International Journal of Law, Human Rights and Constitutional Studies
Volume 6, Issue 1 - 2024, Pg. No. 1-14
Peer Reviewed Journal

Review Article

Empowering Women in the Digital Sphere: Cyber Crime Combat Strategies in Indian Social Media

Samirsinh P Parmar[1], Dr. Swati H. Chauhan[2]

[1]Assistant Professor, Department of Civil Engineering, Dharmasinh Desai University, Nadiad.
[2]Associate Professor, Practice of Medicine Department, Gujarat Homoeopathic Medical College & Hospital, Savli, Dist. Vadodara. Gujarat, India.

I N F O

Corresponding Author:
Samirsinh P Parmar, Department of Civil Engineering, Dharmasinh Desai University, Nadiad.
E-mail Id:
spp.cl@ddu.ac.in
Orcid Id:
https://orcid.org/0000-0003-0196-2570
How to cite this article:
Parmar SP, Chauhan SH. Empowering Women in the Digital Sphere: Cyber Crime Combat Strategies in Indian Social Media. *Int Jour Law Hum Rights Const Stud* 2024;6(1):1-14.

Date of Submission: 2023-11-30
Date of Acceptance: 2024-01-02

A B S T R A C T

As the digital landscape continues to evolve, women face escalating threats in the form of cybercrimes within Indian social media platforms. This paper explores the multifaceted challenges encountered by women in the digital realm and proposes empowering strategies to combat cybercrimes effectively. The study delves into the prevalence of online threats, including cyberbullying, stalking, identity theft, and harassment, targeting women specifically. Recognizing the vital role of social media in women's lives, the paper emphasizes the need for tailored combat strategies. The proposed strategies encompass digital literacy initiatives, enhanced cybersecurity measures, legal frameworks, and community support networks. By empowering women with knowledge and resources, this paper aims to contribute to the creation of a safer and more inclusive digital environment for women in India.

Keywords: Women empowerment, social media, cybercrime, digital awareness, Indian strategies, legal framework.

Introduction

In the dynamic landscape of the digital domain, the substantial impact of Indian social media has seamlessly integrated into the fabric of daily existence. With an increasing number of women embracing the possibilities and interconnectedness facilitated by these platforms, they concurrently confront the growing menace of cybercrimes. This study endeavours to scrutinize the intricate challenges encountered by women navigating the digital expanse and, more critically, to propose all-encompassing strategies for mitigating cybercrimes specifically directed at them. As we observe an unparalleled surge in online engagements, the vulnerabilities ingrained in this digital realm mandate an approach fortified by empowerment. This paper aims to investigate and advocate for robust strategies that leverage awareness, technological resilience, legal frameworks, and communal support to cultivate a more secure and inclusive digital milieu for women in India. By delving into the distinct subtleties of cyber threats faced by women and fostering empowerment, this research strives to contribute to the ongoing dialogue on fortifying the digital future for everyone.

The literature presents a comprehensive exploration of the digital landscape and its intersection with violence against women. The following review synthesizes key findings and insights from various studies and reports.

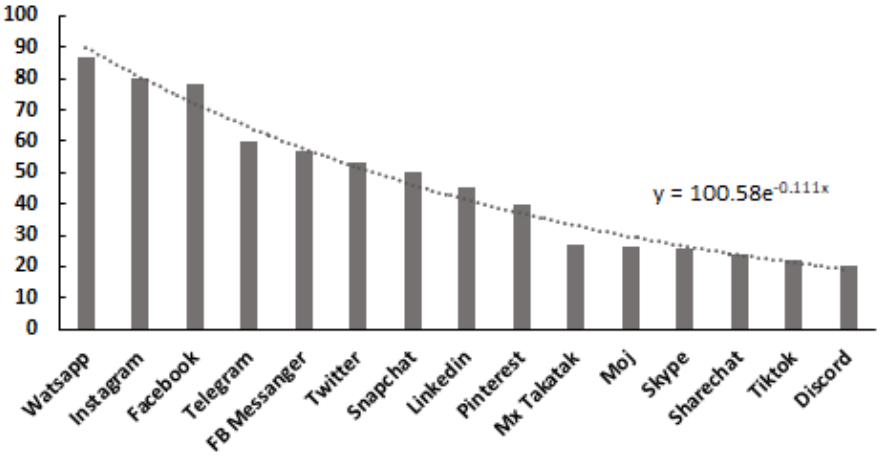
Adriane van der Wilk (2021) emphasized the relevance of international conventions, specifically the Istanbul Convention and the Budapest Convention on Cybercrime, in addressing online violence against women. The paper provides a legal framework for understanding and combating technology-facilitated violence. Cybercrime Investigation (Data Security Council of India) manual offers practical insights into cybercrime investigation. It serves as a valuable resource for understanding the technical aspects of cybercrimes, a crucial component in combating online violence against

women. Halder & Jaishankar (2015 presented a baseline survey on harassment via WhatsApp in urban and rural India. The report delves into the nuances of digital harassment, offering a contextual understanding of the prevalence and nature of online violence against women.

