Tackling Online Abuse

For Prelims: Cyber Harassment, Bharatiya Nyaya Sanhita (BNS), 2023, Information Technology (IT) Act, 2000, High Court, Supreme Court, Digital Personal Data Protection (DPDP) Act, 2023, Deepfake, Digital Literacy Program.

For Mains: Online abuse and its forms, Challenges and remedial steps to tackle online abuse in India.

Source: TH

Why in News?

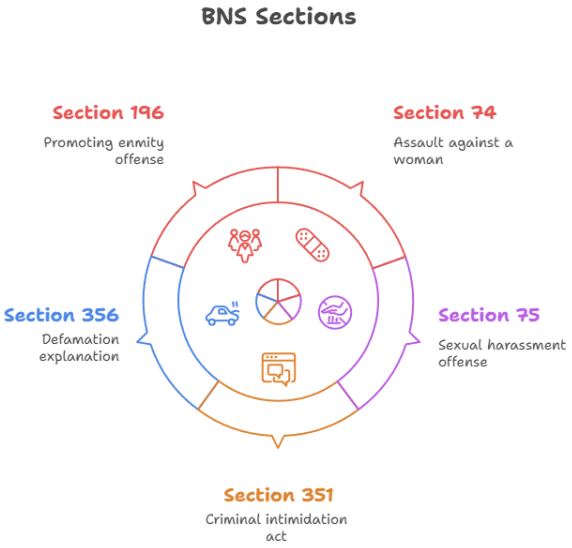
Following the **Pahalgam terror attack**, a **peace appeal** by a victim resulted in her **severe trolling**. Similarly, India's Foreign Secretary **faced abusive remarks** after announcing India-Pakistan ceasefire.

- It revealed India's growing crisis of **cyber harassment and weak regulation** highlighting the need for **legal reform, platform accountability, and victim protection**.

What is Online Abuse?

- **About: Online abuse** (**cyber abuse**, **digital abuse**, or **internet harassment**) refers to any form of **harmful, threatening, or demeaning behavior** that occurs through digital platforms.
  - It can be directed at **individuals, groups, or entire communities** and can take many forms, from **verbal attacks** and **harassment** to the **non-consensual sharing of private information** or images.
- **Types:**
  - **Cyberbullying:** It is the use of digital platforms to **harass, threaten, or humiliate** someone repeatedly, causing **emotional harm**.
  - **Cyberstalking:** It is **persistent, unwanted online monitoring** and harassment that causes fear, involving **repeated messages, tracking activity,** or using spyware and fake accounts.
  - **Trolling:** Trolling is deliberately posting **offensive or provocative messages** online to upset people or disrupt conversations.
  - **Doxxing:** Doxxing, short for **"dropping dox" (documents),** is the **unauthorized** online sharing of **private information**, like addresses or phone numbers, often to harass or threaten victims.
  - **Revenge Porn:** It is sharing or threatening to **share intimate images without consent,** violating privacy and often used for blackmail or humiliation.
  - **Catfishing:** It is creating a **fake online identity** to deceive others, often for emotional, financial, or **malicious purposes.**
- **Status of Cyberbullying in India:** India has the **highest cyberbullying rate globally,** with over **85%** of children reported it.
  - About **46%** reported **bullying strangers** (vs. 17% globally) and **48% bullied someone they know** (vs. 21%).

    - Top forms include spreading **false rumours (39%)**, **exclusion from chats/groups (35%),** and **name-calling (34%).**
- **Legal Provisions to Tackle Online Abuse:**
    - **Bharatiya Nyaya Sanhita (BNS), 2023:**



    - **Information Technology (IT) Act, 2000:**
        - **Section 66C:** Identity theft
        - **Section 66D:** Impersonation fraud
        - **Section 67:** Publishing or transmitting obscene material electronically.
    - **Digital Personal Data Protection Act (DPDP), 2023: DPDP** provides for penalties for failing to **prevent data breaches** leading to harassment
    - **IT (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021:** Social media platforms must disclose the **first originator** of content for investigations into offences like **rape, death threats, sexually explicit material**, and content threatening **state harmony** or **international relations.**
- **Judicial Stand:**
    - ***Shaviya Sharma vs Squint Neon & Ors Case, 2024*:** The **Delhi High Court** ordered **removal of tweets** exposing a woman's **personal details**, recognizing **doxxing's serious privacy and safety risks** despite lacking specific legal status.
    - ***Shreya Singhal v. Union of India Case, 2015*:** The **Supreme Court struck down Section 66A of the IT Act,** which **criminalized "offensive" online speech**, as unconstitutional—protecting free speech while emphasizing that **reasonable restrictions** must be narrowly defined.
    - ***KS Puttaswamy v. Union of India Case, 2017*:** The Supreme Court declared **privacy a fundamental right (article 21)**, laying the foundation to **protect personal data** and prevent **unauthorized online disclosure or doxxing**.

