International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 10-10-2025, Accepted: 09-11-2025, Published: 24-11-2025
Volume 11, Issue 11, 2025, Page No. 115-123

Cyber space and women's safety: A socio-legal study of emerging threats

Dr. Inderjit Kumar[1], Khushbu[2]
[1] Assistant Professor, Department of Law, St. Soldier Law College, Jalandhar, Punjab, India
[2] Department of Law, Guru Nanak Dev University Regional Campus, Jalandhar, Punjab, India

Abstract
Over the years, technology has made widespread development at global level. This technological development has many advantages like increased productivity, improved education and easy access to information, however alongside these advantages it has a dark side too and this side is cybercrime. Cybercrimes are committed against different sections of society but one of the most vulnerable sections which is prone to cybercrime is 'Women'. Cybercrime against women is a serious concern as it is growing at a fast pace and need to be dealt with it. This article examines the rapid growth of cybercrimes committed against women including cyber-stalking, cyber-bullying, cyber-pornography, morphing, cyber-harassment, cyber-sex trafficking, cyber-grooming and phishing. Further, it also focuses on legal framework, enforcement mechanism and methods to combat the prevalence of cybercrime against women. Inadequate legal framework and lack of awareness among people are the prime causes for growing cybercrimes which can be dealt with by providing better training and resources to enforcement agencies and creating awareness among women about these crimes.

Keywords: Cybercrimes, information technology Act, 2000, bhartiya nyaya sanhita (BNS), 2023, indecent representation of women (prohibition) Act, 1986

Introduction

Today's era is known as digital era where internet has become integral and vital part of everyone's life. With the use of internet and technology, it becomes easy to communicate and interact with people through various social media platforms and websites. But at the same time, it has become a significant threat to the society especially women who are most vulnerable to this threat. Although women are considered 'Goddess' in Indian society, yet they face a lot of societal oppression due to patriarchal system of our society in which women are considered lower as compared to men. In this context, the digital landscape has birthed a dangerous new dimension of violence: cybercrime. Consequently, ensuring women's safety has become an increasingly urgent and critical public concern.

Cybercrime is defined as any unlawful activity where a computer, a phone, a network, the internet or any electronic device is used as the primary tool to commit the crime, the target of the crime, or both.

The Cambridge Dictionary defined the term cybercrime as, 'Crime or illegal activity that is done using the internet'. [1]

According to Oxford dictionary, cybercrime means 'Criminal activities carried out by means of computers or the Internet.' [2]

According to Dr. Debarati Halder and Dr. K. Jaishankar, cybercrime is defined as: 'offences that are against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss of victim directly or indirectly, using modern telecommunication networks such as internet (chat rooms, emails, notice – board and groups) and mobile phones.' [3]

Cyber stalking, cyber bullying, cyber pornography, morphing, cyber harassment, phishing and cybersex trafficking are most common type of cybercrime of which women are victim at the present time. Social media platforms like Meta, Instagram, Twitter, Snapchat become main spot for the commission of cybercrimes where morphed photos or videos, or personal information of women are published for blackmailing or financial gains. According to Annual Report of 2023-2024 of National Commission of Women total of 657 complains were lodged with the commission related to cybercrime against women making it third highest category of complaints received. [4] Different laws like 'Information Technology Act, 2000', 'Indian Penal Code, 1860' now called as 'Bhartiya Nyaya Sanhita, 2023', and 'Indecent Representation of Women Act, 1986' were enacted in India providing punishment for cybercrimes and enforcement agencies yet a lot needs to be done in this field to combat the growing menace of cybercrime against women.

Types of Cybercrime Against Women

Cyber stalking, cyber bullying, cyber pornography, morphing, cyber harassment, cyber grooming, cybersex trafficking and phishing are most common and prevalent cybercrimes committed against women at the global level. These cybercrimes are discussed below:

1. **Cyber stalking:** Stalking, in general sense, implies following someone in order to harass or threaten them. When a person follows someone online then it is termed as cyber stalking. In other words, when a person misuse internet services, social media platforms or emails with a view to stalk, threat or intimidating someone, it is termed as cyber stalking. In this crime, perpetrators used to monitor the victim's social media activities obsessively and repeatedly attempting to establish personal interaction despite women's explicit and clear disinterest or without women letting know. It is a repeated and ongoing process of unwanted actions on the part of offender without any kind of physical interaction with the victim.

