

Cyber Crimes and Cyber Safety of Women in India

Mains: GS Paper II | Governance

Why in News?

The Parliamentary Committee on Empowerment of Women, chaired by Dr. D. Purandeswari, submitted a landmark report titled "Cyber Crimes and Cyber Safety of Women".

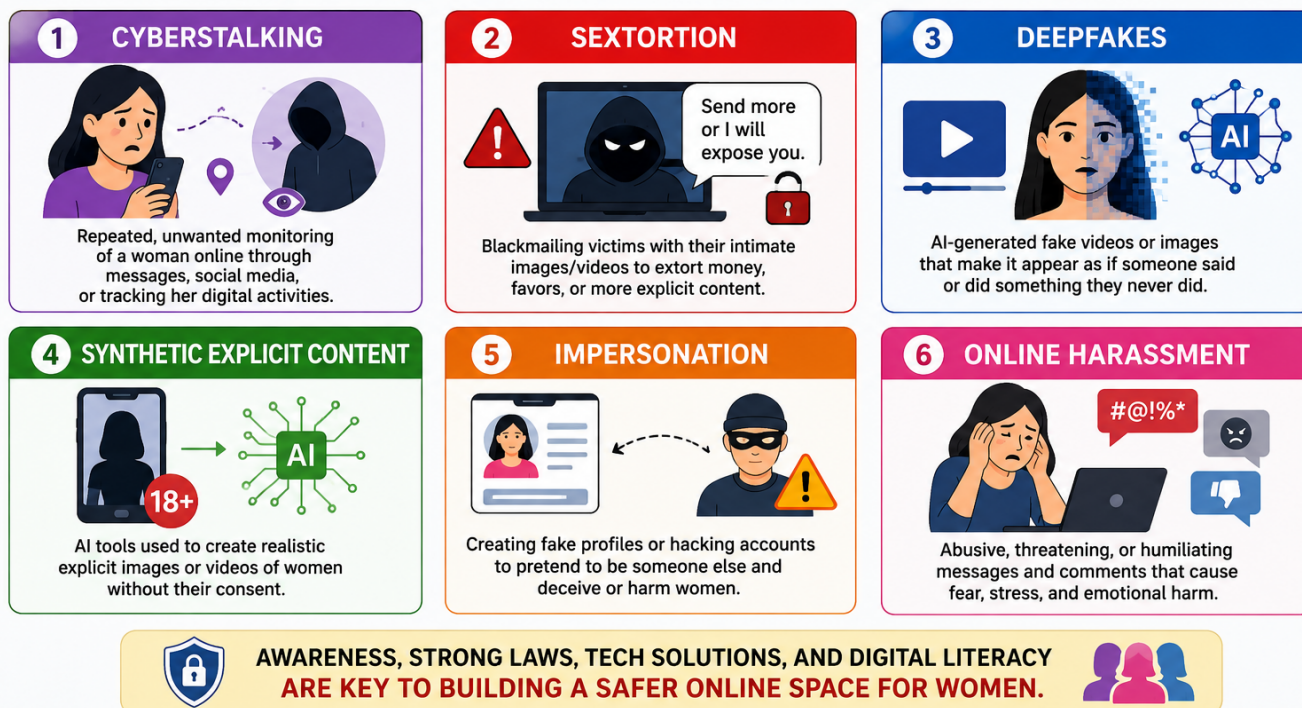
What are the highlights of the report?

- National Crime Records Bureau (NCRB) data revealed a **239% surge in cybercrimes against women** between 2017 and 2022.
- The report also reveals that a multi-fold increase in online offences targeting children.
- The report emphasizes that digital spaces are increasingly weaponized through
 - AI-generated deepfakes,
 - Sextortion,
 - Non-consensual intimate imagery (NCII),
 - Cyberstalking, and
 - Online harassment, necessitating a fundamental overhaul of India's cyber-governance architecture.
- Cyberstalking and online abuse are among the major forms of gender-based cyber violence.

MAJOR EMERGING THREATS

AFFECTING WOMEN ONLINE

CYBER CRIMES AND CYBER SAFETY OF WOMEN



- Social media platforms are frequently used for harassment, impersonation, morphed images and non-consensual sharing of intimate content.
- Under-reporting remains a concern due to social stigma, fear, lack of awareness and limited knowledge of cybercrime reporting mechanisms.

