Randwick International of Social Sciences (RISS) Journal
Vol. 6, No. 4, October 2025 | Page: 442-451
ISSN Online: 2722-5674 - **ISSN Print**: 2722-5666
https://www.randwickresearch.com/index.php/rissj

Addressing Cybercrime Against Women: A Digital Threat of Growing Concern in India

DOI: *https://doi.org/10.47175/rissj.v6i4.1262*

| Sumanth S. Hiremath |

Department of Sociology,
Rani Channamma University,
Belagavi Karnataka. India

sumanthiremath@gmail.com
ORCID ID: 0000-0003-4818-5801

ABSTRACT
The rapid growth of the internet has led to a significant increase in cybercrimes, with women being disproportionately affected. Cyber Violence against Women and Girls (CVAWG) is an increasing concern around the world. Since the age of 15, one in ten women has been the victim of cybercrime. Women in India deal with unique challenges, such as online harassment, stalking, revenge porn, etc. These things have serious effects on their overall health. To find out what causes cybercrime and make the internet safer for women, it is necessary to look at it from a sociological perspective. This means recognising women's freedom and voices online and working to make the internet a more welcoming and empowering place. To effectively address such issues, the Indian Penal Code (IPC) and the Information Technology (IT) Act need to be made more stringent. In addition, knowing how to use computers and the internet is very important for stopping cybercrimes.

KEYWORDS
Cybercrime; CVAWG; online harassment; IPC; IT Act; digital literacy; cyber safety.

INTRODUCTION

In the age of *Information and Communication Technology* (ICT), the internet has changed the way we live, work, and talk to each other. An estimated 6 billion people are projected to be using the internet globally by 2025, as reported in the ITU Facts and Figures 2025 report (ITU, 2025). Although this expansion has brought about many opportunities, it has also resulted in a sharp increase in cybercrimes, which have harmed people, companies, and governments. 'Cybercrime' is a broad term that includes a lot of different illegal activities that happen online or through digital technology. Some examples are hacking, online harassment, cyberbullying, and financial fraud (Sharma, 2019).

In 2020, the *Federal Bureau of Investigation's* (FBI) *Internet Crime Complaint Centre* (ICCC) reported a shocking 1.3 million cases of cybercrime, which cost the US over $4.2 billion. Cybercrime is on the rise around the world and, it affects people from all walks of life. The present paper focuses on women groups, who are more likely to be victims of cybercrime. Sociologists contend that cybercrime frequently reflects and exacerbates pre-existing social disparities, presenting women with distinct challenges in the online realm. *Cyber Violence against Women and Girls* (CVAWG) is becoming a bigger problem around the world because the internet is getting bigger, mobile information is spreading quickly, and social media is being used by more and more people, and as a consequence, it could have big effects on the economy and society (Kumar, S., 2019). The *World Health Organisation* (WHO) reveals that one in three women will have been the victim of violence at some point in her life. Even though the internet is a relatively new and growing thing, it is estimated that one in ten women have already been the victim of cyber violence since they were 15 years of age.

Women in India face problems that are different from those, that men face, such as online harassment, stalking, identity theft, and revenge pornography. These problems can have serious effects on their mental and physical health (Halder & Jaishankar, 2016). Cyber blackmail, threats, cyber pornography, posting and publishing obscene sexual content, stalking, bullying, defamation, image morphing, and making fake profiles are the most common cybercrimes against women. India uses the *Indian Penal Code* (IPC) from 1860 and the *Information Technology (IT) Act* from 2000, which was changed in 2008, to fight cybercrime.

LITERATURE REVIEW

The IPC includes digital acts of sexual harassment, voyeurism, stalking, intimidation, defamation, and insulting modesty. The IT Act covers things like accessing someone else's computer without permission, stealing someone's identity, making fake documents online, and posting obscene content. Therefore, cybercrime is a mix of crime and technology.