2. **Cyber Bullying:** Use of electronic means to bully a person is called cyber bullying. It is often done through sending intimidating or threatening messages, posting bad remarks on the internet to upset or provoke the victim, circulating private and sensitive information online about someone without their consent [5]. It can lead to fatal consequences like mental harassment, anxiety and low self-esteem for the victim. A survey by the Cyber and Media Cell of the Delhi Police found that 40% of cyberbullying victims in India were women. [6]

3. **Cyber Pornography:** Cyber pornography is a distinctive and major cybercrime against women. The word Pornography refers to the image, video or other content depicting sexualized acts to stimulate erotic feelings. Cyber Pornography means the publishing, distributing or designing pornography by using cyberspace. [7] With the use of technology number of images and videos of women are circulated on the different website and social media platforms depicting pornography. Such pornographic content uploaded without victim's consent lead to physical and mental trauma and damage to reputation of women. Even children are not exempted from being targeted by this form of cybercrime.

4. **Morphing:** Morphing is an act of altering or manipulating images and videos to create fabricated versions of original ones. Earlier this method was used by filmmakers or artists for the purpose of animation or for doing some creative work. But at present, cyber perpetrators started misusing this method of morphing for unlawful and illegal purposes and women are most targeted section. Women's images and photos are sometimes morphed by altering their face or body or by removing their clothes depicting objectionable and obscene content. The purpose behind the commission of this cybercrime involves revenge, defamation or blackmailing. Recent technologies like AI and deep fake are main contributor to the growing menace of morphing.

5. **Cybersex Trafficking:** This form of human trafficking involves victims being lured or coerced into engaging in intimate acts that are broadcast or streamed on internet websites or digital platforms. In this offence, the live streaming of forced intimate acts [8] takes place. Victims are often deceived through fake job opportunities or false relationship promises and are compelled to perform intimate activities online. Unlike traditional commercial exploitation trafficking, victims in this context do not have direct physical contact with the perpetrators. Women and children are most frequently targeted in this form of online exploitation.

6. **Cyber Grooming:** Cyber grooming is a crime in which perpetrators develop a friendly and emotional relationship with people online with the hidden intention of forcing them to share their private or nude images and videos engaging in sexual activities. Then they use these photos and images to blackmail victims. As women are more emotional and easier to manipulate, perpetrators use emotional means to manipulate and exploit them.

7. **Identity theft:** Identity theft implies stealing the identity of another. In this type of cybercrime an offender steals the identity of another person like his/her name, password or signature etc. And then use this information to commit an offence like credit card fraud [9], creating fake profiles or harassing impersonated person. This crime is very prevalent against women as fake profiles are created by cyber offenders on the name of such women to harass or threaten them.

8. **Phishing:** Phishing is a process of stealing information through fake emails. It involves fraudulent act of obtaining personal information like bank details, credit card or debit card details, OTP or any password. [10] The cyber criminals appear to be legitimate source such as a trusted website, bank or service provider and lure people to provide their sensitive information and when people on believing such emails trustworthy provide their information criminal save that information and then use such information against them. As women are easier to manipulate so cyber criminals prefer to target them by sending fake emails.

Legislation Against Cyber Crime in India

With a view to combat the growing menace of cybercrimes against women different laws are enacted by legislature in India. These laws include 'Information Technology act, 2000', 'Bhartiya Nyaya Sanhita, 2023' previously known as 'Indian Penal Code, 1860' and 'Indecent Representation of Women Act, 1986'. These enactments are discussed as below:

Information Technology Act, 2000

The Information Technology Act 2000 was enacted with the objective of giving legal recognition for electronic transactions such as e-commerce, creating a legal framework to support the growth of the IT sector and providing protection against misuse of any activities related to e-commerce.

According to recent report published by NCRB in the year 2022, total number of women centric cybercrime cases reported in India under Information Technology Act, 2000 are 2940 out of which 2774 cases reported in states while 166 cases reported in Union Territories with total crime rate of 0.4%. Total of 2614 reported cases were disposed off by the police under IT Act. In other women centric cybercrime including blackmailing, morphing, fake profiles and defamation etc. Total 689 cases were reported in India out of which 680 were reported in states and 9 were reported in Union Territories with a crime rate of 0.1%. [11]

Though IT Act does not make any specific provision relating to protection of women from cybercrime there are general provisions which are applicable to women also and these are as follows:

Section 65: Tampering with computer source documents

Any person who knowingly or intentionally conceals, destroys or alters, or causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable.

So, if a person knowingly or intentionally does himself or cause another person to do an act in three forms namely concealment, destruction or alteration of any computer source code used for computer or computer program, system or network containing any information relating to women, then he is said to commit an offence of tampering with computer source against women. [12]

Section 66C: Identity theft

Whoever fraudulently or dishonestly makes use of the electronic signature, password, or any other unique identification feature of any other person shall be punished.

