CYBERCRIMES AGAINST WOMEN IN INDIA: LEGAL GAPS AND EMERGING CHALLENGES

Rajeev Kumar Singh, Indian Institute of Management, Rohtak

Introduction

The digital revolution has transformed India into one of the largest online populations in the world, significantly altering the access to education, unemployment, communication and self-expression. In the case of women, the internet has provided a new path to learning, to participating in the economy and digital visibility and as a result, they have gained more independence and can now participate more actively in public discourse. This growing digital footprint has provided unprecedented opportunities for empowerment. Simultaneously, it has subjected women to new and deeply concerning forms of vulnerability, rendering online spaces more unsafe.

Over the past few years, cybercrimes committed against women have been on an unsettling rising trend indicating the persistence of gender-based violence in online space. Cyberstalking, cyberbullying, online harassment, revenge pornography, sextortion and the non-consensual sharing of intimate images have become widespread types of abuse. The artificial intelligence-based technologies, especially the deepfake technology have escalated these harms by facilitating the creation and distribution of fabricated sexually explicit content without authorization. These acts extend beyond violation of privacy and lead to abject emotional, social, and reputational harm. The crimes are the contemporary instances of misogyny which undermines the dignity and agency of women in the digital environments.

The magnitude of the issue is reflected in the official statistics. In 2023, India registered more than 4.48 lakh incidences of crimes against women and reported incidents of cybercrime were up by almost 31 percent to about 86,000 cases all over the country.[1]

[1] National Crime Records Bureau, *Crime in India 2023: Statistics on Crimes Against Women and Cybercrime* (Ministry of Home Affairs 2024).

Complaints registered through the National Commission for Women and the National Cyber Crime Reporting Portal also show the further increase in the number of cases of online harassment and image-based abuse.[2] Nevertheless, such statistics are likely to be lower than the actual level of cyber violence as many women are still afraid of being socially stigmatized, fear retaliation, and suffer reputational damage to report such crimes.

Emerging security threats like deepfake pornography, doxxing and anonymous online targeting have complicated regulation and enforcement. Digital content quickly goes viral and it is often impossible to remove it clearly and victims end up living with long-term psychological and social impacts. Despite the fact that the Indian legal framework, in particular, Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, address offences such as stalking, voyeurism, and publishing obscene content, there are still significant loopholes.[3] Many forms of online harm are not recognized as gender-specific crimes, artificial intelligence-based abuse has no clear regulation, there is still a problem with evidentiary issues, and even the law enforcement structures do not always have specialized technical training.

The present paper analyses cybercrimes against women, prevalent in India by exploring the most prevalent forms, social aspects driving them, legal remedies available, as well as new technological issues of concern. It claims that even though a fragmented legal framework is concerned, the absence of gender-sensitive legal mechanisms and a comprehensive regulatory approach to artificial intelligence has left the current laws insufficient to handle the evolving nature of online violence.

Conceptual Framework: Understanding Cybercrimes Against Women

- **Nature of Cybercrime-**

  Cybercrime can be defined as illegal actions executed either by the use of a computer, digital devices, or internet either as a weapon or as an object. Such crimes are marked by anonymity, fast spreading of content, and lack of clear territories. Cybercrimes committed against women tend to uphold the status quo in gender inequalities, gender bias, and power structure, and this allows the

[2] National Commission for Women, *Annual Report 2022–23* (Government of India)
[3] Information Technology Act 2000, ss 66E, 67, 67A.

perpetrator to harass, intimidate, and control a victim with little fear to hold them accountable in the short term.[4] The harmfulness of such offences is further being increased by their constant and borderless character.

- **Cyberstalking-**

  Cyberstalking refers to the process of repeated and unwanted spying, use of communication or monitoring of a woman using digital tools like social media, emails or messaging software. It can be extremely intimidating and scary most of the time as this can limit the presence of the victim online and their everyday activities.

- **Cyberbullying and Online Harassing-**

  Cyberbullying and online harassment contain harassing messages, threats, defamation and collusion trolling meant to embarrass or intimidate women. Pseudonymity that accompanies online platforms fosters recurrent maltreatment and heightens mental damage due to the exposure of the audience.

- **Revenge Pornography-**

  Revenge porn is the sharing of intimate content or videos without a person's consent, which is typically shared by an ex-boyfriend or girlfriend. Those acts cause serious reputational damage, emotional trauma and social exclusion, with women being disproportionately affected.[5]

- **Morphing and Deepfake Abuse-**

  Morphing and deepfake abuse constitute a digitally altered image or fabricated sexually explicit content that is created by artificial intelligence. These habits are a menacing trend in their realism, quick propagation and the inability to tell the difference between the falsified information and the original sources.

