The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 4 | Issue 2 | February 2026
ISSN: 2583-973X (Online), SJIF IF: 5.6
Website: www.theacademic.in

From Online Abuse to Offline Impact: The Expanding Crisis of Cyber Crimes Against Women

Pratiksha Mandal

Under-graduate Student, 3rd Year, St. Xavier's College (Autonomous), Kolkata, West Bengal, India

Email : itstrisha2403@gmail.com

DOI : https://doi.org/10.5281/zenodo.18873287

ARTICLE DETAILS

Research Paper

Accepted: 18-02-2026

Published: 10-03-2026

Keywords:

Cyber crime, Women, Digital Victimization, Security, Cyber threats.

ABSTRACT

For centuries, women across India and the West have faced systemic marginalization—denied voting rights, restricted from owning property, subjected to exploitative labor, and oppressed by practices like sati and dowry-related violence. Their subordination has been reinforced by rigid hierarchies of class, caste, and patriarchy. Reformers such as Betty Friedan, Raja Ram Mohan Roy, Ishwar Chandra Vidyasagar, and Elizabeth Cady Stanton challenged these injustices, fighting for women's dignity, autonomy, and legal recognition. In the twenty-first century, this oppression has shifted into digital spaces, where cybercrimes—from stalking to deepfake pornography—have become one of the fastest-growing forms of violence against women. This study argues that cybercrime is not merely a technological threat, but a grave human rights crisis requiring urgent legal, institutional, and societal action.

Introduction

The terrain of women's oppression has transformed significantly in the digital age. While earlier discrimination was rooted in visible socio-political structures, contemporary gendered violence increasingly operates within everyday digital spaces. Social media platforms such as Instagram, Facebook, and Twitter (now X) have created unprecedented opportunities for expression and empowerment, yet they have also opened new avenues for abuse.

Cybercrime against women—including cyberstalking, non-consensual image sharing, deepfake pornography, trolling, doxxing, and online harassment—has become one of the fastest-growing forms of victimization. Unlike traditional violence, digital abuse is borderless, anonymous, algorithmically amplified, and permanently archived. It invades private spaces, weaponizes personal data, and causes lasting psychological, social, and professional harm, often silencing women in virtual public spheres.

This threat cuts across caste, class, and regional lines, particularly affecting women who rely on technology for education, work, and activism. Addressing it requires strong legal frameworks, institutional cyber cells, digital literacy, and coordinated action, as it represents a serious structural and human rights challenge.

Methodology

This research aims to explore the nature, extent and causes of cyber crimes against women and children by an exploratory way. Online content analysis through the lense of news articles,social media posts are also important. Primarily, journals and books are the sources for the development of the following topic.The study will raise awareness about the increasing Cyber crimes against women. It will also throws the light upon the policy making and law enforcement agencies.

The Expanding Digital Underworld: Escalating Cyber Threats Against Women and Children

Cybercrimes targeting women and children extend far beyond breaches of privacy; they erode digital identities, destabilize emotional well-being, and, in extreme cases, push victims toward self-harm or suicide. The impact is deeply psychological, infiltrating the most intimate dimensions of personal life. The digital underworld has become increasingly accessible. Malware kits, botnets, hacking services, and surveillance tools are now traded openly in dubious online marketplaces, lowering the threshold for criminal entry. As a result, individuals with little or no technological expertise are drawn into the cybercrime ecosystem, forming organized syndicates that operate across regions. This democratization of digital criminality has intensified both the scale and sophistication of online exploitation, making cyber violence a rapidly expanding and deeply concerning social crisis.

1. Cyberbullying:

Cyberbullying involves the use of social media, gaming platforms, dating apps, and messaging services to threaten, shame, or humiliate a target. It may include spreading false rumours, sharing manipulated

images, body-shaming, caste- or religion-based slurs, and coordinated online ridicule. While gender-neutral in theory, women and teenage girls are disproportionately targeted, often facing character assassination and reputational harm.