Identity theft refers to misuse of the identity of another in order to commit an offence. This section was enacted with aim of protecting the identity of users online. As per this section, if a person unlawfully uses the identity of another person, particularly, of a woman, for instance electronic signature, password of any device or social media accounts or any kind of her unique identification feature with fraudulent and dishonest intention he is said to have committed the offence of identity theft of women. The offence of identity theft is completed the moment there is dishonest or fraudulent downloading, extracting or copying of electronic signature, password etc.

Section 66D: Cheating by personation by using computer resource

Whoever by means of any communication device or computer resource cheats by personating, shall be punished.

Personation, in general terms, means pretending to be someone else. [13] If a person uses any means of communication device like phones, computers, tablets etc. or any electronic source to personate a woman with intention of cheating and inducing a person to accept, agree, transact or deliver any information or data then, offence of cheating by personation is committed against women. Cheating on the person under this section does not include only impersonated person but also those who are being deceived by the said act.

For example: if a person creates a fake profile of women on matrimonial or other networking website with the intention to cheat then he is liable to be punished under sec 66D of IT Act, 2000.

Section 66E: Violation of privacy

Any person who, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished;

'Publishes' means reproduction in the printed or electronic form and making it available for public.

Transmit means to electronically send a visual image with the intent that it be viewed by a person or persons.

This section was introduced to criminalize unauthorised [14] and non-consensual capturing and publication of private images of a woman in electronic form. According to this section, if a person does the act of capturing, publishing or transmission of image of a private area of women with intention or knowledge, then he is liable for violating the privacy of women. Consent of women is an essential for holding someone liable under this section. If the particular act was carried out with the consent of a woman then that act does not attract liability under this section. Installation of spy cameras, hidden cameras or any communication device with intent to violate the privacy of women falls under this section.

Section 67: Publishing or transmitting obscene material in electronic form

Any person who, publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished.

This section was added with the purpose to put limitations on the publication or transmission of obscene material in electronic form. Publication or transmission of obscene material such as image or video depicting women involved in sexual acts or in private act etc. are made penalized under this section.

In Ranjit D. Udeshi v. State of Maharashtra [15], Supreme Court held that main test of obscenity is whether the tendency of the matter charges as obscene is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall. In this connection the interest of our contemporary society and particularly the influence of the book on it must not be overlooked. Court also held that sec 292 of IPC (294 BNS) is a reasonable restriction on freedom and speech of expression under Article 19(1) of India constitution as it makes sure that decency and morality to be maintained.

Sec 294 of Bhartiya Nyaya Sanhita, 2023 coincide with section 67 of IT Act, 2000 as it also deals with the publication of obscene material.

Sec 294 of Bhartiya Nyaya Sanhita: Sale etc. of obscene books etc.

Sub section (1) of said section explain obscenity as, ' a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, including display of any content in electronic form shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.'

Sub section 2 punishes those who sell, distribute, exhibit, import, export or in any manner convey publicly the obscene books or any other material of the same effect.

Sec 67 of IT Act and 294 of BNS are complementary to each other as they both regulate publication of obscene material whether online or offline. While offence under section 67 IT Act, 2000 is specifically deals with publication or transmission of obscene material in electronic form, section 294 Bhartiya Nyaya Sanhita, 2023 has a broader scope and deems any content displayed, both in, electronic form as well as in physical form in book, pamphlet, paper, writing, drawing, representation, figure or any other object of it, obscene if it is lascivious or appeal to prurient interest or if it has tendency to deprave or corrupt the mind of person.

State of Tamilnadu v. Suhas Kutti [16]

was the first case of cybercrime conviction under Information Technology Act, 2000. In this case, accused, a friend of victim wanted to marry her, but she married someone else. After her divorce he tried again to marry her but this time too she rejected him. On this rejection out of frustration he posted victim's phone number and offensive

remarks against her on different forums falsely suggesting that she was soliciting. In consequence of this she started receiving degrading and harassing calls from people. Accused also made fake accounts of victim on Yahoo with objective of damaging victim's reputation. He was charged and then sentenced under section 67 of Information Technology Act, 2000 by the court of Chief Metropolitan Magistrate.

Section 67A: Publication or transmission of material containing Sexually explicit act etc. In electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct, shall be punished.

As per this section, if a person publishes, transmits or disseminates any material containing sexually explicit act [27] or conduct of women or related to any women and such publication or transmission is in electronic form then that person shall be liable for committing the offence against women under this section. The core of offence under this section is the explicit nature of content. This is a stringent provision added to curb the electronic dissemination of sexually explicit content involving women.

Section 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. In electronic form: Whoever

a. Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
b. Creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
c. Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
d. Facilitates abusing children online; or
e. Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children shall be punished

This section punishes those who publish or transmit, create text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distribute material in electronic form which depict children in obscene or indecent or sexually explicit manner [18] or cultivates, entices or induces children to online relationship or records in any electronic form own abuse or that of others and if the children involve girl child then it will constitute the offence of cybercrime against women.