In simple terms, a cybercrime is *"any act or crime that involves the use of a computer. It is when someone commits a crime online and hides behind a computer screen".*

Women are particularly affected by cybercrime, and many cases go unreported because of social stigma and fear of retaliation. This makes it harder to deal with the problem. In these cases, the effects on women can be very bad, such as money problems from theft or fraud, emotional pain and trauma, physical harm from acid attacks or assaults, anxiety, depression, and mental distress. People sometimes even blame the woman for what happened, which makes the situation toxic and makes them less likely to speak up. This paper situates cybercrime against women within a continuum of abuse, examining its legal frameworks, statistical realities, and sociological ramifications.

Cybercrime and Statistics

India is one of the few countries that publishes detailed, annual crime statistics through the *National Crime Records Bureau* (NCRB). Recent reports on crime in India indicate a rise in overall cybercrime cases alongside persistently high levels of crimes against women. Following are the numerical statistics that highlight that both offline and online harms continue to be pressing concerns:

1. The NCRB 2023 report records 86,420 cybercrime cases, reflecting an increase of over 30 per cent from 2022, with the cybercrime rate rising from 4.8 to 6.2 cases per lakh population. In the same year, crimes against women exceeded 4.48 lakh, with a crime rate of 66.2 per lakh female population, slightly higher than in 2022.
2. The NCRB data show that cybercrime incidents went up by 18.4 per cent from 2019 to 2021, and incidents involving women went up by 28 per cent. This statistic means that women are being targeted more quickly than the average user. In 2021, 10,730 incidents, or about 20.2 per cent of the 52,974 registered cybercrime cases, were classified as crimes against women. This data shows how gendered the cybercrime category is (NCRB, 2025).
3. The *National Cybercrime Reporting Portal* (NCRP) says that there were 48,475 reported cases of online crimes against women in 2024. This increase is about 118.4 per cent more than the number of cases reported in 2020. This rapid growth shows that as more women use technology, they are more likely to be victims of abuse that technology makes easier, rather than just benefiting from better connectivity (NCRP, 2025).
4. The NCRP has made it easy to file a complaint. However, some complaints do not result in a formal First Information Report (FIR), and many women do not complain at all. Independent studies indicate that almost 45 per cent of victims do not report

because they are afraid that the police will not believe them, and another 30 per cent stay quiet to avoid being embarrassed in public (NCRP, 2025).

RESEARCH METHODS

Patriarchy 2.0 – Sociological Perspective:

Cybercrime against women is a digital version of old-fashioned rules that keep men in charge. It is not a new problem; it is just that the way power works in society has changed because of the internet. Here are some important ideas that will help you understand this:

1. Online threats and harassment have big effects in real sense world. For instance, WhatsApp threat made a woman stop going to college and social events. This shows that violence online can happen in real life, which means it is a continuum.
2. Men often use technology to control women's bodies and sexuality, which is like how power works in the real world. *For instance*, it is an extension of the *'male gaze'*, which sees women as things that men should control. Some men asking women for passwords or sharing private photos without their permission, which is also known as 'revenge porn'.
3. The *"Bulli Bai"* and *"Sulli Deals"* apps went after well-known Indian women of a certain religion. They were both hateful towards women and religion. This intersectionality makes it even worse to harass people online.
4. When people are anonymous online, they are less likely to hold back, which means they say and do things they would never do in real life. Anonymous trolls say hateful things because they know they will not get in trouble.

All of these things make the internet a bad place for women, where they are attacked, silenced, and controlled. It is not just what one person does; it is also a sign of bigger problems in the world.

RESULTS AND DISCUSSION

Different Kinds of Cybercrime Against Women

The digital world in India has become a new stage for gender-based violence. These The digital world in India has become a new stage for gender-based violence. These offences are not merely technical infractions; they frequently represent deliberate acts of control, retribution, or exploitation, indicative of entrenched patriarchal norms (Evangelin et al., 2023). The following list shows the main types of cyber violence against women in India today:

1. **Digital Surveillance and Cyberstalking:**

   Cyberstalking is when someone uses electronic communication repeatedly to harass, scare, or watch a woman. It is like being followed in real life, and it often leads to violence in real life (Gurumurthy et al., 2019). In Indian pop culture, the idea of always chasing someone is often romanticised. However, from a sociological point of view, this shows a dangerous sense of male entitlement to a woman's time and attention. The internet offers inexpensive and low-risk resources for this monitoring.