2. Cyberstalking:

Cyberstalking is the digital extension of physical stalking. It includes persistent monitoring, repeated unwanted communication, threats, identity theft, and tracking online activities. Offenders exploit anonymity, easy access to personal data, and technological tools to intimidate victims. It may occur through emails, social media surveillance, spyware, or even hacking into personal devices—creating fear without physical contact.

3. Cyber Harassment:

This encompasses threatening emails, sexually explicit messages, impersonation, and coercive demands for sexual favours. It often overlaps with online sexual harassment, including unwelcome advances, explicit remarks, and extortion.

4. Digital Impersonation:

Creating fake social media profiles, email IDs, or websites in a person's name with intent to defame or blackmail constitutes digital impersonation. Perpetrators fabricate "avatars" to circulate false statements, solicit money, or damage reputations—turning identity into a weapon.

5. Trolling:

Trolling refers to deliberately provocative or inflammatory online behaviour intended to disrupt conversations and incite hostility. Trolls exploit freedom of speech to post offensive comments, distorted memes, edited visuals, and communal or political propaganda. In extreme cases, online trolling escalates into coordinated digital mob harassment or even offline violence.

6. Morphing and Deepfakes:

Morphing involves digitally altering images without consent, often inserting a woman's face onto explicit content. With the rise of deepfake technology and editing apps, such manipulation has become alarmingly easy. These images are used for blackmail, revenge, or extortion, leaving victims stigmatized and emotionally traumatized.

7. Cyber Defamation:

Publishing defamatory content, hacking accounts, or creating fake profiles to circulate false allegations is another prevalent offence. Women are frequently targeted to undermine their credibility and social standing.

8. Voyeurism and Privacy Invasion:

This crime involves capturing or disseminating images or videos of women engaged in private acts without consent. Non-consensual sharing of intimate images—often termed "revenge porn"—constitutes a severe violation of privacy and autonomy.

The Growing Challenge

Technology advances faster than legislation, creating regulatory gaps that cyber offenders exploit As innovation accelerates, so does the sophistication of cyber violence. Addressing this surge demands stronger legal frameworks, technological vigilance, and widespread digital awareness to protect women from becoming targets in the vast and vulnerable online sphere.

Case Study: AI-Driven Image Manipulation and Coercion in a University Setting

In 2024, a 19-year-old undergraduate student at a metropolitan university became the target of AI-enabled cyber exploitation after publicly speaking against sexist remarks made during a campus event. Within days, anonymous social media accounts began circulating fabricated images portraying her in sexually explicit contexts. These visuals were created using freely available face-swapping and generative AI applications that required no advanced technical expertise. The manipulated images were accompanied by defamatory captions questioning her character and morality.

Shortly thereafter, the student received private messages threatening wider circulation of the content unless she issued a public apology and withdrew from her leadership position in a student organization. The perpetrator also demanded personal photographs, escalating the coercion into attempted sextortion. Although the images were entirely fabricated, their hyper-realistic quality created confusion and reputational harm among peers.

The psychological impact was severe. The student reported anxiety, insomnia, social withdrawal, and declining academic performance. Fear of stigma—particularly in a cultural environment where women's

reputations are disproportionately scrutinized—intensified her distress. The incident eventually led to a formal complaint with the university's cyber cell and local authorities.

This case illustrates how artificial intelligence has transformed digital harassment into a sophisticated instrument of control. The accessibility of AI-powered editing tools enables individuals to weaponize technology against women who assert autonomy or challenge patriarchal norms. The harm extends beyond virtual spaces, disrupting education, leadership opportunities, and mental well-being. Such incidents underscore the urgent need for AI regulation, institutional safeguards, and gender-sensitive cybercrime redressal mechanisms to prevent the normalization of technology-facilitated intimidation.