[4] UN Women, *Online and ICT-facilitated Violence Against Women and Girls* (2020).
[5] *State of West Bengal v Animesh Boxi* (2018) SCC OnLine Cal 1393.

- **Sextortion-**

  Sextortion involves individuals who intimidate others to disclose their personal pictures or other private information unless the victim yields to sexual or monetary requests. It takes advantage of fear, shame and social stigma to put victims under duress.

- **Impact on Victims-**

  Women are the victims of cybercrimes that have far reaching psychological, social, and economic damages. Victims are also likely to have anxiety, depression, and loss of self-esteem, as well as, social isolation and withdrawal in the digital environment. And at work, this type of abuse may ruin a career, reduce the number of jobs available, and cost in terms of legal and mental health costs.

Statistical Trends in India

- **NCRB Statistics Trends (Recent Years)**

  As per the latest crime in India 2023 report issued by the National Crime Records Bureau (NCRB), it was revealed that cybercrimes in India increased considerably as 86,420 cases of cybercrimes of all types were registered under different parts of the law in 2023, as compared to 2022. This trend demonstrates a consistent upward trend of cyber-crimes in the past years - approximately 65,893 cases in 2022 and more than 86,000 cases in 2023.

  Among 86,420 cases, 59,526 (68.9%) instances were driven by fraud, 4,199 cases (4.9%) were related to sexual exploitation and 3,326 cases (3.8%) to extortion, highlighting the prevalence of financially and sexually harmful activity on the internet.

  Meanwhile, the total crime in India grew by approximately 7.2 percent in 2023, and 6.24 million cognizable crimes were registered. 2023 alone recorded a crime within every five seconds around the country.[6]

[6] National Crime Records Bureau, *Crime in India 2023* (overall cognisable crime statistics).

- **Online Harassment: Growth of complaints**

  There is a correlation between the decrease in cybercrime registration and the number of complaints linked to digital harassment and abuse. There have been explosion of cases pertaining to cyberstalking, threats, identity theft and sharing intimate material without consent in platforms, like the National Cyber Crime Reporting Portal. Even though these figures cover several types of cyber-crimes, they indicate a significant increase in the number of complaints of female online harassment.[7]

- **Under Reporting of Crimes against Women**

  According to NCRB data as well, the number of crimes against women grew slightly by 0.4% - 0.7%, which means that the number of crimes against women also rose to 448211 cases in 2023 compared to 445256 cases in 2022. Nevertheless, these official numbers might be even less than the real rates of cyber violence since most women do not report cases, considering the fear of being stigmatized, threatened, and damaged by the reputation. There is data that claims that a minor percentage of gender-based violence victims report the events to the authorities, and this fact implies that the actual rates of cybercrime committed against women are much greater than indicated by the NCRB statistics.

- **Urban vs Rural Divide**

- The emotional space between urban and rural in the use of internet and patterns of reporting is evident. The increase in the registered cases of cybercrimes recorded in urban areas is attributed to the fact that digital access is increased, awareness is increased and reporting mechanisms are with increased awareness are easily available. Urban centres have more women who are likely to make complaints over the cybercrime portal or local cyber police cells. By contrast, in rural regions, there are simply fewer registrations, not necessarily because of the reduced number of crimes, but because of the reduced internet access, lower

[7] Ministry of Home Affairs, Government of India, *National Cyber Crime Reporting Portal: Statistical Overview* (latest available data).

levels of digital literacy, and the presence of more robust social stigma, which stop law enforcement agencies and prevent victims less willing to seek help.[8]

- **Disparity between Registered Cases and Real Incidents.**

  The gap between NCRB numbers and actualities at the ground level shows that there is a big gap in reporting. The official statistics indicate only the registered and documented cases, as a significant portion of cyber harassment is not reported. This omission highlights structural problems with consciousness, access to justice and systems of supporting victims, all of which provide an incomplete understanding of the actual extent of cybercrime against women in India.

Indian Legal Framework that deals with the Cybercrimes against women

India lacks one specific law dealing under cybercrimes against women. Rather, these offences have been dealt with in a mix of the provisions on Information Technology Act, 2000, Indian Penal Code, 1860 (IPC), and its offshoot, the Bharatiya Nyaya Sanhita, 2023, (BNS) and some special legislations. Although these laws aim to control online wrongdoings all together, they have not initially been put in place to deal with the gendered, technological and transnational aspects of digital abuse. Due to this, the legal mechanism is still compartmented, proactive, and largely unresponsive, when it comes to addressing the lived experiences of women in cyberspace.

Information Technology Act, 2000

The main law that regulates the cyberspace in India is the Information Technology Act, 2000. The Act was established mainly to advance e-commerce and the e-governance concepts but in 2008, the Act was amended to include regulations on cyber offences. The IT Act is gender-neutral, though, some of its provisions are regularly used when it comes to cases of online abuse of women.