Jenefa S. (2017) studied that, how social media is a tool of violence against women. The research sheds light on the various ways in which social media platforms contribute to, and sometimes amplify, violence against women, offering a nuanced perspective on the intersection of technology and gender-based violence. Kovacs, Padte, and Shobha SV (2013) investigated verbal online abuse against women in India. By examining the dynamics of online abuse, the research contributes to understanding the nature of gender-based violence in digital spaces. Beliriya N K and Abhilasha (2020) exclusively focussed on the legal challenges and proposed solutions to cybercrime against women in India. It provides a legal perspective on addressing online violence, offering insights into the gaps and potential remedies within the legal framework. Saumya Uma (2017) focused on outlawing cyber-crimes against women in India, offering a legal analysis and proposing measures for better protection. The paper contributes to ongoing discussions on legal frameworks to combat online violence.

Figure 1.Most used social media platforms in India in the year 2022.

Sr. No.	Social Media Platform	Starting Year	Communication Interfaces
1	LinkedIn	2003	Message, Images, Video, Voice Messages, Articles
2	Facebook	2004	Message, Images, Voice Call, Video, Live Video, GIFs
3	YouTube	2005	Message (Comments), Video, Live Video, Premieres
4	Twitter	2006	Tweet (Text), Images, GIFs, Video, Voice Messages
5	WhatsApp	2009	Message, Images, Voice Call, Video Call, Status Updates
6	Instagram	2010	Message, Images, Video, IGTV, Reels, Stories, Voice Messages
7	Pinterest	2010	Message, Images, Video
8	Snapchat	2011	Snap (Text, Images, Video), Chat, Voice and Video Calls
9	Telegram	2013	Message, Images, Voice Call, Video Call
10	Roposo	2014	Message, Video, Live Video, Challenges
11	ShareChat	2015	Message, Images, Video, Voice Call
12	Triller	2015	Message, Video, Music Collaboration
13	TikTok	2016	Message, Video, Live Video, Duets, Challenges
14	Josh	2020	Message, Video, Duets, Challenges
15	MX TakaTak	2020	Message, Video, Duets, Challenges
16	Koo	2020	Message, Voice Messages



Ref: https://oosga.com/social-media/ind

Figure 1.Soical media users percentage on different platforms

Viswanath and Basu A. (2015) studied an innovative mobile app designed to collect data on women's safety in Indian cities. It sheds light on technological solutions that aim to enhance women's safety, providing insights into the role of technology in preventing violence against women. These studies collectively contribute to the understanding of online violence against women, combining legal, technical, and social perspectives. The literature underscores the urgency of addressing this issue holistically, considering legal frameworks, technological innovations, and societal norms.

India's social media landscape is dynamic, witnessing transformative shifts, regulatory measures, and substantial growth, making it a key player on the global stage. India, as the world's most populous country with the second-largest number of internet users, boasts a highly attractive yet competitive internet market. Despite only 43% of the population having internet access, a robust social media user base spends an average of 2.6 hours daily on various platforms.

Introduction to Social Media

Social media platforms refer to online services or applications that facilitate the creation, sharing, and exchange of user-generated content, as well as the networking and interaction between users. These platforms provide a virtual space for individuals to connect, communicate, and share various forms of content such as text, images, videos, and links. It's important to note that while social media platforms offer numerous benefits, they also come with challenges, including issues related to privacy, online harassment, and the spread of misinformation. Users should be mindful of their digital presence and use these platforms responsibly.