   How it works: It includes keeping an eye on a woman's whereabouts through social media "check-ins," keeping track of her "last seen" status on WhatsApp, or using spyware to look at her call logs.

   For instance, a man who has been turned down for his love/marriage proposal makes several fake Instagram accounts to message a woman after she blocks him. He uses her UPI ID (which comes from payment apps) to find out her full legal name. Then, he finds her LinkedIn profile to find out where she works, and finally, he shows up in person.

2. **Non-consensual Intimate Imagery (NCII):**
   The NCII is also known as *'revenge porn'*. The Non-consensual Intimate Imagery (NCII) offence entails the dissemination of sexually explicit images or videos of a woman without her consent, frequently perpetrated by a former partner. This crime uses the idea of *"izzat"* (honour) as a weapon. The perpetrator knows that in Indian culture, a woman's sexual behaviour is closely tied to her family's social status. The goal of releasing these pictures is not only to embarrass the victim, but also to *cause "social death,"* making her *"unmarriageable"* or shameful in the eyes of her community.

   For example, a man posts private pictures of his ex-girlfriend on a pornographic website after they break up, along with her phone number in the caption. After that, the woman gets many calls asking for money, which makes her leave her social and professional life. (Chetan, 2020).

3. **Morphing and Deepfakes (AI-Facilitated Abuse):**
   When you morph or make deepfakes, you use image-editing software or AI to put a woman's face on a pornographic body or video. This kind of violence says that a woman can be hurt even if she is not there in person. People can steal her digital identity to make her look bad. It shows how technology has made women's bodies into things that can be bought and sold without their permission.

   For instance, the Rashmika Mandanna incident in 2023. A deepfake video of actress Rashmika Mandanna went viral and made people all over the country angry. Even though she could have taken legal action, the event showed how weak regular women are. If a celebrity's image can be changed so easily, a college student or stay-at-home mom has little chance of proving her innocence to a conservative family, which could hurt her chances of getting married.

4. **The 'Loan App' and Sextortion Scam:**
   Sextortion is when someone threatens to release private photos or damaging information unless the victim pays money or has sex. This crime takes advantage of people who are desperate for money and afraid of social situations. In recent years, predatory digital lending has hurt women more than men, especially those who do not have access to formal banking.

   For instance, a woman downloads a "instant loan" app that isn't regulated. The app needs her permission to look at her contacts and gallery. Even after she pays back the loan, recovery agents use her own pictures, change them to show naked bodies, and send them to her parents, boss, relatives, friends, and other contacts on WhatsApp to blackmail her into paying very high interest rates.

5. **Fraud in Marriage and Love:**
   Criminals make fake profiles on dating apps or marriage sites to trick women into sending them money. This crime takes advantage of the huge social pressure to get married in India. Fraudsters go after people who are weak, like widows, divorcees, or women in their late 30s and 40s who want to be with someone in a society that judges them.

   For instance, a scammer pretends to be a rich NRI (Non-Resident Indian) doctor or engineer on a dating site. He says he sent a clear gift that is stuck in customs after months of getting emotionally close to the woman. He asks her to send lakhs of rupees to a bank account to *"clear the penalty."*

6. **Style of Doxxing Harassment:**

'Doxxing' is when someone puts a woman's private information (like her home address, workplace, and phone number) online so that other people can harass her. This is often intersectional, going after women because of their political beliefs, caste, or religion. The goal is to silence outspoken women and force them back into the home, which is called *"Digital Purdah"* (Gurumurthy et al., 2019); (Nadine, 2018).