- **Section 66E – Invasion of Privacy**

  Section 66E criminalises an action of capturing, publishing or transmitting an image

[8] Internet and Mobile Association of India (IAMAI), *Digital in India Report* (latest edition).

of the intimate parts of a person without their consent, when the act compromises their privacy. The penalty is a maximum of three years imprisonment or a fine of up to 2 lakh rupees which is liable to both.

This is exceptionally applicable in matters relating to voyeurism, secret recording, and the sharing of intimate photos out of consent. Nonetheless, it is agonized with immense shortcomings. It does not specifically address digitally manipulated images, morphed pictures and deepfakes made with the human-like artificial intelligence. Further, proving the intentionality is a series of evidence issues because it is the victims who have to demonstrate the intent to deliberately breach cybercrime laws rather than accidentally.

- **Section 67 - Publishing or Transmitting Obscene Material**

Section 67 proscribes publication or transmission of obscene material in the electronic form. It sentences a maximum of three years in prison and a fine on first time offenders but those caught in a second or third offense receive heavier penalties.

The clause is usually applied to situations with abusive content, explicit messages, and posts that are sexually offensive toward women. But it is not concerned mainly with individual dignity, but with the protection of the morality of the people. The lack of definition of what constitutes obscenity has created inconsistent judicial interpretation and discrimination in application.[9]

- **Section 67A - Publication of Sexually Explicit Material**

The section 67A is concerned with material that includes sexually explicit acts or practices. It contains the prison term of not more than five years and fine of ten lakh rupees.

This clause has frequently been used in response to revenge porn and leaked sex videos and explicit deepfakes. Although it is relevant, the section does not focus on consent or emotional harm. It sees the crime primarily as a matter of content control

[9] Apar Gupta, 'Obscenity Law and the Internet in India' (Internet Freedom Foundation Policy Brief).

as opposed to a grave violation of bodily privacy and autonomy.

- **67B - Child Sexual Content**

  The section 67B of the criminal code prohibits the production, distribution and viewing of sexually explicit materials involving children. It applies in scenarios where girls under the age of majority are groomed, exploited, or targeted by use of pornography online.[10]

  This section is also more victim-focused than other provisions have been. It points out the discrepancy in the Indian legal structure where children are offered full protection under the law yet adult women are not.[11]

Indian Penal Code (IPC) and Bharatiya Nyaya Sanhita (BNS), 2023

In its past, the IPC, 1860 was the foundation of the Indian criminal justice system. In 2023, it was substituted by the Bharatiya Nyaya Sanhita (BNS) which is designed to remodel the criminal law on India. A large number of IPC provisions that applied to cybercrimes involving women have been preserved in substance, although renumbered and reorganized under the BNS.

- **Voyeurism - IPC Section 354C / BNS Equivalent**

  The IPC in section 354C criminalized voyeurism which is defined as a witnessing, capturing, or distributing photographs of a woman performing a private act without her consent.

  This clause recognised the aspect of privacy breach as a sexual violence. Within the BNS, voyeurism remains a punishable crime and it preserved the essence of consent and private space. This provision is applied to leaked videos, hidden camera videos, and screen recordings that are uploaded online in the digital context. But similarly to its IPC counterpart, it pays inadequate attention to manipulated or AI sourced imagery.

[10] Protection of Children from Sexual Offences Act 2012.
[11] Apar Gupta, 'Obscenity Law and the Internet in India' (Internet Freedom Foundation Policy Brief).

- **Stalking - IPC Section 354D / BNS Equivalent**

  Section 354D IPC phrased stalking as comprising of repeated efforts to connect with a woman, spy on her activity, or receive unwanted communication by an electronic means. This was a significant step towards accepting cyberstalking as a crime.

  The BNS maintains the stalking as an offense, including online forms of intimidation. Enforcement is nonetheless weak. It is common that law enforcement agencies define stalking with a thin slice meaning that they pay attention to physical presence and not online harassment, frustration, and pretence.

- **Defamation - IPC Sections 499 and 500 / BNS Equivalent**

  The sections 499 and 500 IPC concerned criminal defamation and sanction against false pronouncements that aimed at damaging reputation. These provisions find their application in cyber related cases that involve fake profiles, morphed images, and false allegations on the internet.

  Defamation is stored in its altered form in the BNS. The use of criminal defamation is however problematic. It changes the emphasis from victim protection to free speech arguments and does not usually consider the specificity, irreversibility, and virality of reputational damage in the digital context.

- **Insulting the Modest of a Woman - IPC 509 / BNS Equivalent**

  The section 509 of the IPC had criminalized words, gestures or actions meant to hurt the dignity of a woman. Courts have applied it to sexually coloured comments, abusive messages and even online harassment.