Legal Remedies in the Context of Increasing Cyber Crimes Against Women

The rapid expansion of digital platforms has significantly increased women's participation in social, professional, and educational spaces online. However, this digital inclusion has also resulted in a sharp rise in cyber crimes specifically targeting women. Online abuse today ranges from sexual harassment, stalking, and identity theft to revenge pornography and privacy violations. These offences are not merely technical violations—they deeply affect a woman's dignity, mental health, reputation, and social standing, especially in conservative and rural settings.

Recognizing this growing threat, Indian law provides a structured framework under the **Indian Penal Code, 1860 (IPC)** and the **Information Technology Act, 2000 (IT Act)** to protect women in cyberspace. These provisions aim not only to punish offenders but also to safeguard privacy, autonomy, and constitutional rights in the digital environment.

1. Sexual Harassment – Section 354A IPC

With the increasing use of social media, messaging applications, and professional networking platforms, sexual harassment has taken new digital forms. Section 354A IPC criminalizes sexual harassment, including:

- Unwelcome sexual advances
- Demands for sexual favours
- Showing pornography against a woman's will
- Making sexually coloured remarks

In cyberspace, these acts commonly appear as unsolicited explicit messages, obscene images, coercive online propositions, or degrading comments on social media. The law prescribes imprisonment up to three years and fine for serious forms of harassment, and up to one year for sexually coloured remarks.

This provision is crucial in addressing the normalization of online misogyny and verbal abuse directed at women.

2. Cyberstalking – Section 354D IPC

Cyberstalking has become one of the most common forms of online violence against women. Section 354D IPC criminalizes:

- Repeated unwanted communication
- Persistent attempts to establish contact despite refusal
- Monitoring a woman's internet use or electronic communication

Offenders may face imprisonment up to three years on first conviction along with a fine. This provision directly addresses behaviours such as tracking social media activity, sending repeated threatening messages, creating multiple fake accounts to contact a woman, or using digital tools to monitor her location.

Given the psychological trauma and fear caused by cyberstalking, this section plays a critical preventive role.

3. Violation of Privacy – Section 66E IT Act

In the digital age, privacy violations have become alarmingly common. Section 66E of the IT Act criminalizes the intentional capture, publication, or transmission of images of a person's private body parts without consent.

This section is particularly relevant in cases involving:

- Hidden camera recordings
- Morphed or edited intimate photographs

- Non-consensual sharing of private images

The punishment may extend to three years of imprisonment or fine up to two lakh rupees. For women, especially those in rural or socially conservative communities, such violations can result in severe social stigma and emotional distress.

4. Identity Theft – Section 66C IT Act

Identity theft is frequently used as a tool to target women online. Section 66C penalizes fraudulent use of another person's electronic signature, password, or unique identification feature. This provision is often invoked in cases involving:

- Hacking of social media accounts
- Unauthorized access to personal data
- Misuse of digital credentials

Punishment includes imprisonment up to three years and fine up to one lakh rupees. Protection of digital identity is vital as women increasingly depend on online platforms for work, education, and communication.

5. Cheating by Personation – Section 66D IT Act

Online impersonation has become a widespread method of exploitation. Section 66D punishes cheating by personation using a computer resource.

It applies in situations where offenders:

- Create fake social media profiles
- Pretend to be someone else to build fraudulent relationships
- Manipulate women emotionally or financially

The offence carries imprisonment up to three years and fine up to one lakh rupees. This provision is especially relevant in cases of online relationship fraud and emotional blackmail.

6. Voyeurism – Section 354C IPC

Section 354C IPC addresses voyeurism, which includes watching, recording, or sharing images of a woman engaged in a private act where she expects privacy.

Even if the image was initially shared consensually, its distribution without consent constitutes an offence. Punishment ranges from one to three years for first conviction and may extend up to seven years for subsequent convictions.

This section directly responds to the rising incidents of leaked intimate videos and revenge pornography targeting women.