As per the NCRB report of 2022, total 2251 cases were reported specifically under section 67A and 67B of Information Technology Act, 2000 for publishing or transmitting sexually explicit material. Out of these 2251 cases 2094 cases were reported in states and 157 cases were reported in Union Territories with a crime rate of 0.3%. [19]

In Avinash Bajaj v. State [20] a listing offering an obscene MMS video clip with description 'DPS girl having fun' took place on a website named as Baazee.com and offence was made out under section 67 of IT Act for publication of obscene material. Delhi High court observed that 'the text of listing leaves no doubt that the object being offered for sale was obscene. By not having appropriate filters that could have detected the words in the listing or the pornographic content of what was being offered for sale, the website ran a risk of having imputed to it the knowledge that such an object was infact insane. The advertisement might itself have been inserted by seller, but website facilitated the sale by carrying the listing which informed the potential buyer that such a video clip that is pornographic can be procured for a price. Therefore, it cannot be said that baazee.com in this case did not even primary facie cause the publication of obscene material.

Section 72. Breach of confidentiality and privacy.

If any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished.

This section was enacted with the purpose to protect and ensure confidential information and to punish those who has unauthorized access to any information without the consent of disclosing party.

As per report total of 916 cases of women centric cybercrime under IT Act, 2000 were true but there were insufficient evidence in these cases which is one of the major cause of increasing acquittal rate. The pendency percentage of cybercrime under IT Act is 77.2%. [21]

Bhartiya Nyaya Sanhita (Bns), 2023

The Bhartiya Nyaya Sanhita was enacted in the year of 2023 and came into force on 1st July 2024 replaced Indian penal code,1860. This law made wide provisions relating to crime against women under Section 75, 78, 79 which were previously 354A to 354D under Indian Penal Code, 1860 added through Criminal Amendment Act, 2013.

Section 75. Sexual Harassment

1. A man committing any of the following acts

1. physical contact and advances involving unwelcome and explicit sexual overtures; or
2. a demand or request for sexual favours; or
3. showing pornography against the will of a woman; or
4. making sexually coloured remarks.

This section is gender-specific and is particularly designed to safeguard women from gender-based harassment by men. As per this provision, if a man engages in conduct explicitly mentioned under Section 75 of the Bharatiya Nyaya Sanhita—such as unwelcome and explicit intimate behaviour, solicitation for intimate favours, [22] displaying pornography against a woman's will, or making indecent or intimacy-related remarks—he shall be punished for the offence of gender-based harassment of women. When such acts are carried out through electronic means or online platforms, they are categorised as cyber offences against women.

Punishment for offences fall under (i), (ii), (iii) of section 75 is up to 3 years or fine or both whereas Punishment for offences fall under (iv) is up to 1 year or fine or both.

Section 77: Voyeurism

Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with Imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be able to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall abo be liable to fine.

This section penalizes those acts which violates the privacy of women. It punishes those who watches or captures the image of a woman engaged in a private act under circumstances where she reasonably expects privacy and believes that no one is watching or observing her. A mere act of dissemination of image of woman engaging in private act is made an offence under this section.

If women consent to capture image of her engaging in private act but does not consent to its dissemination then a person, if disseminate such images, shall be punished with voyeurism. [23] The offence of voyeurism is considered as an offence which undermines the right to privacy, dignity and bodily autonomy of a woman. Acts involving electronic transmission or dissemination of image of woman can also attract section 66E (violation of privacy) and section 67 (publication or transmission of obscene material) of IT Act, 2000.

Section 78: Stalking

Any man who

1. Follows a woman and contacts, or attempts to contact such woman to faster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
2. Monitors the use by a woman of the internet, e-mail or any other form of electronic communication, commits the offence of stalking.

Stalking means following someone with the intention of harassing or threatening. Sec 76 BNS contains twofold offences firstly, following a woman and contact her to develop personal interaction despite a clear indication of disinterest by such woman and secondly monitoring the use of internet, email or any other electronic communication by women which constitute cybercrime against women. Attempt to contact a woman is in itself a punishable offence under this section. One of the essential ingredients of an offence under section 76 BNS is that the act of stalking must have been done repeatedly by the offender.