  This offence is still perpetuated by the BNS, though the notion of modesty is highly patriarchal. It emphasizes honour over autonomy and dignity hence is improperly positioned to take care of the contemporary digital abuse.

- **Obscenity - IPC 292 / BNS Equivalent**

  Section 292 IPC had criminalized the sale, distributions and circulations of obscene

material. Similar provisions are preserved by the BNS.

Similar to the Section 67 of IT Act, these provisions focus on moral standards more than victim centred harm. They are not able to identify the emotional, psychological as well as professional effects of online sexual abuse.

Other Relevant Laws

- **Indecent Representation of Women (Prohibition) Act, 1986**

  The purpose of the Indecent Representation of Women (Prohibition) Act, 1986 is to outlaw how women are represented obscenely, derogatively, or indecently in advertisements, publications, writings, paintings, or by way of any other form of visual representation. Even though the Act is not digital age, it has been applied so that it applies to digital content, such as posts on social media, online adverts, and websites.

  The applicability of this Act to cyber situations is that objectification is considered a harm. It touches upon commodification and sexualization of female bodies in the public sphere. Nevertheless, the Act is obsolete and is weakly implemented. It does not touch on consent-related offenses like revenge porn, deep fakes pornography, or image morphing. Neither does it offer procedural protections or digitally targeted enforcement tools.

- **Protection of Children against Sexual Offences (POCSO) Act, 2012**

  POCSO act is applicable where the victim is a minor, even in cases of cyber grooming of minor girls, online exploitation and the use of digital pornography. The Act makes it illegal to produce, keep, spread, and even use child sexual abuse material (CSAM).

  The significant thing about POCSO is that it is victim-centred. It identifies psychological damages, procedures favourable to children and trials with time limits. Paradoxically, there is no legislation of this scale and sensitive to adult females against online sexual abuse. This inequality demonstrates that there is structural discrepancy in the Indian law system, as protection is reduced with age.

Overlaps, Ambiguities and problems of Enforcement

The primary issue about the current legal system is that the IT Act, the IPC/BNS, and the special legislation overlap with each other.[12] An example of such an act could be considered a form of revenge pornography that could attract all the following sections of the IT Act Section 66E, 67A (voyeurism), Section 509 (insulting modesty), and defamation cases.

Although the various charges might seem advantageous, they tend to confuse police officers, misframe FIRs, and cause delays in the process. The victims are often forced to walk around a web of legal rights and rules so that it discourages them to seek justice.[13]

Also, majority of the provisions are reactive and not preventive. They punish behaviour when it is too late as the abuse has already happened but do not put prevention systems or controls into place.

Gender-Neutral Drafting and its Consequences

In India, most of the cyber laws are not gender-specific. Although neutrality may seem a progressive path to take, it fails to consider the fact that women are more likely to be targeted through cyber abuse, and that the abuse has gendered characteristics, including sexual harassment, image-based abuse, stalking, and character destruction.[14]

Cybercrime being identified as a type of gender-based violence fails to be established as such, which leads to:

- Inadequate specialised procedures to women victims
- Lack of trauma-based research
- Poor services to assist the victims

[12] Law Commission of India, *Report No. 243: Section 66A of the Information Technology Act, 2000* (2014).
[13] Bureau of Police Research and Development (BPR&D), *Manual on Cyber Crime Investigation* (Ministry of Home Affairs).
[14] UN Special Rapporteur on Violence Against Women, *Online Violence Against Women and Girls from a Human Rights Perspective* (2018).

- Low conviction rates

In contrast to domestic violence or sexual assault legislation, cybercrimes do not experience the principles of bodily autonomy, dignity or equality conceptualisation.[15]

Evidentiary and Jurisdictional Issues

Cybercrimes have special difficulties with gathering of evidence. The digital evidence is easy to delete, edit or store in other foreign servers.[16] There is poor knowledge by the victims to maintain evidence, and law enforcers are not well trained.

Another significant problem is the jurisdiction. Offenders can also be found in other states or countries and thus investigating them will be very slow and complex. The current legislation does not present any straightforward protocols in dealing with transnational cybercrimes most notably those that touch on social media networks whose headquarters are not located within India.[17]

Lack of AI-Specific Regulation

Among the most evident loopholes in the existing legal framework, the lack of the specific regulation of the AI-generated abuse can be singled out. Deep fake pornography, voice morphing, and hyper-real morphing are explicitly not a crime in Indian law. [18]

Although such activity can be loosely classified as obscenity, defamation or even privacy laws, this can only be done loosely. The problem of AI-based abuse brings forth new issues like the matter of consent, authorship, intent, and harm that laws and regulations were established to mitigate in the past.