Significant Cases

India over the time has changed its response in courts about cybercrime against women, and it is because of some following few significant cases:

1. **The Ritu Kohli Case-The First Case of Cyberstalking:**
   The Incident: A man used Ritu Kohli's name to chat on a number of different online sites. This is widely seen as India's first case of cyberstalking. He gave out her real home phone number and told other men to call her to talk about sex. Ritu was scared and upset by many dirty calls at all hours.

   Legal Importance: Back then, there was not a specific law against cyberstalking. The police had to come up with a creative way to file the case under Section 509 of the IPC, which deals with outraging the modesty of a woman. This case woke up the legislature and showed them that a criminal could ruin a woman's peace of mind without ever touching her. It played a big role in the later introduction of Section 66A, which was later struck down, and in the recognition of electronic stalking.

2. **Suhas Katti v. State of Tamil Nadu (2004)**:
   The Incident: The accused, who was a family friend of the victim, started sending her dirty messages after she said no to his marriage proposal. He then made a fake Yahoo group in her name and posted false information about her, which led to her getting harassing calls.

   Legal Importance: This case is said to be the first conviction under the Information Technology Act of 2000. The court found the defendant guilty of obscenity under Section 67 of the IT Act and forgery under Section 469 of the IPC. The decision was made quickly, within seven months of the charge sheet. This set a precedent that digital evidence, like IP address tracing, can be used in court and is enough to convict someone. It made it clear that saying bad things about a "reputable woman" online is a very serious crime.

3. **State of West Bengal v. Animesh Boxi (The 'Virtual Rape' Case):**
   The Incident: Animesh Boxi, the person who was accused, wanted to get back at his girlfriend for breaking up with him. He put private, personal videos of her on a porn site on the internet. The victim's family had to deal with a lot of social stigma.

   Legal Importance: The court gave the defendant five years in prison with no chance of parole. Even though there was no physical rape, the prosecution pointed that; the act was a 'virtual rape' of the victim's dignity. Such case reveals that cybercrime can hurt a person's reputation just like a physical harm. The prosecution also acknowledged that in the digital era, a woman's 'modesty' encompasses her digital information, and transgressions thereof necessitate stringent penalties.

4. **Dr. L. Prakash Case (The Link Between Power and Pornography):**
   The Incident: An orthopaedic surgeon Dr. L. Prakash from Chennai, was arrested for luring women, filming sexual acts with them, and selling the videos to foreign websites.

   Legal Importance: This case was one of the first big cases in India, which dealt with the business side of cyber pornography. For breaking the IT Act and the Immoral Traffic

(Prevention) Act, Dr. L. Prakash was found guilty. The case proved that cybercriminals are not just hackers without faces. It showed how men in positions of social power and authority could use technology to exploit women all over the world, turning women's bodies into digital goods for profit (Chetan, 2020).

Digital Silence- Barriers to Justice for Women

Even though there are strong laws and institutions, women victims in the digital space are silences and still have a hard time because of systemic and sociological problems. Following are few instances:

1. **Patriarchal Bargain and Digital Purdah:**
   Family become as a main obstacle, as in most of the Indian homes, a woman can only use technology if certain conditions are met. If she tells her family that she is being harassed, they often take her phone or limit her internet access instead of helping her. The consequence of this is, women go into a *'Digital Purdah',* which means they stay away from the internet to avoid fights. This result in significant underreporting referred to as the 'dark figure' of crime.

2. **Institutional Victim-Blaming:**
   The attitudes of the police officers matters. As the police officers often do not know in some cases, how to be sensitive to gender issues. People who report sharing images without their permission are often asked personal questions like, *"Why did you take that picture in the first place?"* This changes the blame from the criminal to the victim's morals.

3. **Technical and Jurisdictional Delays:**
   Concerning the cross-border data, cybercrime knows no borders. The person who did the crime could be in any place of the world, the victim could be in any other corner of the world, and the data could be stored on servers in the US (Facebook/Instagram). It takes a long time to get data from foreign intermediaries using *Mutual Legal Assistance Treaties* (MLATs). By the time the evidence is in, the damage to the woman's reputation from the virus is usually permanent.