Ritu kohli v. Manish Kathuria [24] is first case related to cyber stalking, in this case Manish Kathuria who is a culprit used to stalk Ritu Kohli by following her on chat website and abused her. He disseminates victim's phone number to various people. After that, he started chatting on website www.mirc.com under victim's identity and used obscene and filthy language. Due to this she started receiving obscene calls from people. On reporting the matter to police culprit got arrested under section 509 IPC for outraging the modesty of women. However, this section does not cover cyberstalking. But through this case government realized the need to deal with cyberstalking as a result sec 66A was introduced in Information Technology Act, 2000 which deals with punishment for sending offensive messages through communication services etc. But in the case of Shreya Singhal v. Union of India [25] Struck down section was struck down as it curtails the freedom of speech and expression of people.

Section 79: Word, gesture or act intended to insult modesty of a woman.

Whoever, intending to insult the modesty of any women, utters any words, makes any sound or gesture, or exhibits any object in any form, intending that such ward or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such women, he shall be punished with simple imprisonment for a term which may extend to three years, and who with fine.'

This section does not explicitly contain any provision relating to cybercrime but if any person through online communication, message, gesture or otherwise with the use of electronic means commit an act intruding upon the privacy of women amounting to outrage her modesty then he shall be liable for such act.

Section 111: Organized crime

Any continuing unlawful activity including kidnapping, robbery, vehicle theft, extortion, land grabbing, contract killing, economic offences, cyber-crimes, trafficking in people, drugs, illicit goods or services and weapons, human trafficking racket for prostitution or ransom by the effort of groups of individuals acting in concert, singly or jointly, either as a member of an organized crime syndicate or on behalf of such syndicate, by use of violence, threat of violence, intimidation, coercion, corruption o related activities or other unlawful means to obtain direct or indirect, material benefit including a financial benefit, shall constitute organized crime.

Earlier, the provision of organized crime was not included in IPC. In BNS, this provision has been added under section 111 and cybercrimes are explicitly recognized under the definition of organized crime. Organized crime syndicates have expanded their operations into the realm of cybercrime, including hacking, identity theft, online fraud, and cyber espionage. When target of such organized crime is women, it constitutes an offence of organized crime against women. This section aims to prevent cyber criminals acting in groups or on behalf of syndicate and provides a comprehensive tool to prosecute them for involving in digital offences that affect women's dignity and privacy.

Indecent representation of women (prohibition) act, 1986.

Indecent Representation of Women Act, 1986 was enacted with the objective of prohibiting indecent representation of women through advertisements or in publications, writings, paintings, figures or in any other manner irrespective of the medium used. This Act defines indecent representation of women as any depiction of woman's figure, her form, body or any part in such a manner that is obscene, indecent, derogatory to women or which may deprave, corrupt or harm the public morality or morals. [26]

Section 3. Prohibition of advertisements containing indecent representation of women. No person shall publish, or cause to be published, or arrange or take part in

the publication or exhibition of, any advertisement which contains indecent representation of women in any form.
This section prevents the dissemination of advertisements which portray or depict women indecently. [27] It punished an indecent representation of women in advertisement regardless of medium used for publication or exhibition of any advertisement including digital and e-advertisements under their ambit making it an offence of cybercrime. Mere participation in the publication or exhibition of such an indecent advertisement is sufficient to constitute an offence under this section.

Section 4. Prohibition of publication or sending by post of books, pamphlets, etc., containing indecent representation of women. No person shall produce or cause to be produced, sell, let to hire, distribute, circulate or send by post any book, pamphlet, paper, slide, film, writing, drawing, painting, photograph, representation or figure which contains indecent representation of women in any form.
Section 4 of the Act prohibits the production, sale etc. of any book, pamphlet, paper, slide, film, writing, drawing, painting, photograph, representation or figure which contains indecent representation of women in any form. If any person distributes or circulate the material prescribed under this section by sharing, forwarding or uploading on digital platforms containing indecent representation of women then it will fall under offence of cybercrime against women and that person shall be punished under section 6 of the said Act.