7. Publishing Obscene Material – Section 67 IT Act

Section 67 criminalizes the publication or transmission of obscene material in electronic form. It applies when content is lascivious, appeals to prurient interests, or tends to corrupt viewers.

In the context of crimes against women, it is frequently invoked when:

- Obscene images are circulated online
- Fake profiles publish defamatory sexual content
- Women are targeted through pornographic misuse of their photographs

Punishment may extend up to three years of imprisonment and fine up to five lakh rupees for first conviction.

8. Publishing Sexually Explicit Content – Section 67A IT Act

Section 67A deals specifically with sexually explicit acts or conduct in electronic form. It prescribes stricter penalties—imprisonment up to five years and fine up to ten lakh rupees on first conviction.

This section is often applied in:

- Cyber pornography rackets
- Revenge porn cases

- Non-consensual circulation of explicit videos

Given the growing trend of digital sexual exploitation, this provision acts as a strong deterrent.

9. Breach of Confidentiality – Section 72 IT Act

Section 72 penalizes unauthorized disclosure of electronic records or personal information obtained through lawful access.

This is particularly relevant when:

- Private data is leaked by service providers
- Confidential information is misused for harassment
- Personal records are shared without consent

The punishment may extend to three years' imprisonment and fine up to five lakh rupees.

The increasing incidence of cyber crimes against women reflects deeper structural inequalities, digital illiteracy, and misuse of technological advancements. Women often face targeted abuse intended to silence, shame, or control them in virtual spaces.

The Indian Penal Code and the Information Technology Act together provide a comprehensive legal shield addressing harassment, stalking, identity theft, obscenity, privacy violations, and digital exploitation. However, effective protection depends not only on statutory provisions but also on awareness, timely reporting, efficient cyber policing, and societal sensitivity toward victims.

As women continue to assert their presence in digital spaces, the law must remain a dynamic instrument—ensuring that cyberspace is not a domain of fear, but a space of empowerment and equal participation.

Landmark Cyber Crime Case Laws in India

Judicial precedents in India have played a transformative role in shaping the evolution of cyber jurisprudence. As technology advanced faster than legislation, courts were compelled to interpret traditional criminal law principles in the context of cyberspace. The following landmark cases

collectively demonstrate how Indian courts have responded specifically to issues of cyber harassment, obscenity, identity misuse, and digital exploitation of women.

The Ritu Kohli Case (2000)

The Ritu Kohli case is widely recognized as one of the earliest reported instances of cybercrime against a woman in India. The matter arose in Delhi when an individual, Manish Kathuria, allegedly impersonated Ms. Ritu Kohli in online chat rooms. He used her name to post obscene messages and even circulated her residential telephone number, falsely inviting others to contact her for inappropriate conversations. As a result, she began receiving a barrage of unsolicited and vulgar phone calls.

At the time, India's cyber law framework was still nascent. Although the Information Technology Act, 2000 had recently been enacted, specific provisions addressing online impersonation were limited. The accused was booked under Section 509 of the Indian Penal Code (insulting the modesty of a woman) and Section 67 of the IT Act for publishing obscene material in electronic form.

This case is significant not only because it highlighted the vulnerability of women in digital spaces, but also because it exposed gaps in the legal regime, prompting stronger legislative and enforcement mechanisms in subsequent years. It marked the judiciary's initial confrontation with the complexities of online identity misuse and cyber harassment targeting women.

State of Tamil Nadu v. Suhas Katti

This case stands as a milestone in Indian cyber law enforcement as it resulted in the first conviction under Section 67 of the Information Technology Act, 2000 in a case involving online harassment of a woman. The accused, Suhas Katti, posted obscene and defamatory messages about a divorced woman in a Yahoo message group. He also created a fake email account in her name and circulated offensive content, leading to harassment and mental distress.