4. **Dark Figure of Crime:**
   In the dark figure of crime, about 45-50% of victims do not report cybercrimes because they are afraid of being embarrassed in public *(Log Kya Kahenge—what will people say?).* This changes the official numbers (crime rate statistics) and lets the criminals keep breaking the law without being caught.

Legal Framework and Institutional Response

The *Government of India* (GoI) has set up number of institutional ways to fight cybercrime against women because they see the threat rising. Further, the India's legal approach to cybercrime against women has undergone a significant transformation with the transition from the colonial-era *Indian Penal Code* (IPC), 1860, to the *Bharatiya Nyaya Sanhita* (BNS), 2023. This shift represents an attempt to modernise criminal law to address the complexities of the digital age (Kleinsasser et al., 2015). Follows are the legal frameworks and institutional responses:

1. **The Transition: A Comparative Analysis**
   The BNS retains the core essence of the IPC but refines definitions and introduces specific provisions to tackle modern digital offences.

Offence Category	Old Provision	New Provision	Key Changes & Sociological Implication

	(IPC)	(BNS 2023)	
Sexual Harassment	**Section 354A**	**Section 75**	**Expanded Scope**: • While IPC 354A criminalised physical advances, BNS Section 75 is interpreted to cover unwelcome digital advances, such as sending lewd WhatsApp messages or unsolicited explicit images *('cyber-flashing').* • It recognises that harassment can occur without physical proximity.
Voyeurism	**Section 354C**	**Section 77**	**Technological Neutrality**: • This section punishes capturing images of a woman engaging in a private act. • The BNS reinforces that this applies regardless of the device used *(hidden cameras, hacked webcams, or drones),* addressing the *'panopticon'* effect of modern surveillance technologies.
Stalking	**Section 354D**	**Section 78**	**Explicit Digital Inclusion**: • This is the most critical update. BNS Section 78 explicitly states that monitoring a woman's use of the internet, email, or any other form of electronic communication constitutes stalking. • This legalises the sociological concept of *'cyberstalking'* as a crime equivalent to physical stalking.
Insult to Modesty	**Section 509**	**Section 79**	**Digital Dignity**: • This section penalises words, gestures, or acts intended to insult a woman's modesty. • In the digital context, this covers intrusive online comments, trolling, and privacy violations that may not fit neatly into other categories but still degrade a woman's dignity.
Deceitful Promise	**(Ambiguous)**	**Section 69**	**Love Jihad & Romance Fraud**: • A controversial but significant new addition. • It criminalises sexual intercourse obtained by *'deceitful means',* including a false promise of marriage or suppressing one's identity. • While politically debated, sociologically, this addresses *'catfishing'* and romance scams where men use fake profiles to exploit women sexually.

Source: *Taxmann Research & Editorial Team, "[Comparative Study] Bharatiya Nyaya Sanhita 2023 (BNS) & Indian Penal Code 1860 (IPC)", 8 January 2024.* ***www.newsminute.com***

2. The Information Technology (IT) Act, 2000

The IT Act remains the primary special law for electronic offences, working in tandem with the BNS:

- *Section 66E:* Punishes privacy violations (capturing/publishing private body parts).
- *Section 67 & 67A:* Penalise the transmission of *'obscene'* and *'sexually explicit'* material respectively.
- *Section 66C & 66D:* Criminalise identity theft and cheating by personation (crucial for fake profile cases).

3. **Cybercrime Prevention against Women and Children (CCPWC):**
   The *Ministry of Home Affairs* (MHA) started the Cybercrime Prevention against *Women and Children* (CCPWC) Scheme with money from the *Nirbhaya Fund*. Its goal is to set up cyber forensic labs, teach police officers, and hire junior cyber consultants. It also aims to close the *'technical gap'* in investigations by giving state police the tools and knowledge they need (MHA, 2023).
   Under the CCPWC scheme, judges and public prosecutors need to be trained for cultivating the knowledge, skills and attitude required to ensure gender equality in the digital context. This will go a long way in survivors' access to justice. Pune city has an informal study circle for lawyers, judges and other stakeholders on cybercrimes. Such efforts for continued exchange of ideas can be useful to promote feminist approaches to the law.