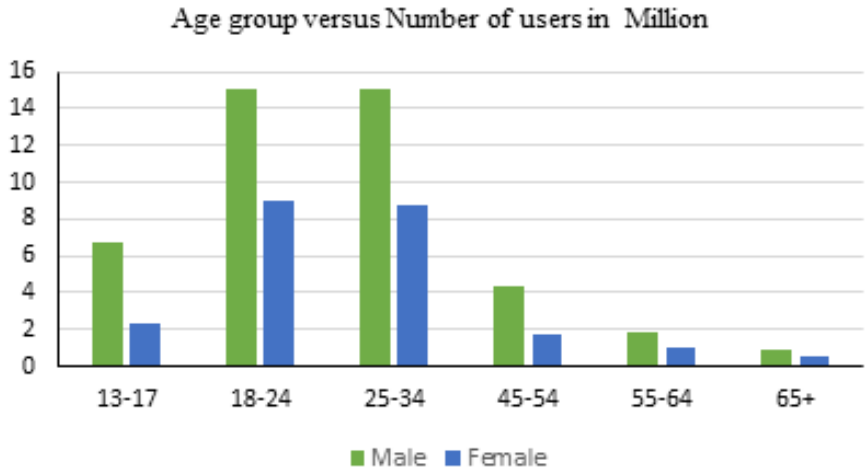
Usage of Social Media

Social media platforms are versatile, meeting diverse user needs. Communication features like direct messaging and comments enable real-time interaction. Networking allows connections based on shared interests, affiliations, or relationships, fostering effective digital networking. Content sharing empowers users to distribute updates, photos, videos, and articles, influenced by individual privacy settings.

Social media is a crucial source for information discovery, offering news and trends. Users curate feeds to stay informed by following relevant accounts. Entertainment includes varied content like videos and memes, providing leisure opportunities. Businesses leverage social media for dynamic promotional activities, advertising products, services, and events. Online communities form around specific topics, fostering a sense of belonging. Social media serves educational purposes, with organizations sharing knowledge. Activism thrives on these platforms, providing space to raise awareness and mobilize support. Interactivity allows users to provide feedback, facilitating engagement within the digital community. Overall, social media's versatility empowers users for diverse online experiences.

India is poised to become the largest market for social media advertising spending outside of China in the next decade. Latest data as of January 2023 indicates around 448.8 million Facebook users and approximately 252.41 million Instagram users in India.

Male users constitute approximately 72.99%, while female users account for around 27.01% on Facebook, and on Instagram, male users make up around 72.74%, with female users at 27.26%. Social commerce is on the rise in India, with a predicted compound annual growth rate of 55-60% between FY 2020-2025, expanding the market from $1.5-2 billion to $16-20 billion. A study by Oxford University reveals that 54% of Indians turn to social media for "truthful" information, surpassing the global average of 37% and the US at 29%.



Ref: https://oosga.com/social-media/ind

Figure 2.Usage of social media according to age group in the year 2022

Figure 3.Flowchart of transference of Cyber-crime

Cyber Crime Against Women - Statistics for India

The prevalent cybercrimes targeting women encompass activities such as cyber blackmail, threats, cyberpornography, dissemination of explicit sexual content, stalking, bullying, defamation, morphing, and the creation of fraudulent profiles. Table-A (Appendix) indicates the pros and cons for the usage of social media.

As of 2019, there has been an overall increase of 18.4% in cybercrime incidents. However, the specific cases of cybercrimes against women have witnessed a steeper rise, escalating by 28%, as reported by the National Crime Record Bureau.

According to the data, out of the 52,974 incidents registered in 2021, 20.2% (10,730 incidents) were documented as crimes against women. The state-wise distribution highlighted Karnataka with the highest count of instances (2,243), trailed by Maharashtra (1,697) and Uttar Pradesh (958) in 2021.

Figure-3 demonstrates the operational flowchart of the occurrence of cyber-crime. The availability of devices such as smart phones, tablet, pc's and smart TV's are plays pivotal role in increase of cyber-crime. Equally the availability of internet facility to the end user, from urban to rural population in last decade is one of the causes of increase in cyber-crime against women.

The surge in cybercrime can be attributed to various factors:

1. Escalation in online traffic.
2. Insufficient awareness.
3. Limited technical knowledge among both law enforcement and the general public.
4. Challenges encountered in the investigation of cybercrime cases.