Legal Provisions Relating to Cybercrime Against Women in Global Context
The Budapest Convention, officially known as the Convention on Cybercrime, was the first international treaty to address crimes committed via the internet and other computer networks. The Convention covers offences such as illegal access to computer systems, data interference, computer-related fraud, and the creation and distribution of child exploitation material. [28] However this convention provides general provisions that apply to all individual regardless of gender without specific focus on cybercrime against women.
In UK cyber harassment is primarily regulated by the 'Protection from Harassment Act, 1997' which states that a person must not pursue a course of conduct which amounts or he knows or ought to know amounts to harassment of other. However, this act is considered conservative to regulate gender centric cyber harassment. While the Computer Misuse Act, 1990 was enacted with the aim of protecting both men and women from unauthorized access to computer material, it also serves the need for preventing acts that amount to harassment of women. The Criminal Justice and Courts Act, 2015 criminalized the disclosure of private intimate photographs or films. The Malicious Communications Act, 1988 aims to protect individuals from cyber-trolling through messages or comments that cause anxiety or distress to the victim. [29]
Despite being a global power USA is also not protected from dark and ugly side of internet i.e. cybercrime. In US, there is no national legislation for protection against cybercrime against women instead states have enacted their own laws relating to cyber stalking and harassment. States such as Albama, Arizona, Hawaii etc. enacted laws prohibiting harassment by electronic means, computer or email communication. Texas enacted the 'Stalking by Electronic Communication Act, 2001'. [30] US federal Anti-Cyber stalking law was enacted in 1999 in California with aim to prevent cyber stalking. The Computer Fraud and Abuse Act, criminalizes unauthorized access to computer network or systems. Privacy Act of 1994 provides safeguards against invasion of privacy through misuse of records by federal agencies.
Recently UN General Assembly passed a resolution for combatting cybercrime recognises the importance of addressing cybercrimes. While this resolution does not explicitly focus on cybercrime against women, it recognizes the impact of cyber-related offenses such as cyber stalking, online harassment and non-consensual dissemination of images on vulnerable groups, including women and children.

Methods of Protection Against Cybercrime
Following are the measures which women can employ to protect them from cybercrime:

1. **Strong, Unique Passwords:** Every application and site require a password. This password must be complex, utilizing a minimum of 14 characters, and be a combination of uppercase and lowercase letters, numbers, and symbols. [31] Crucially, never reuse the same password across multiple sites or applications; use a password manager to securely store unique credentials.

2. **Multi-Factor Authentication (MFA):** MFA requires two forms of verification to access an account, significantly raising the barrier to unauthorized entry. If a criminal compromise a password, they are still blocked without the second factor (e.g., a time-sensitive code sent to a phone or generated by an authenticator app). MFA should be enabled on all critical accounts.

3. **Avoid Sharing Sensitive Information:** Users must be highly mindful of the personal information they share online, including photos, videos, and location data, especially with strangers. Oversharing can lead to misuse for purposes like identity theft, pornography, or blackmail. Always pause and evaluate the risk before posting content or providing details on social media.

4. **Regular Software and System Updates:** System flaws or 'vulnerabilities' are often exploited by cybercriminals. Vendors release regular software and operating system updates specifically to 'patch' these security gaps. Preventing exploitation requires diligently installing all updates as soon as they are available.

5. **Avoid Suspicious Links (Phishing Defence):** Many cybercrimes, including credential theft and malware delivery, are committed using malicious links (phishing). Always verify the sender's identity and the link's destination before clicking. Ensure the website URL begins with 'https' (secure) before entering any sensitive data. If in doubt about an email, verify the communication through an official channel (like calling the organization directly).

6. **Strict Privacy Settings:** All social media and online accounts should be set to the highest possible privacy levels (e.g., 'Friends Only' or 'Private'). This controls who can view personal information, photos, videos, and updates, significantly limiting exposure to unwanted attention, cyberstalking, and data harvesting.

7. **Digital Footprint Minimization:** Actively manage your online presence. This involves: (a) Deleting inactive or unused accounts (social media, old shopping sites, forums) that hold personal data. (b) Turning off location services and restricting mobile app permissions that unnecessarily access your camera, microphone, or contacts. (c) Regularly searching for your own name to identify and remove any publicly available personal details (doxing prevention).

8. **Secure and Encrypted Communication:** For sensitive communication, utilize platforms and apps that offer end-to-end encryption. This ensures that messages, photos, or files shared can only be read by the intended recipient, protecting content from interception by malicious third parties or platform providers.

9. **Immediate Documentation and Reporting:** If harassment or cybercrime occurs, do not delete any evidence. Immediately document the incident by taking screenshots of all abusive messages, profiles, and posts, noting the time and date. Report the abuse to the platform (social media site) and then to the relevant law enforcement authority (Cyber Crime Cell or the appropriate section under the Bharatiya Nyaya Sanhita) for formal investigation.

While the study draws extensively from existing statutes and judicial precedents, it also identifies critical emerging dimensions of cybercrime against women that have received limited scholarly attention. In particular, it highlights the urgent need to examine how artificial intelligence, deepfake technology, and algorithmic manipulation have transformed the nature of digital victimization. These technologies have blurred the line between consent and fabrication, enabling sophisticated forms of image-based abuse and reputational harm that current legal frameworks only partially address. Linking this development with India's Digital Personal Data Protection Act, 2023, the study contributes to the ongoing discourse on how privacy, consent, and informational autonomy can be constitutionally safeguarded in the digital age.