4. **National Cyber Crime Reporting Portal (NCRP):**
   It is a central place for people to report cybercrimes online. The special feature of this is that, it has a separate section for *'Crimes against Women and Children'* that lets people report crimes without giving their names, which helps get rid of the stigma that comes with it. (NCPCR, 2017).

5. **National Helpline Numbers:**
   The number *'1930'* is a special helpline for reporting cyber crime and the national women helpline number is 181. Victims of 'sextortion' and loan app frauds need to freeze their money before it is stolen even though this is mostly for financial loss.

6. **Indian Cybercrime Coordination Centre (I4C):**
   The *I4C* was established by MHA, in New Delhi to provide a framework and eco-system for *Law Enforcement Agencies* (LEAs) for dealing with cybercrime in a coordinated and comprehensive manner. It finds and blocks harmful apps and websites (like loan apps) that unfairly target weak groups. (MHA, 2023); (I4C).

Forward Path-Cyber Awareness and Solutions

To strengthen public awareness on cybercrimes, the government has taken the following multi-platform outreach strategy (PIB, 2025):

1. The Government has launched citizen-centric outreach campaigns through radio, newspapers, and metro announcements to caution people about cyber frauds.
2. The *National Cyber Coordination Centre* (NCCC) has been set up by CERT-In to generate necessary situational awareness of existing and potential cyber security threats.
3. The government engages the public by conducting '*Cyber Safety and Security Awareness Weeks'* through the MyGov platform.
4. A '*Handbook for Adolescents and Students'* is published to guide young people in cyber safety and security.
5. Social media is used to spread cyber awareness and safe practices to prevent cybercrime.

In order to prevent cyber violence, it is necessary to make significant changes to society as a whole, not just fix the laws. To stop cybercrime against women, it is necessary to look at the things that cause it, like how men think, how society works, and how power works (Noble, 2018). Following are some important solutions:

1. **Legal & Investigative Reforms:**
   The law and investigations need to change a lot. The first step is to set up *Fast-Track Cyber Courts* (FTCC) that handle cybercrime cases speedily. So that the victims won't

have to spend more time in court. In addition, it is very important to strictly enforce BNS 78 so that police do not ignore complaints and instead file them right away under the stalking law.

2. **Technological Interventions:**
   One way that technology can help stop online abuse is through algorithmic accountability. It uses *artificial intelligence* (AI) to find and flag abusive content on social media sites, like private photos that were shared without permission. In addition, *'Panic Button Apps'* can also let the police and people you trust like family members, friends know if someone is bothering you online.

3. **Educational and Social Reforms:**
   Educational and social reforms are very important to eradicate any sort of crimes. *'Cyber Hygiene'* should be taught in schools, colleges, and universities. Lessons on privacy, digital consent, and the effects of cyberbullying should be part of curriculum.
   'Bystander Intervention Training' teaches people how to report abuse online. It was the first empirical evaluation of an online bystander intervention program designed to prevent sexual violence (Kleinsasser et al., 2015).

4. **Addressing Root Causes:**
   It is crucial to focus on the root causes, starting with raising awareness among people of online harassment and its effects on them. If women are taught, how to use computers and the internet safely, they will feel more confident of themselves while online surfing. Strengthening laws can make sure that people who break the law are punished, and bystander intervention can make it normal for people to speak up. Lastly, challenging and restricting patriarchal norms, can curtail the cybercrime against women that is going on and can make online spaces more friendly and respectful. (Kumar, N., 2019).

CONCLUSION

The cybercrime against women in India has become an urgent concern that needs to be looked at and dealt with right away. This needs to be fixed. The laws need to be strengthened, people need to learn how to use technology properly, and victims need to be able to seek help. To make the internet a safer and friendlier place for everyone, it is necessary to understand the social background and address the issues that lead to him or her.