Types of Cyber Crimes Against Women

- **Online Harassment and Cyberbullying:** Online harassment and cyberbullying involve the use of digital platforms to send threatening, hurtful, or intimidating messages to an individual. It often includes persistent attacks, public humiliation, and the spread of false rumors. Perpetrators exploit the anonymity of the internet to target victims repeatedly. This can include posting hurtful comments on social media, sharing embarrassing information, or creating fake profiles to impersonate the victim. Victims of online harassment may experience emotional distress, anxiety, depression, and even physical harm in extreme cases. It can also lead to reputational damage, affecting personal and professional relationships.
- **Revenge Porn:** Revenge porn involves the unauthorized sharing of intimate images or videos, typically by a person seeking revenge after a relationship breakdown. Perpetrators share explicit content without the consent of the victim, often to harm their reputation. This may involve the distribution of intimate images or videos through social media, websites, or other online platforms. Victims of revenge porn face severe emotional distress, damage to personal relationships, and potential harm to their professional reputation. Legal consequences for perpetrators vary by jurisdiction.
- **Online Stalking:** Online stalking involves the persistent pursuit of an individual on the internet, often characterized by monitoring their online activities, gathering personal information, and maintaining unwanted contact. Stalkers use various online platforms to track and harass their victims. This can include sending threatening messages, monitoring social media accounts, and gathering personal information to use against the

victim. Online stalking can cause severe psychological distress, anxiety, and a constant feeling of invasion of privacy. Victims may alter their online behavior to avoid further harassment.

- **Identity Theft:** Identity theft is the unauthorized use of someone's personal information, such as financial details or social security numbers, to impersonate the victim. Perpetrators obtain personal information through various means, including phishing, data breaches, or social engineering. Stolen information is then used for financial gain or to commit other crimes. Victims of identity theft can suffer significant financial losses, damage to credit scores, and legal complications. Restoring one's identity can be a lengthy and challenging process.
- **Financial Fraud:** Financial fraud involves the use of deceptive practices to obtain financial information and commit fraudulent activities online. Perpetrators use tactics such as phishing emails, fake websites, or malware to obtain sensitive financial information. Stolen details are then used for unauthorized transactions, identity theft, or draining bank accounts. Victims may experience significant financial losses, unauthorized transactions, and challenges in recovering stolen funds. Financial fraud can also lead to reputational damage.
- **Catfishing:** Catfishing is the creation of a fake online persona to deceive others, often for romantic relationships or financial gain. Perpetrators use false information, images, and narratives to establish trust with the victim. Once trust is gained, cat fishers may exploit victims emotionally or financially. Victims of catfishing often experience emotional distress, heartbreak, and financial losses. The realization of being deceived can have lasting psychological effects.
- **Online Grooming:** Online grooming involves building a relationship with a minor online, often with the intention of exploiting them sexually. Predators use manipulation, flattery, and gifts to gain the trust of a minor. The goal is to engage in inappropriate activities, which may escalate to sexual exploitation. Online grooming can have severe consequences for minors, including emotional trauma, sexual exploitation, and long-term psychological harm. Early intervention is crucial to prevent harm.
- **Hate Speech and Misogyny:** Hate speech and misogyny involve the use of online platforms to spread discriminatory, offensive, or misogynistic content targeting individuals or groups based on gender. Perpetrators use online platforms to disseminate content that promotes hatred, discrimination, or violence against individuals based on their gender. This can include sexist comments, threats, or harmful stereotypes. Online hate speech contributes to a hostile online environment and can lead to real-world harm. Victims may experience emotional distress, fear, and a sense of exclusion.
- **Phishing and Social Engineering:** Phishing and social engineering involve deceptive tactics to trick individuals into divulging sensitive information, often through fake emails or websites. Perpetrators create fake websites, emails, or messages that appear legitimate to trick individuals into providing confidential information. Social engineering exploits human psychology to manipulate people into revealing sensitive details. Phishing attacks can lead to identity theft, financial fraud, and unauthorized access to personal information. Victims may unknowingly provide access to passwords, credit card details, or other sensitive data.
- **Cyberstalking via GPS and Location Services:** Cyberstalking via GPS and location services involves using technology to track the real-time location of a victim through GPS or other location services. Stalkers leverage technology to monitor the physical movements of their victims. This information may be obtained through GPS tracking or location services on smartphones and other devices. Victims of cyberstalking via location services may experience a loss of privacy, fear for their safety, and potential physical harm if the stalker escalates their activities.
- **Email Spoofing:** Email spoofing involves the creation of emails with a forged sender address, intending to deceive the recipient about the origin of the message. Perpetrators use techniques to manipulate email headers and sender information to make the email appear as if it is from a trusted source. This can be used for phishing attacks or spreading malicious content. Email spoofing can lead to the spread of malware, unauthorized access to sensitive information, and phishing attacks. Individuals and organizations may fall victim to scams or compromise their cybersecurity.