Furthermore, the paper opens avenues for empirical exploration by suggesting interviews or surveys involving women victims, cybercrime enforcement officials, and digital rights advocates. Such engagement would provide first-hand insight into enforcement challenges, institutional biases, and lived experiences of online harassment. Combined with analysis of recent high-profile cases post-2022, this approach can bridge the gap between statutory intent and operational reality—thereby enriching the doctrinal understanding of cyber law with socio-legal evidence and practical relevance.

Conclusion

In the digital era with the rise of technology, cybercrimes against women including cyber stalking, bullying, pornography, harassment, cybersex trafficking and morphing are also rising at an alarming rate. These cybercrimes have long lasting impact on women including psychological as well as reputational damage. The vulnerability of women to manipulation makes them soft target of cyber offenders jeopardizing their safety, social and mental well-being. Different countries enacted legislations to curb the growing menace of cybercrime against women. While India has strong legal framework prescribed under Information Technology Act, 2000 to combat these crimes yet there is need for significant improvements for the protection of women and to ensure justice.

Suggestions

1. **Boost Awareness and Digital Rights:** Many women, especially those from underserved regions, don't know the laws that protect them from cybercrime or how to report incidents. We must launch easy-to-understand awareness programs and workshops about digital safety and legal rights. These efforts should clearly explain who to report crimes to and how the legal process works. Government and local organizations need to collaborate to bring these vital workshops to every community.

2. **Integrate Cyber Safety Education:** We need to teach digital ethics and safety proactively. Cybercrime education must be a formal, required part of the academic curriculum across all schools and colleges. This training should go beyond basic computer skills to teach students about being responsible digital citizens, respecting privacy, and understanding the severe real-world consequences of online misconduct.

3. **Strengthen Laws and Enforcement:** Despite existing regulations, cybercrime is still rising because the legal system is often too slow and lacks specialization. We must make laws more effective and introduce very strict punishments for cybercriminals. Law enforcement agencies require better training and tools to investigate digital crimes. Crucially, laws must be updated immediately to address new threats like AI-generated crimes and deepfakes.

4. **Create Women-Only Reporting Centers:** A significant barrier to reporting is the fear of shame and humiliation in typical police settings. The government must establish women-centric cybercrime complaint centers in all communities. These centers should be staffed only by female police officers and counsellors to ensure a safe, supportive, and comfortable environment. They must also allow complaints to be filed easily in local languages**.**

5. **Enact Special Laws for Women's Cybercrime:** Relying on old, general laws is insufficient. The country urgently needs to create a special, separate law that deals only with cybercrimes committed against women. This specific framework must clearly define offenses (like doxing and non-consensual image sharing) and ensure that victims are protected while offenders face severe, specialized punishment.

6. **Mandate Tech Platform Accountability:** Technology and social media companies must be held responsible for the harmful content on their platforms. The law should impose strict and mandatory duties on platforms to quickly remove illegal content (such as revenge images) as soon as it is reported. Platforms must also be required to preserve digital evidence and cooperate immediately with police investigations.

7. **Enhance Justice System Sensitivity:** Cybercrime cases often fail because the police, prosecutors, and judges lack technical knowledge or exhibit gender bias. There must be mandatory, specialized training for all legal personnel on digital forensics, the severe emotional trauma caused by online violence, and how to eliminate victim-blaming. Court procedures must prioritize the victim's dignity and well-being.

8. **Prioritize Global Cooperation:** Since many cyber offenders operate from abroad, local police cannot catch them alone. India needs to establish fast, efficient agreements and treaties with other countries. This is essential to quickly share data, track down, and prosecute cybercriminals who exploit international borders to commit crimes against women.