The sociological perspective that examines structure, culture, and agency, it is insufficient to merely enact laws that enhance the safety of digital futures. In India, the opening up of data to everyone has happened faster than digital literacy and safety measures. This process has led to cultural lag, which means technology is more dynamic than the norms that must be established to control it. Women's presence, speech, pleasure, and dissent in online spaces should not be seen as risks that need to be managed but as legitimate ways of expressing autonomy that the state, platforms, and society as a whole must protect. Instead, there is a pressing need for a new approach to citizenship and rights that emphasises inclusivity and empowerment while recognising women's voices in the digital realm. Such an approach can enhance the digital space for all, particularly in terms of advancing women's rights and fostering the overall well-being of the community.

REFERENCES

Chetan, M.G. (2020). *Woman's phone hacked, contacts get obscene pictures*. The New Indian Express Newspaper.

https://www.newindianexpress.com/cities/bengaluru/2020/aug/04/womans-phone-hacked-contacts-get-obscene-pictures-2178712.html

Debarati Halder and K. Jaishankar (2016). *Cyber crimes against women in India*. SAGE, pp. 272.

Evangelin, W., Anitha B., and D. Tony Arpudharaj. (2023). Examining Cybercrime against Women in India: Understanding its Impact and Exploring Remedial Safety Measures. *Mukt Shabd Journal, 12*(8), 625–638.

Gurumurthy, Anita, Vasudevan, Amrita, and Chami, Nandini. (2019). *Born digital, Born free? A socio-legal study on young women's experiences of online violence in South India*. IT for Change. https://itforchange.net/sites/default/files/1662/Born-Digital_Born-Free_SynthesisReport.pdf

Indian Cybercrime Coordination Centre (I4C). https://i4c.mha.gov.in

International Telecommunication Union (ITU) (2025). Facts and Figures 2025. https://www.itu.int/itu-d/reports/statistics/2025/10/15/ff25-internet-use/

Kleinsasser, A., Jouriles, E. N., McDonald, R., & Rosenfield, D. (2015). An Online Bystander Intervention Program for the Prevention of Sexual Violence. *Psychology of violence, 5*(3), 227–235. https://doi.org/10.1037/a0037393

Kumar, N. (2019). *All you need to know about Cyber law in India*. Enter Slice. https://enterslice.com/learning/cyber-law-in-india/

Kumar, S. (2019). *Cybercrime against women: Right to privacy and other issues*. Research Gate. https://www.researchgate.net/publication/344153821

Ministry of Home Affairs (MHA), (2023). *Handbook on the Bharatiya Nyaya Sanhita, 2023*. Bureau of Police Research Development. GoI, New Delhi. https://bprd.nic.in/uploads/pdf/BNS%20Book_After%20Correction.pdf

Nadine, Graham. (2018). Cyber crimes against women in India. *Asian Journal of Women's Studies, 24*(3), 413-417, https://doi.org/10.1080/12259276.2018.1496783

National Commission for Protection of Child Rights (NCPCR), (2017). *Being Safe Online-Guideline for raising awareness among children, parents, educators and general public*. GoI, New Delhi. www.ncpcr.gov.in

National Crime Records Bureau (NCRB). (2025). *Crime in India 2023: Statistics*. Ministry of Home Affairs, Government of India.

National Cyber Crime Reporting Portal (NCRP). https://cybercrime.gov.in/Webform/Accept.aspx

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York University Press.

Press Information Bureau (PIB) (2025), Government of India. https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3&reg=3&lang=1

Sharma, D. (2019). *Cyber Crime In India: Are Women A Soft Target?* LegalServiceIndia.com. https://www.legalserviceindia.com/legal/article-639-cyber-crime-in-india-are-women-a-soft-target.html

Taxmann Research & Editorial Team. (2024). *Comparative Study*. Bharatiya Nyaya Sanhit (BNS) 2023, & Indian Penal Code 1860 (IPC). 8 January 2024. www.newsminute.com