The complaint was filed in 2004, and notably, the case was investigated and adjudicated swiftly. The court convicted the accused under Sections 469 (forgery for harming reputation) and 509 IPC, along with Section 67 of the IT Act. The prompt conviction within a relatively short span demonstrated the judiciary's readiness to treat cyber offences against women with seriousness equal to conventional crimes.

The case established that defamatory and obscene content posted online carries the same legal consequences as similar acts committed offline. It also set a precedent for cyber forensic investigation and digital evidence admissibility in Indian courts in cases involving women's dignity and reputation.

Dr. Prakash v. State of Tamil Nadu

This case involved a medical practitioner accused of producing and distributing pornographic content involving young women through digital means. The matter came to light when victims reported exploitation involving obscene photographs and videos that were allegedly circulated internationally.

The prosecution invoked Section 67 of the IT Act, which criminalizes the publication or transmission of obscene material in electronic form. The case demonstrated that professional status or social standing does not shield an accused from liability in cyber offences, particularly where women are sexually exploited.

It reinforced the principle that the internet cannot be used as a platform for commercial sexual exploitation of women. Importantly, the case also underscored the role of digital forensics and cross-border cooperation in tracing online pornography networks involving female victims.

Puri Cyber Pornography Case

In one of Odisha's earliest cybercrime convictions involving harassment of a woman, the accused created a fake email account and fabricated online profiles linking the complainant's wife to explicit content. He uploaded obscene material and associated the victim's contact details with pornographic platforms, causing severe reputational damage and harassment.

The accused was prosecuted under Sections 66C (identity theft), 67, and 67A (sexually explicit material) of the IT Act. The court imposed a stringent sentence, reportedly extending up to six years of imprisonment.

This case is notable because it expanded the enforcement of Section 67A, which deals specifically with sexually explicit material rather than mere obscenity. It also highlighted the psychological, social, and reputational trauma suffered by women victims of digital defamation and revenge pornography.

Psychological Vulnerabilities, Rural Illiteracy, and Digital Exploitation

Identity Crisis, Loneliness, and Psychological Vulnerability

The rapid transformation brought about by globalization and modernization has deeply altered social and family structures, particularly in countries like India where the joint family system once provided emotional security and collective supervision. Migration from rural areas to urban centres in search of employment has led to the widespread adoption of nuclear family systems. While nuclear families offer privacy and independence, they have simultaneously weakened traditional networks of emotional support, shared responsibility, and social monitoring.

In rural contexts, this shift has been even more disruptive. Women who migrate or whose family members migrate often experience isolation, reduced guidance, and limited emotional support. Work pressures and fragmented relationships have created a climate of loneliness where individuals increasingly turn to social networking platforms and online communities for companionship and validation.

For women—especially those from rural and semi-urban backgrounds—this digital exposure often occurs without adequate awareness of cyber risks. Limited digital literacy and low levels of formal education make them particularly susceptible to online deception, emotional manipulation, and cyber harassment. According to workforce participation trends in India, women's engagement in formal employment remains significantly lower than men's, particularly in rural areas. This economic dependency further compounds vulnerability, as many women lack financial autonomy to seek legal remedies or technological safeguards.

The psychological need for recognition, communication, and social belonging often pushes women toward online platforms without fully understanding privacy settings, identity protection mechanisms, or cybercrime reporting channels. This identity crisis—where traditional support systems weaken while digital exposure increases—creates fertile ground for cyber exploitation.

Facebook Fake Profile Exploitation: A Tool of Harassment and Defamation

Social networking platforms such as Facebook have become common spaces for interaction, expression, and networking. However, the public visibility of profiles can be weaponized against unsuspecting women, particularly those from rural or less digitally aware backgrounds.

A common pattern of abuse involves the creation of fake profiles in the name of a woman. These profiles may display her real name, photograph, address, or phone number. In more malicious cases, perpetrators

morph original photographs into obscene or nude images. The fake profile often portrays the victim as a prostitute or a woman of "loose character" seeking sexual relations.