What are the key dimensions of gendered cybercrimes?

- **Deepfakes** - Generative AI tools allow the creation of hyper-realistic, non-consensual deepfake images and videos, causing psychological, social, and economic damage to women.
- **Sextortion** - Fraudulent romantic engagements on dating/social media platforms transitioning into blackmail and financial exploitation.
- **Cyberstalking** - Malicious exposure of private personal information (addresses, phone numbers) alongside persistent harassment, often driving victims to delete their digital footprint entirely (digital exclusion).
- **Anonymized Fake Profiles** - The widespread availability of unverified, anonymous accounts on gaming, social media, and messaging platforms enables persistent abuse with near-total impunity.

What are the structural bottlenecks in the existing system?

Dimension	Key Bottleneck / Deficit	Impact on Victims
Investigative Capacity	Acute shortage of trained cyber investigators and certified digital forensic personnel across state police forces.	High case pendency, loss/corruption of ephemeral digital evidence.

Platform Accountability	Delayed responses by social media intermediaries to takedown requests; lax verification of user profiles.	Rapid virality of objectionable content; prolonged trauma for victims.
Reporting Mechanisms	Complexity of the National Cyber Crime Reporting Portal (NCRP); social stigma and fear of police interactions.	Severe under-reporting, especially in rural and tier-2/3 regions.
Judicial Capacity	Lack of specialized training among prosecutors and lower court judges in handling digital evidence and online harms.	Low conviction rates and delayed trial proceedings.

What are the major recommendations of the parliamentary standing committee?

- **Forensic Decentralization** - Establish additional regional forensic units, mobile cyber forensic vans, and deploy dedicated digital forensic consultants in every state.
- **Specialized Judicial Units**- Set up dedicated prosecution units for cybercrimes against women and mandate specialized training modules on digital evidence across state judicial academies.
- **Scaling Up 'CyberShakti** - Expand the Ministry of Electronics and Information Technology's (MeitY) **CyberShakti** program, creating a dedicated vertical to train women police officers, cyber-cell personnel, and frontline social welfare officials.
- **Mandatory KYC Verification** - Introduce mandatory Know Your Customer (KYC)-based verification across all social media, dating, and gaming platforms to eliminate fake profiles and anonymous harassment.
- **Proactive AI Monitoring**- Deploy advanced AI tools (such as MeitY/MHA's Proactive Monitoring Tool) to detect child sexual abuse material (CSAM) and non-consensual imagery proactively.
- **Shorter Takedown Timelines** - Enforce a strict **24-hour SLA (Service Level Agreement)** for initiating content takedown via the **SAHYOG portal**.
- **Child-Centric Digital Guardrails** - Formulate age-appropriate usage limits and safety regulations to protect children and adolescents from psychological harms.
- **Grassroots Complaints Enablers** - Empower local touchpoints Anganwadi centres, ASHA workers, Women Helplines, and Panchayat Digital Kiosks to register complaints on the NCRP on behalf of victims while maintaining strict confidentiality.
- **Grievance Escalation Matrix** - Establish a clear escalation protocol for victims if local police stations fail to act in accordance with the Standard Operating Procedure (SOP).
- **Standalone Gender-Sensitive Cyber Law** - Initiate a time-bound legislative process to draft a comprehensive, gender-sensitive cybercrime framework that explicitly addresses emerging threats like deepfakes, sextortion, and AI-driven harassment.

What is the way forward?

- Transitioning from the current reactive model under the Information Technology (IT) Act, 2000 to a proactive, victim-centric regime.
- Thus, it recognizes "digital bodily integrity" as an extension of Article 21 (Right to Life and Personal Liberty).
- Strengthening cross-functional coordination between the Ministry of Home Affairs (MHA), MeitY, Ministry of Women and Child Development (MWCD), and state police forces through real-time data sharing via the Indian Cyber Crime Coordination Centre (I4C).
- Integrating digital citizenship, online consent, and cyber safety modules into school and college curricula to address the root cultural causes of online discrimination.

Reference

[PRS India | Cyber Crimes and Cyber Security of Women](#)

