time (36–72 hours) is too long that should be preferably reduced to less than 36 hours.

(ii) Onboarding of all Intermediaries on 'SAHYOG Portal' of I4C.

(iii) Technology Use: more AI-driven content detection, proactive blocking of harmful content, usage of Stop.NCII like tools.

(iv) Monthly reports on takedowns (millions of items removed: sexual content, CSAM, harassment, bullying, impersonation).

(v) Usage of regional language support via BHASHINI application.

(vi) Digital Investigation Support Centres (DISCs) in all states/UTs

(vii) Involvement of Local MPs/ MLAs in awareness drive.

(viii) Availability of Gender-segregated grievance data disposed by GAC.

5. Then, the Representatives of both the Ministries replied to the queries/clarifications sought by the Members on the subject and noted the suggestions given by the Committee. The Chairperson further requested them to furnish the written replies to those queries/clarifications which could not be clarified/replied to during the sitting.

6. The Chairperson then thanked the representatives of the Ministries for appearing before the Committee and furnishing valuable information on the subject.

(The witnesses then withdrew)

7. A verbatim record of the sitting of the Committee has been kept.

The Committee then adjourned.

Appendix-IV

COMMITTEE ON THE EMPOWERMENT OF WOMEN (2025-2026)

MINUTES OF THE 11th SITTING OF THE COMMITTEE HELD ON TUESDAY, 19th AUGUST, 2025

The Committee sat from 1500 hrs. to 1700 hrs. in Committee Room No. '01', Ground Floor, Block - A, Extension Parliament House Annexe, New Delhi.

PRESENT

Smt. Sudha Murty - Chairperson (Acting)

MEMBERS

LOK SABHA

2. Smt. Lovely Anand
3. Smt. D. K. Aruna
4. Smt. Shobhanaben Mahendrasinh Baraiya
5. Ms. Iqra Choudhary
6. Smt. Kriti Devi Debbarman
7. Smt. Kadiyam Kavya
8. Smt. Jyotsna Charandas Mahant
9. Smt. Hema Malini
10. Smt. Mahima Kumari Mewar
11. Smt. Delkar Kalaben Mohanbhai
12. Smt. Sudha R.
13. Smt. Himadri Singh
14. Dr. Rani Srikumar
15. Smt. Smita Uday Wagh

RAJYA SABHA

16. Dr. Sangeeta Balwant
17. Ms. Swati Maliwal
18. Smt. Maya Naroliya
19. Smt. Sunetra Ajit Pawar
20. Smt. Sadhna Singh

SECRETARIAT

1. Smt. Neena Juneja - Director
2. Smt. Sonia Sankhla - Executive Officer

Representatives of the Ministry of Electronics and Information Technology

1. Shri Amitesh Kumar Sinha - Additional Secretary
2. Smt. Savita Utreja - Scientist G and Group Coordinator

Representatives of the 'Meta'

1. Shri Rakesh Kumar Pandey - Joint Secretary
2. Shri Rajesh Kumar - CEO, I4C

Representatives of the 'Google'

1. Shri Rakesh Kumar Pandey - Joint Secretary
2. Shri Rajesh Kumar - CEO, I4C

(*As the Hon'ble Chairperson was absent on the said sitting due to some unavoidable reasons, Smt. Sudha Murty, M.P. presided over*)

At the outset, the Chairperson (Acting) welcomed the Members to the sitting of the Committee convened to hear the views of the Representatives of the Ministry of Electronics and Information Technology, Google & Meta on the subject - 'Cyber Crimes & Cyber Safety of Women' and informed the Committee that due to unavailability of Hon'ble Chairperson, she had been asked to chair the scheduled sitting on that day.

(The witnesses were then called in)

2. The Chairperson (Acting), then welcomed the Representatives of Representatives of the Ministry of Electronics and Information Technology, Google & Meta and invited their attention to Direction 55 of the Directions by the Speaker, Lok Sabha regarding confidentiality of the proceedings and requested to present their views on the subject under examination.

3. Firstly, the representatives from MeitY informed that they had already appeared before the Committee on 09.06.2025 and 22.07.2025 and on that day only social media intermediaries had been called to present their on the subject. Representatives of Google and Meta then briefed the Committee and during the deliberation, Members of Parliament

inter-alia raised strong concerns over the widening gap between platforms' stated policies and the ground reality of cyber safety for women. Key issues were highlighted including delays in removal of unlawful content such as NCII, deepfakes and child sexual abuse material, the unchecked proliferation of fake accounts, lack of transparency in complaint handling, weak safeguards in regional languages, and allegations of platforms misusing sensitive user data. MPs pressed Google and Meta to provide year-wise and city-wise complaint data, staff strength deployed in India, and average turnaround time for responding to law enforcement requests through the SAHYOG portal. They suggested new women-centric tools such as a Safe Comment Section on YouTube and Safe DM filters on Instagram, alongside stronger awareness campaigns in regional languages, cyber safety education in schools, and partnerships with NGOs. While Google and Meta outlined their existing policies, AI-driven detection tools, safety initiatives, and large-scale content removals, they acknowledged gaps and assured written replies to specific queries. MeitY underscored the importance of intermediary cooperation and data sharing. The way forward identified by the Committee during the sitting were stricter enforcement of 24-hour takedown rules, improved transparency and accountability, development of India-specific AI safeguards, stronger law enforcement coordination, and treating women's online safety as a core responsibility rather than CSR activity.

4. The Chairperson then thanked the representatives of the MeitY, Google & Meta for appearing before the Committee and furnishing valuable information on the subject.

(The witnesses then withdrew)

5. A verbatim record of the sitting of the Committee has been kept.

The Committee then adjourned.

Appendix-V

COMMITTEE ON THE EMPOWERMENT OF WOMEN (2025-2026)

MINUTES OF THE 21st SITTING OF THE COMMITTEE HELD ON TUESDAY, 17th March, 2026

The Committee sat from 1500 hrs. to 1600 hrs. in Committee Room No. 'D', Ground Floor, Parliament House Annexe, New Delhi.

PRESENT

Dr. D. Purandeswari - Chairperson

MEMBERS

LOK SABHA

2. Smt. Lovely Anand
3. Smt. D. K. Aruna
4. Smt. Kriti Devi Debbbarman
5. Dr. Kadiyam Kavya
6. Smt. Jyotsna Charandas Mahant
7. Smt. Mahima Kumari Mewar
8. Smt. Delkar Kalaben Mohanbhai
9. Km. Sudha R.
10. Smt. Himadri Singh
11. Dr Rani Srikumar
12. Smt. Smita Uday Wagh

RAJYA SABHA

13. Dr. Sangeeta Balwant
14. Smt. Sagarika Ghose
15. Ms. Swati Maliwal
16. Smt. Sudha Murty
17. Smt. Maya Naroliya
18. Smt. Sadhna Singh

SECRETARIAT

1. Smt. Jyochnamayi Sinha - Joint Secretary
2. Shri Sreekanth S. - Deputy Secretary
3. Shri Yogesh Verma - Committee Officer

2. At the outset, the Chairperson welcomed the Members to the sitting of the Committee. The Committee, thereafter took up for consideration the draft Report on the subject 'Cyber Crimes and Cyber Safety of Women'. The Chairperson read out the salient features of the recommendations. Then, after some deliberations, the Committee adopted the Report without modification.

3. The Committee authorized the Chairperson to finalize the Report and present the same to both the Houses of Parliament.

The Committee then adjourned.