In rural societies, where social reputation holds immense importance, such defamation can cause severe emotional trauma, social ostracism, and even threats to physical safety. Villagers and acquaintances who see the fake profile may believe it to be authentic, leading to unsolicited calls, messages, and public humiliation. The damage extends beyond digital space—it infiltrates family honour, marriage prospects, and community standing.

Legal Provisions Applicable:

Such acts attract liability under Section 66E (violation of privacy) and Section 67 (publishing obscene material) of the Information Technology Act, 2000, along with Section 509 of the Indian Penal Code for insulting the modesty of a woman.

Who is Liable:

The individual who creates, uploads, or manages the fake profile is legally responsible. Where intermediaries knowingly permit defamatory or obscene content, liability may also extend under specific circumstances.

Common Motives:

Jealousy, revenge, rejection of romantic proposals, personal disputes, or social rivalry often motivate such crimes.

Typical Modus Operandi:

The perpetrator usually creates a fictitious email account—often through free services—using false identity details. This email is then used to register on social media platforms and create an offensive profile. Because rural women often lack knowledge of reporting mechanisms or digital evidence preservation, the offender may continue harassment unchecked.

The lack of rural cyber awareness programs and limited access to cyber cells further aggravate the issue, leaving victims psychologically distressed and socially stigmatized.

Cyber Pornography and Revenge Exploitation

Cyber pornography has evolved into a vast and profitable global enterprise. Unfortunately, women—especially those unaware of digital safeguards—frequently become unwilling victims. In rural and semi-urban settings, hidden recording devices in changing rooms, hotels, or rented accommodations have been used to capture private moments without consent. With the advent of smart devices connected to the internet, remote recording has become technically easier.

A particularly disturbing trend involves revenge pornography. Former partners or anti-social elements upload intimate videos or photographs to defame women, extort money, or settle personal scores. In conservative rural societies, the impact of such exposure can be devastating—leading to psychological breakdown, forced withdrawal from education or employment, and even self-harm in extreme cases.

Cyber pornography includes the creation, circulation, and sale of explicit videos or images through websites, messaging applications, and social media platforms. Some offenders monetize such content by accepting online payments and granting access to paying viewers. In other cases, the sole objective is character assassination.

Legal Provisions Applicable:

Sections 67 and 67A of the Information Technology Act, 2000 criminalize the publication or transmission of obscene and sexually explicit material in electronic form.

Typical Modus Operandi:

The suspect registers on pornographic platforms using fictitious credentials and uploads the content. In commercial cases, the offender collects payments for downloads or viewing access. In revenge cases, videos are broadcast through messaging apps or circulated widely to maximize humiliation.

The Rural Dimension: Illiteracy and Lack of Cyber Awareness

One of the most pressing concerns in addressing cyber crimes against women is rural illiteracy and digital ignorance. Many rural women are first-generation internet users. They may not understand privacy controls, password security, data sharing risks, or cyber complaint procedures. Cultural taboos often prevent them from reporting crimes involving sexual content due to fear of social stigma.

Furthermore, limited access to cybercrime police stations, poor digital infrastructure, and lack of awareness campaigns widen the justice gap between urban and rural victims. Even when laws exist, enforcement becomes ineffective without awareness and accessibility.

To combat cyber crimes effectively, rural outreach programs must focus on:

- Digital literacy training for women and girls.
- Awareness of privacy settings and safe social media practices.
- Information about legal remedies and cybercrime helplines.
- Community-level sensitization to reduce victim blaming.
- Strengthening rural cyber cells and fast-track complaint systems.