Critical Analysis of the Legal Framework

Despite the availability of numerous statutory instruments to combat cybercrimes in India, the structure of the system is scattered, obsolete, and lacks gender sensitivity.[19] The

[15] Justice J.S. Verma Committee Report on Amendments to Criminal Law (2013).
[16] Ministry of Electronics and Information Technology (MeitY), *Guidelines for Cyber Crime Investigation and Digital Evidence Handling*.
[17] INTERPOL, *Global Cybercrime Strategy* (2022).
[18] NITI Aayog, *Responsible AI for All – Approach Document* (Government of India).
[19] Apar Gupta & Raman Jit Singh Chima, *Reforming India's Cyber Laws: Need for Rights-Based Framework*,

majority of legislations were also made without fore-seeing the magnitude, velocity, and irreversibility of the digital damage.

Criminal law was to be modernised with the IPC being stipulated as the Bharatiya Nyaya Sanhita. Nonetheless, the BNS does not change substantive reform of IPC extensively, but limits significant changes in the field of cyber gender-based violence.

Due to lack of specific legislation on cyber harassment and internet-based gender-based violence, women have relied on vaguely applicable provisions that cannot identify the severity of online harassment.

Judicial Review: Key Case Law

The Indian judicial system has been instrumental in the interpretation of the existing laws to handle the cybercrimes against women, frequently filling in the gaps in the laws with progressive logic. Without any specific law addressing online gender-based violence, courts have turned to constitutional values, developing conceptions of privacy, dignity, and autonomy, and intensive interpretation of criminal statutes.[20] A number of pioneering cases are an indication of the increasing sensitivity of the judiciary to the online aspect of gendered harm.

State of West Bengal v. Animesh Boxi (2018)

The case is commonly considered the first high profile conviction on revenge porn in India. The accused posted the nude photos of the victim that were morphed by him in pornographic sites after she refused to listen to his house. The Calcutta Sessions Court sentenced him to five years of rigorous imprisonment under Section 354A, 354C, 354D, 509 IPC, and other applicable IT Act provisions.

The significance of this case is that it acknowledges that image-based sexual abuse is a grave offense to dignity, reputation and mental health. The court considered that such acts have a long-term adverse impact on the social identity and emotional stability of a woman. The decision went beyond the conventional ideas about physical injury and identified digital violence as a type of sexual violence. This was a move towards the realization of

Internet Freedom Foundation.

[20] Gautam Bhatia, *The Transformative Constitution* (HarperCollins 2019).

cybercrime as not only a technical crime, but a personal assault of an individual scale.

Shreya Singhal v. Union of India (2015)

Even though it is not a woman-centred case, Shreya Singhal plays an essential role in defining how online speech should be regulated. The Supreme Court overturned Section 66A of the IT Act criminalising offensive or annoyance contents as it was considered to be vague and it breached the freedom of speech under Article 19(1)(a).

The judgment has two implications in the view of gender justice. On the one hand, it safeguards people against an arbitrary arrest. On the other, it eliminated one of the frequently, though not regularly, employed means to limit online harassment. This revealed a regulatory gap wherein victims of online abuse were deprived of a single, highly specific offer of an act on cyber harassment.

The case brings out the conflict between the freedom of expression and the safeguard of digital damages. It highlights the necessity of accurate victim-focused legislation as opposed to the vague censorship-focused laws.

K.S. Puttaswamy v. Union of India (2017)

In this landmark ruling, the Supreme Court acknowledged the right to privacy as a fundamental right to the constitution in the Article 21. The Court ruled that privacy is inherent in human dignity, autonomy and personal freedom.

This ruling has far-reaching effects on cybercrimes against women. It establishes a constitutional basis of claims regarding non-consensual image sharing, voyeurism and deepfake abuse. The Court focused on the fact that individual freedom depends on bodily integrity, informational control, and decisional autonomy.

The verdict allows courts to regard online crimes not as moral violations, but as constitutional ones by connecting the concept of privacy and dignity. It similarly helps to argue that cyber abuse is not a small inconvenience but a gross infringement of rights, which has to be addressed by powerful law enforcement actions.

Relevant High Court Judgements: Court on Cyberstalking and Harassment

Different High Courts have played a leading role in the development of cyber

jurisprudence. Although the case Sabu Mathew George V. Union of India (2018) revolved around the regulation of online content, the Court referred to the accountability of the platforms and the duty of intermediaries to avoid harm.

In online harassment and other cyber-stalking incidents, High Courts have started viewing continuous digital harassment as a criminal offense and not a minor misconduct. The issues have made the courts instruct police to respond to complaints in time, identified the emotional trauma of online abuse, and condemned the insensitive response of law enforcement agencies.

All these judgments represent a change of a morality-based approach to a rights-based one.

Jurisprudential Tendencies and growing Sensitivity

It is evident that a trend has been developing through judicial reactions: courts are becoming more open to engaging in the interpretation of traditional criminal provisions in the context of current digital realities. They are coming to realise that there is irreversible damage to cybercrimes because online information is viral and far reaching.