What are the Challenges in Tackling Online Abuse in India?

- **No Dedicated Law**: India currently **lacks a specific law** that directly addresses **online hate speech and trolling** comprehensively.
    - Existing laws don't cover ongoing online abuse unless it's **obscene, threatening, or fraudulent**.
    - Stalking laws are **gender-specific (limited to men targeting women)** and target individual intent, **overlooking mass online harassment**.
- **Content Moderation Challenges:** Social media companies are taking significantly fewer **content screening** and **proactive measures** to address **hate speech** in **India** compared to the **US** and **EU.**
    - Platforms like **Telegram** are facing legal action for **permitting criminal activity,** while **profit motives** have weakened moderation, allowing **hate speech to**

spread.

- **Ambiguity over "Publicly Available Data"**: The **Digital Personal Data Protection (DPDP) Act, 2023** exempts **"publicly available"** personal data but **lacks a clear definition**, creating ambiguity.
    - This gap may enable cybercrimes like **doxxing,** as **fragmented data** from various platforms can be **easily combined for harassment or intimidation**.
- **Enforcement Gaps**: There is **lax implementation** of the **IT Rules** in **India**, leading to weak enforcement of **digital safety** and **accountability standards.**
    - Victims, especially of **gendered abuse**, face disbelief and **victim-blaming,** discouraging legal recourse.

What can be Remedial Steps to Tackle Online Abuse in India?

- **Legal & Policy Reforms:** A dedicated **cyber harassment law** should be enacted to clearly define and criminalize **doxxing, deepfake abuse, and coordinated trolling**.
    - Amend the **IT Act** and **BNS** to clearly define **obscene, threatening, and hate speech** for clarity and to prevent misuse.
- **Strengthening Enforcement:** To effectively combat cybercrime, it is essential to establish **specialized cyber cells** and **train police in areas like IP tracking and identifying anonymous accounts**.
    - A leading example is **Kerala's Cyberdome**, which brings together **police, ethical hackers, academia, and tech firms** to advance **cybercrime detection, digital forensics, and AI-based surveillance.**
    - Implement robust **whistleblower protections** to safeguard victims reporting **online abuse** from retaliation and **counter-harassment**.
- **Tech & Platform-Level Solutions:** Leverage **AI-powered detection** and machine learning to **flag hate speech, deepfakes, and abusive trends,** enabling real-time moderation of violent and sexual content.
    - Implement **user verification systems** to penalize **fake profiles** and **bot-driven harassment.**
- **Public Awareness:** Implement **digital literacy programs** in schools and colleges to teach **responsible social media use** and to **debunk fake news, hate narratives, and conspiracy theories**.
    - Launch **anti-trolling campaigns** promoting positive behavior and **countering communal and sexist abuse** through influencers and media.
- **Corporate Responsibility:** Platforms should adopt **ethical monetization policies** by **stopping algorithmic amplification of hate** and demonetizing abusive content creators.
    - Social media firms should enforce **strict monitoring of online abuse**, similar to the measures implemented in the **US** and **Europe**.

Conclusion

Stopping online abuse requires **strong laws, better enforcement, tech innovation, and societal change**. While **free speech must be protected**, accountability for **organized harassment, hate speech, and privacy violations** is non-negotiable. A balanced approach—protecting free speech while safeguarding victims—is essential to combat cyberbullying, doxxing, and hate speech in the digital age.

Drishti Mains Question:

Analyze the need for dedicated legislation to tackle cyber harassment and online trolling in India.

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims

Q. In India, under cyber insurance for individuals, which of the following benefits are generally

covered, in addition to payment for the loss of funds and other benefits?

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialized consultant to minimize the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only

(b) 1, 3 and 4 only

(c) 2 and 3 only

(d) 1, 2, 3 and 4

Ans: (b)

Q. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only

(b) 1 and 2 only

(c) 3 only

(d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. (2022)