Reference

1. Nicholas Negroponte, Being Digital Vintage Books, 1995, 230.
2. 'Cybercrime' Cambridge Dictionary, Cambridge University Press, https://dictionary.cambridge.org/dictionary/english/cybercrime. Accessed 19 March, 2025.
3. Cybercrime,' Oxford Dictionaries, Oxford University Press, http://www.oxforddictionaries.com/definition/english/cybercrime. Accessed, 2025.
4. Saroha, Rashmi. 'Profiling a Cyber Criminal.' International Journal of Information and Computation Technology,2014: 4(3):253-58, http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf. Accessed 19 Mar. 2025.
5. National Commission for Women. Annual Report 2023–2024. 2024, https://ncw.nic.in/. Accessed 23 Mar. 2025.
6. 'Cyberbullying Law in India.' LawCrust, LawCrust Legal Consulting, https://lawcrust.com/cyber-bullying-law-india/#:~:text=India%20does%20not%20have%20a,Act%2C%202000%20(IT%20Act). Accessed 20 Mar. 2025.
7. Yadav Harish. 'Unveiling the Dark Side of Cyberspace: A Study of Cyber Crimes Against Women in India.' IJFANS International Journal of Food and Nutritional Sciences, 2022, 10. Accessed,2025.
8. Asthana, Subodh. 'Cyber Pornography.' iPleaders Blog, 2019. https://blog.ipleaders.in/cyber-pornography. Accessed 20 Mar. 2025.
9. 'Cybersex Trafficking.' Wikipedia: The Free Encyclopedia, Wikimedia Foundation, https://en.wikipedia.org/wiki/Cybersex_trafficking. Accessed 20. 2025.
10. Vijayalaxmi B. 'Cyber Crime Against Women in India—A Critical Analysis.' International Journal of Law, 2019, 5, Accessed 23 Mar. 2025.
11. Pathak Akanksha Prateek Tripathi. 'Digital Victimization of Women in Cyberspace: An Analysis of Effectiveness of Indian Cyber Laws.' NLU Assam Law Review, 2024, 7. Accessed 24 Mar. 2025.
12. National Crime Records Bureau. Crime in India 2022. Ministry of Home Affairs, Government of India, 2022, 224. https://images.assettype.com/barandbench/2023-12/dc0ba053-a1f0-4e6a-a5f8-e7668ddd2249/NCRB_STATS.pdf. Accessed 23 Mar. 2025, 5:18 p.m.
13. Gupta Priya. 'Cyber Crime Against Women in Indian Context: An Overview.' Journal of Research in Humanities and Social Science,2020:8. Accessed 25 Mar. 2025.
14. Mishra Shashya. 'Dimensions of Cybercrime Against Women in India – An Overview.' International Journal of Research and Analytical Reviews, 2018, 5. Accessed 26 Mar. 2025.
15. Ahlawat Himani and Som Lata Sharma. 'Cyber Crimes Against Women in India.' Shodh Kosh: Journal of Visual and Performing Arts,2024:1539–1544:6:5. https://www.granthaalayahpublication.org/Arts-Journal/ShodhKosh/article/download/2430/2172/31639. Accessed 26 Mar. 2025.
16. AIR 1965 SC 881
17. C.C. No. 4680 of 2004.
18. 'Cyber Crimes Against Women.' Legal Service India, https://www.legalserviceindia.com/legal/article-8918-cyber-crimes-against-women.html. Accessed 28:2025.
19. 'Cyber-Crimes Against Women.' Vikaspedia, Ministry of Women & Child Development, https://socialwelfare.vikaspedia.in/viewcontent/social-welfare/women-and-child-development/women-development-1/legal-awareness-for-women/cyber-crimes-against-women?lgn=en. Accessed 26 Mar. 2025.
20. Supra note 10
21. (2005) 3 CompLJ 364 (Del).
22. Supra note 10 at 236
23. Nikke, Assistant Professor of Law, Department of Law, Gurugram University, Gurugram. 'Cyber Crime Against Women in India.' International Journal of Creative Research Thoughts (IJCRT), 2024,12:4 ISSN 2320-2882, https://www.ijcrt.org/papers/IJCRT2404234.pdf. Accessed 25 Mar. 2025.
24. Nayak Dr. Meghabahen N. 'Use of Cyber World to Commit Crimes Against Women.' Sarvalokum: Law and Society - Multidisciplinary National Peer-Reviewed Journal,2025,1:(2):265–269. Accessed 26 Mar. 2025.
25. C.C. No. 14616/2014.
26. AIR 2015 SC 1523.
27. Indecent Representation of Women (Prohibition) Act, 1986, Sec. 2(c).
28. Kapoor, Vanshika. 'The Indecent Representation of Women (Prohibition) Act, 1986 in Time of Social Media.' iPleaders Blog, 2024, 31 https://blog.ipleaders.in/the-indecent-representation-of-women-prohibition-act-1986-in-time-of-social-media/. Accessed 28 Mar. 2025.
29. 'Budapest Convention on Cybercrime.' Wikipedia: The Free Encyclopedia, Wikimedia Foundation,

https://en.wikipedia.org/wiki/Budapest_Convention_on_Cybercrime. Accessed 28 Mar. 2025.
30. Pandey, Pooja. 'Comparative Analysis of Cybercrime against Women in India, UK USA.' Junikhyat: Journal of Multidisciplinary Studies, http://junikhyatjournal.in/no_8_jun_20/9.pdf. Accessed 5 Nov. 2025.
31. Myneni SR. Information Technology Law (Cyber Laws). 2nd ed., Asia Law House, Hyderabad, 2021, 549.
32. Burge, Simon. '12 Ways to Prevent Cyber Crime.' International Security Journal,2024, 7. https://internationalsecurityjournal.com/ways-to-prevent-cy-crime/. Accessed 28 Mar. 2025.