Nevertheless, the judicial intervention is case-based and reactive. The law can be interpreted by courts, but not adopted instead of detailed legislation. Judicial creativity is still relied upon by the victims instead of statutory clarity.

Law Enforcement Mechanism and Institutional Responses

The success of any legal framework, in many aspects, lies in the enforcement. The application of technology sophistication, jurisdictional boundaries, and social obstacles are complicated problems that the law enforcers in India encounter in the area of cybercrimes against women. Even though various institutional processes have been put in place to deal with cyber offences, their operation is still unequal and, in most cases, victims are not given the chance to receive a timely and sufficient solution.

- **Cyber Crime Cells**

  Specialised units have been put in place in some of the states to investigate technology related offences under Cyber Crime Cells. Case handling through these

cells is anticipated to take care of hacking, internet fraud, cyberstalking, identity theft, and image abuse. Hypothetically, these specialised units are supposed to offer technical skills and quicker redressal.

Nevertheless, practically, lots of cyber cells are understaffed, under-resourced and unequally distributed regions. Cyber units are usually not functional in rural and semi-urban premises, and hence the victims have to turn to the ordinary police unit, which may be technically incompetent. Moreover, non-immediate forensic analysis and reliance on third parties to provide the services undermine the quality of investigations.

- **National Cyber Crime Reporting Portal**

To improve online complaints especially racial crimes involving women and children, the National Cyber Crime Reporting Portal was launched to allow the victims to make complaints through the internet. This portal offers the possibility to report anonymously under some categories and submit the evidence digitally.

Although the portal is a new step to a new direction, their practical use is still restricted. A very large number of the victims have a problem navigating the interface, reading about the types of legal categories, and uploading evidence. Also, cases received with past complaints made via the portal take a long time before they are handed over to the local police stations. Absence of real-time tracking and lack of sufficient follow-up mechanisms further decrease confidence on the system by the people.

- **Role of Police and Investigation Challenges**

The police act as the main gatekeepers of a criminal justice system. They play an important part in registering the FIRs, gathering evidence, and making investigations. Nevertheless, there are a number of problems which remain.

First, most police officers still consider cyber bullying a mundane or non-serious crime especially where no physical injury is taken. The victims are often discouraged to file any formal complaint. Secondly, cyber offences are anonymous

and transnational and therefore it is challenging to identify the individuals perpetrating them. Third, digital evidence, including deleted messages, temporary or encrypted products, is volatile, thus making forensic procedures more difficult.

Another problem that impedes investigations is jurisdictional confusion. Crimes that are committed internationally among states or countries necessitate inter-agency co-ordinations, which are usually slow and bureaucratic.

- **Training Gaps Across Enforcement Agencies**

  Lack of specialised training in the form of one of the most crucial institutional shortcomings. The field of cybercrime investigation needs technical expertise, legal knowledge, and consideration to the victims. But the majority of police education courses are obsolete and do not pay enough attention to computer crimes.

  Officers do not have the acquaintance to the new technologies like artificial intelligence, deepfakes and encrypted communications. The result of this is inadequate framing of the charges, poor handling of evidence and poor critiquing of the prosecution.

  The lack of gender-sensitisation training is also important. Cyber abuse victims usually develop humiliation, fear, and trauma. Detecting insensitive questions, victim-blaming, and dismisses encourage disrespect and encourage injustice in the system.

- **Critical Assessment**

  Even though institutional efforts to combat cybercrime have been realized in India, the ecosystem of enforcement is still too little and sporadic. The infrastructure deficits, expertise deficit, and culture biases in law enforcement remain to hinder the access of the victims to justice. Meaningful protection of women in the cyberspace cannot be achieved solely by legal provisions unless these changes are systemic, technological and sensitising.

Legal Gaps in Addressing Cybercrimes Against Women

Although there are various statutory provisions under the Information Technology Act,

2000 and the Bharatiya Nyaya Sanhita (previously IPC), the legal provisions do not seem to have been updated forms of cybercrime against women. The technology-law disconnection has generated severe constraints in protection, enforcement and redressing to victims.

- **Obsolete Definitions in the IT Act**

  IT Act was implemented in 2000 when there were no social networks, smart devices, messaging encryption, and AI or various other technologies in existence. Therefore, much of its definitions and crimes are not able to reflect recent forms of digital abuse. Deepfake pornography, AI morphed images, doxxing, and organised online harassment campaigns are not explicitly mentioned in the statute.

  The areas concerned with obscenity and sexually explicit material pay much attention to publication or transmission, however, they do not emphasise on non-consensual production or alteration of digital images. This leads to the law enforcement depending on wide or farfetched interpretations which compromises the legal certainty and usually to the advantage of the accused.