International Cyber Law Trends and Protections

Across the world, cyber laws are no longer limited to basic computer offences. Modern legal frameworks now address a wide range of digital harms. These include:

- **Data protection and privacy laws** safeguarding personal information
- **Recognition of digital evidence** in courts
- **Cybersecurity response mechanisms**
- **Liability of intermediaries and internet service providers**
- **Cross-border cooperation and extradition of offenders**
- **Regulation of hate speech and online abuse**

These global developments show that cyber law is evolving to protect individuals more effectively, especially women who are often targets of online abuse. Many countries have introduced specific measures against cyberbullying and non-consensual image sharing. Such models provide valuable lessons for strengthening protections for women in India and position the issue within a broader global conversation on digital safety.

National Cyber Crime Reporting Portal (cybercrime.gov.in)

India has introduced the **National Cybercrime Reporting Portal (NCRP)** to make reporting online offences easier and more accessible, particularly for women and children.

- **Centralized Complaint Mechanism**

Victims can file complaints online from anywhere in the country through a single platform, reducing the need to physically visit multiple police stations.

- **Anonymous Reporting**

In sensitive cases such as cyberstalking, revenge porn, or online defamation, complainants can choose to remain anonymous. This is crucial because fear of stigma often prevents women from reporting abuse.

- **Helpline and Complaint Tracking**

The portal connects users to the national helpline **1930** and allows tracking of complaint status, promoting transparency and support.

While these systems exist, many women are still unaware of them, which limits their effectiveness.

- **Special Focus on Crimes Against Women & Children**

The portal specifically recognizes and categorizes offences such as:

- Online grooming and exploitation
- Cyberstalking and repeated harassment
- Non-consensual sharing of intimate images
- Threats, obscene messages, and abuse
- Fake profiles and digital defamation

This reflects official acknowledgment that women face unique risks online and that such crimes are serious, reportable, and traceable under the law.

- **Enforcement and Accessibility Challenges**

Despite the infrastructure, practical gaps remain. Users have reported technical issues, delays, and limited follow-up. For women with low digital literacy, navigating online reporting systems can itself be intimidating.

This highlights an important reality: legal mechanisms must not only exist but must function smoothly and sensitively to truly support victims.

Role of the Indian Cybercrime Coordination Centre (I4C)

The **I4C** supports cyber safety by:

- Training police and judicial officers
- Conducting awareness campaigns
- Engaging cyber volunteers
- Strengthening digital forensic capabilities
- Providing multi-language support

Together, these developments indicate progress, but also remind us that awareness and effective implementation are key to making cyberspace genuinely safer for women.

Cinematic Reflections of Increasing Cyber Crimes Against Women

Indian cinema has increasingly begun to mirror the darker realities of the digital age. Films such as *Hacked* (2020), a Hindi techno-thriller with global streaming reach, and *Drishyam*, which highlights the manipulation and concealment of digital evidence within a crime narrative, foreground the anatomy of technological misuse and its devastating consequences. In *Hacked*, the narrative revolves around a teenage hacker who, unable to accept rejection, weaponizes his technological expertise against an older woman—invading her privacy, manipulating her digital footprint, and orchestrating a sustained campaign of psychological warfare. Through surveillance, data theft, and online defamation, the film illustrates how revenge in the digital era transcends physical confrontation and mutates into invisible yet relentless harassment.

Such portrayals underscore a critical truth: cybercrime against women is rarely confined to screens. Digital abuse frequently spills into offline spaces, manifesting as workplace intimidation, reputational sabotage, blackmail, and coercion. Misuse of private images, emails, or confidential data becomes a tool to suppress professional growth, deny promotions, block increments, or force compliance. Women are often silenced through threats of exposure, character assassination, or social stigma—mechanisms that exploit patriarchal biases already embedded within institutional structures.

By dramatizing these dynamics, contemporary films expose how information technology, while empowering, can also be manipulated to reinforce gendered control. Cyber-enabled revenge, surveillance, and harassment reveal a disturbing convergence of misogyny and technological power—transforming personal rejection into systemic exploitation.