- **Lack of a specialised Law on Cyber Harassment**

  Cyber harassment is not yet accepted by the Indian law as a separate and independent offence. Rather, law enforcers seek to align online abuse to existing norms as stalking, defamation, obscenity or insult to modesty. These agreements were initially designed to cover physical-world crimes and do not entirely apply to the continuous online harassment, trolling, or organised hate speech.

  Cyber harassment is frequently recurring, secret and site (platform)-related harassment that causes serious psychological injury that might not satisfy the technical components of any prevailing wrongdoing. Lack of a specific legal clause leads to under-classification, watering down of charges as well as inconsistency in judicial interpretation.

- **Jurisdictional Issues**

  Hackings and cybercrimes often go across borders. A perpetrator can be placed in

one state or country and servers in another jurisdiction and the victim in another. Indian criminal law, however is territorial in its functioning of the procedure to a great extent. Delay and frustration to the victims are caused when even police stations decline to accept complaints on the basis of lack of jurisdiction.

As much as there are arrangements of extraterritorial use, enforcement would prove to be slow and complex unless international cooperation is provided. This legal-technical incompatibility provides impunity to out-of-local-jurisdiction offenders.

- **Absence of Victim-Centric Procedures**

Procedural law is still not sensitive enough to address the victims of cyber abuse. No standard procedures exist in the instant of taking down non-consenting intimate image, retention of digital evidence, and psychological assistance. The victims are also made to repeatedly recount traumatic events in the absence of privacy protection.

The protection of anonymity of complaints is not always provided, even though there is the stigma that is attached to the image-based abuse. The system is still imposing procedure to victims as opposed to guaranteeing timely protective action.

- **Delays in Investigation and Trial**

Cybercrime investigations entail computer forensics, cross-plateau partnership, and computer abilities, all of which add to delays. Clogged laboratories and bottlenecks in the procedures impede collection of evidence. When cases get to trial, digital evidence can be lost, accounts deleted or trails erased.

Delays in judicial systems also undermine deterrence as the victims of the litigation lose confidence in the system and culprits get away without facing justice in time.

- **Overall Assessment**

Thereby, in as much as India has a quilt of legal stipulations, the system is non-technologically modern, lacks conceptual clarity, and procedures that are victim-centric. The law is a potential reactive tool, not a proactive tool unless there are

special measures, which are demanded to curb swiftly changing forms of cyber threats on women.

Emerging Challenges in the Digital Age

This is due to the accelerated development of the digital technology, which now presents new kinds of cyber harm that current legal and enforcement systems do not cope with. Women, especially, have new threats that are more advanced, unidentified and impossible to track.

- **Deepfakes and AI-Generated Abuse**

  The development of artificial intelligence has led to development of extremely realistic forged images, video clips and audio clips. The use of deepfake is becoming more and more pronounced towards overlaying the faces of women on overt material with no apprehension, resulting in extreme damage, reputations, and mental. In comparison to traditional morphing, AI-generated material is more difficult to locate and to further propagate on a large scale. This is because current obscenity and defamation laws are silent on synthetic media and the agencies that enforce their laws must find ways of extrapolating the old-fashioned laws as per the new-fashioned crimes.

- **Encrypted Platforms and Anonymity**

  It is also rather hard to track the offenders as end-to-end encrypted messaging services and anonymous social media accounts make it hard to track the users. Offenders may use VPN, false accounts, or temporary profiles and harass, intimidate, or blackmail women. Although encryption guarantees the privacy of users, it has security implications by posing investigative obstacles, not all law enforcement agencies have access to identification information as fast as necessary. Privacy versus accountability is one of the senior legal policy conflicts.

- **Cross-Border Cyber Offences**

  Various cybercrimes are based out of India and criminals capitalise on the various jurisdictions and capability between the two countries. Hosting servers, domain

names and platform ownership can be based in other countries, which implies that mutual legal assistance treaties (MLATs) and international collaboration are needed. These are long and bureaucratic, thus enabling the offenders to escape responsibility. The internet has become borderless and has overtaken criminal justice systems which are territorially limited.

- **Accountability of Social Media Platform**

  The responsibility of spreading abusive content lies at the centre of social media firms yet they have little responsibility. Opaque redress grievance systems, haphazard moderation and slow removal of content have an ineffective consequence as it leaves victims without relief evidenced in time. Although the intermediary liability regulations demand the platforms to demonstrate due diligence, this is not consistently enforced and the victims are often unable to have the harmful content removed in time.

- **Lack of Digital Literacy Among Women**

  Many women, especially in rural and semi-urban communities, are not aware of the online safety software, privacy, and legal solutions. Poor digital literacy makes them susceptible to phishing attack, blackmail and impersonation. Silence and under-reporting are also due to fear of social stigma and knowledge gap on ways of reporting.