Limitations Faced During the Study

One of the main challenges I faced while working on this topic was the limited availability of detailed and focused books on cyber crimes against women. While cyber law as a subject is well covered, material that deeply explores its gendered impact is comparatively scarce. Most sources explain legal provisions but do not fully capture the lived experiences and emotional realities of women affected by digital abuse.

Although online resources are accessible and useful, much of the content tends to be repetitive. Many articles rely on the same case laws, statistics, and legal sections, offering limited fresh insight or deeper analysis. The availability of information often feels broad, but not necessarily profound.

A deeper limitation lies in the issue itself—cyber crimes against women are widely underreported due to fear, stigma, and lack of awareness. When victims hesitate to come forward, documentation remains incomplete. This silence naturally reflects in academic research, making the subject appear less developed compared to others.

These limitations do not diminish the importance of the topic; rather, they highlight the urgent need for more research, awareness, and open dialogue. In many ways, the gaps in literature mirror the gaps in societal acknowledgment that still need to be bridged.

Conclusion

Women today are no longer fully safe even in their most private digital spaces. Personal messages, photographs, and social media profiles—once seen as intimate and secure—have become vulnerable to misuse and exploitation. Cyber crimes against women are not just technical violations; they reflect deep-rooted gender inequalities amplified by technology. The emotional trauma, reputational damage, and social stigma caused by online abuse can be profoundly damaging.

Addressing this growing threat requires shared responsibility. Women must be equipped with digital awareness and knowledge of legal remedies, while society must reject victim-blaming and promote accountability and respectful online conduct. Families, institutions, platforms, and law enforcement all play a role in shaping safer digital environments.

Cyberspace should empower, not intimidate. Protecting women online is not only a legal duty but a collective social commitment to dignity, safety, and equality.

Bibliography

- CDT Ghaziabad. (n.d.). *Cyber crimes against women & children*. CDT Academic Publications.
- Chanakya National Law University. (2025). *Cyber crimes against women and prevention*. CNLU Academic Publications.
- Chaudhary, S., & Sood, R. (2014). *Mapping cyber crimes against women in India*. *International Research Journal of Commerce and Law, 1*(5). IRJCL Publications.
- International Journal of Law, Justice and Jurisprudence. (2024). *Prevention of cyber-crime against women in India*. *International Journal of Law, Justice and Jurisprudence, 4*(1), 38–49. IJLJJ Publications.
- Kumar Rao, A. (2023). *Revenge pornography: Socio-legal impact*. Jus Scriptum Law Journal. Jus Scriptum Publications.
- Mondaq Ltd. (2024). *The scope of teachers' disciplinary powers: An analysis of the Kerala High Court's ruling on corporal punishment and criminal liability*. Mondaq Publishing.

- National Law University and Judicial Academy, Assam. (n.d.). *Cyber crimes against women: Legal perspectives*. NLUALR Publications.
- Onwuadiamu, G. (2023). *Cybercrime in criminology: A systematic review of criminological theories, methods, and concepts*. *Journal of Economic Criminology*. Elsevier Publications.
- Quest Journals. (2020). *Cyber crimes against women and children*. *Journal of Research in Humanities and Social Science, 8*(1), 75–79. Quest Journals Publications.
- Roopinder Singh. (2023). *Strengthening the IT law*. Independent Legal Commentary Publications.
- Sharma, S. (2023). *Cyberbullying and online harassment in India: Legal provisions and key judicial developments*. Legal Commentary Series.
- State Cyber Cell v. Yogesh Pandurang Prabhu. (2020). *Case analysis*. iPleaders Blog Publications.
- State of Tamil Nadu v. Suhas Katti. (2004). *Case analysis*. Black n' White Journal of Law.
- TheLaw Institute. (2023). *Digital forgery: The evolution of counterfeiting in the digital era*. Law Notes Publications.
- Tigde Law Firm. (2023). *Cyber scams in India: Bank fraud protection and digital safety*. Tigde Legal Publications