Comparative Perspective

Comparison of the regulations of other states, which contain provisions on online abuse, presents a good idea to enhance the Indian response to cybercrimes against females.

- **United Kingdom**

  The issues related to online harassment are covered by the Malicious Communications Act, 1988 and the Communications Act, 2003, which are the main legal regulations of the United Kingdom. These legislations are used to criminalise electronic communication that is grossly offensive, threatening or is aimed at causing distress or anxiousness. Online Safety Act, 2023 has also broadened the

platform responsibility, which is the requirement that the tech companies actively help to prevent harmful content, such as image-based abuse and online harassment. The UK scheme is also important because it specifically acknowledges that digital communication can harm one and puts more regulatory responsibilities on the social media networks.[21]

- **United States of America**

No one comprehensive federal mechanism regarding cyber harassment exists in the United States, yet a number of federal and state-wide laws exist that concern online abuse. The laws governing cyberstalking, interstate threats and non-consensual sharing of intimate images are implemented using the federal provisions like 18 U.S.C. SS 2261A (cyberstalking). A large number of states have created particular laws on revenge porn. The civil remedies which include restraining orders and tort claims also offer alternative modes of relief to the victims. But powerful protections of free speech under the First Amendment at other times restrict criminal prosecutes.[22]

- **Lessons For India**

These models have important lessons to offer to India: a specific legislation against cyber harassment is required, the harm based on psychology and image needs to be better identified, and the responsibility of the platform must be reinforced. Victim-friendly solutions in combination with an active regulatory framework would be of significant service to ensuring the protection of women digitally.

Recommendations

- **Need for a Dedicated Cyber Harassment Law**

India does not have a well-defined law that directly responds to online gender-based abuse. There should be a specific law specifying the offence that includes cyber

[21] UK Government, *Online Safety Act 2023* (UK Parliament), https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.
[22] USA – Cyberstalking & Revenge Porn Laws:
U.S. Department of Justice, *Cyberstalking and Cyberharassment Laws in the United States*, 2022, https://www.justice.gov/criminal-ccips/cyberstalking

harassment, doxxing, sexual abuse on a deepfake basis, and spreading intimate images without the consent of the victim. This would be an acknowledgement that these are different crimes, which would be enforced with a uniformity as a specific crime.

- **The amendments to the Information Technology Act, 2000**

  IT Act has to be amended according to the realities on the ground. It should be specifically covered with AI-generated works, deepfake abuse, and identity morphing. Consent should be defined more clearly, the standards of the digital evidence, the responsibility of intermediaries should also be defined in a more concise way, to seal the boundaries of interpretation.

- **Fast-Track Cyber Courts**

  Failure to deliver justice and trial promptly undermines deterrence and increases victimisation. This can be achieved by creating special fast-centred cyber courts that have trained judges and prosecutors that will help to dispose of cases connected with internet mistreatment quicker and enhance judicial knowledge of technological evidence.

- **Social Media Accountability and AI Regulation**

  The social media sites need to have greater legal responsibility in order to stop and delete the negative contents. They should be imposed with time limitations on taking down, the existence of transparent grievance systems, and the punishment of failure to comply. Moreover, artificial intelligence technologies that can create intimate deepfakes need to be controlled by the use of compulsory protective mechanisms and traceability requirements.

- **Awareness and Legal Aid to Women**

  The protection against laws cannot work unless the victims know their rights. National digital literacy education, higher education campaign and easy access to free legal services and psychological counselling are all necessities. Women empowerment, where they are informed and given systems that support them in

terms of reporting and recovery can also go a long way.

Conclusion

The Indian digital growth has provided opportunities of education, employment and expression particularly to women. However, gender-based violence reproduction has also been replicated through new and more pervasive forms through the same online spaces. Cyberstalking, harassment over the Internet, non-consented sharing of images, sextortion, and deepfake abuse due to artificial intelligence indicate that technology is used wrong to impinge on the dignity, privacy and autonomy of women.

As can be seen in this project, despite having a number of legal provisions in place in India vacuously in response to the Information Technology Act, the Bharatiya Nyaya Sanhita, and other laws, the framework is schizophrenic and can only partially be said to be functional. The lack of the law, enforcement, jurisdictional challenges, poor reporting, and a lack of digital awareness limits the access to justice by victims. Meanwhile, the ever-changing technologies, as well as anonymous Internet networks, are complicating cyber crimes and make it difficult to control them.

The problem requires immediate and joint intervention. With the rising presence of women in the digital world, legal and institutional reactions need to keep up on the changing technology. Laws: It is necessary to strengthen the laws, enhance enforcement, and hold the platform accountable in order to create a safer cyberspace. Finally, any action to protect women online is not only about cyber regulation but also the primary focus of gender justice and the protection of essential rights in the digital era.