Governing Factors Which Increase Cyber Crimes Against Women In India

The increase in cyber-crimes against women in India can be attributed to several governing factors. These factors contribute to a challenging environment where women become more susceptible to various forms of cyber threats and offenses. Some key factors include:

- **Digital Gender Divide:** The existing digital gender gap contributes to women's limited access to digital technologies and literacy, making them more vulnerable to online exploitation.
- **Anonymity on Social Media:** Anonymity enables the creation of fake profiles with the intent to deceive or harass. Perpetrators can easily impersonate others or create fictitious identities to carry out cybercrimes

against women. Anonymity allows individuals to make false accusations against women without fear of repercussions. Anonymous individuals may engage in the unauthorized collection and dissemination of private information, infringing upon the privacy of women.

- **Irresponsible Social Media Operation:** Social media platforms warns and guides against cybercrime before registering into it. They also make available various security features to prevent any unlawful activities against users. But sometime knowingly or un knowingly users are not using such security features. This is one of the major causes of cyber-crime against women.
- **Lack of Awareness:** Limited awareness among women about the potential risks and security measures in the online space contributes to their increased vulnerability.
- **Inadequate Legal Framework:** Gaps and inadequacies in the legal framework related to cyber-crimes against women, coupled with slow legal processes, hinder justice delivery.
- **Geographical location of Criminal:** In cyber world, the criminal can be possible from any country, state, religion, group etc. which is hardly possible to trace digitally. Punishment to such criminals requires international laws and court which is nearly impossible in current world order, hence the cyber crime against women increases just because of geographical location of the criminals.
- **Impersonation and Fake Profiles:** The creation of fake profiles and impersonation on social media platforms for malicious purposes is a prevalent issue, causing harm to women's reputations.
- **Privacy Concerns:** The challenge of protecting personal information and privacy in the digital age is a significant concern, with data breaches and online privacy violations posing threats to women.
- **Technological Advancements:** While technological advancements have brought numerous benefits, they have also provided more sophisticated tools and methods for cyber criminals to target women online.

Dealing With Cyber Crime Against Women in India

Preventing Cyber Crime Against Women In India

The internet has become an integral part of our daily lives, fundamentally transforming how we communicate, connect with friends, share updates, engage in gaming, and conduct online shopping. It has a profound impact on various aspects of our day-to-day existence.

In the vast expanse of cyberspace, we are virtually connected with millions of online users worldwide. As the use of cyberspace continues to rise, cybercrimes, particularly those targeting women and children, such as cyber stalking, cyber bullying, cyber harassment, child pornography, and dissemination of inappropriate content, are also on the rise. To ensure a secure online experience, it is crucial to adopt certain cyber safety practices that contribute to making our online interactions safe and productive. The preventive measure for cybercrime against women is divided in two parts. One for the role of parents for crime against girl child and second as preventive measures for teen to adult aged women group.

Promoting Cyber Awareness and Hygiene for Parents

Initiate open conversations with your children regarding potential online threats such as grooming, bullying, and stalking. Stay informed about their online activities and establish clear guidelines for internet and online game usage.

- **Be vigilant for signs of behavioral changes:** If you observe your child spending more time online and becoming defensive or secretive about their online activities, it could be indicative of cyberbullying. Engage in open dialogue and encourage them to participate in other activities. Safeguard your child from cyber grooming, a deceptive practice where someone establishes an emotional connection with a child through social media or chat platforms for potential sexual exploitation. Children may unintentionally remove privacy settings on social media to expand their friend circle. Parents should educate them on responsible social media use and assist in configuring robust privacy settings.
- **Exercise caution with links and attachments:** Avoid clicking on links or files received via email, text messages, or social media from unknown sources. This precaution is crucial to prevent potential malware infections on your device.
- **Cover your webcams:** Protect your privacy by covering webcams when not in use, especially on devices like laptops. This precaution helps prevent any unauthorized observation, recording, or exploitation of daily activities through hacked webcams.
- **Implement parental control measures:** Install antivirus software with parental control features or dedicated parental control software on your children's devices. Regularly review the privacy settings of the social media platforms they use.
- **Prioritize software updates:** Keep your operating system and software up-to-date to patch vulnerabilities that hackers may exploit. Avoid downloading software, games, music, or apps from untrusted sources to minimize security risks.
- **Secure browser settings:** opt for the latest browser versions and install secure browsing tools to protect against hackers and malware. Regularly update these tools to ensure continuous protection against potential threats.

Promoting Cyber Awareness and Hygiene Among Women (Teens, and Young Adults)

Safeguard Your Online Presence Just as You Protect Yourself

In case you haven't configured the appropriate settings on your social media accounts, your photos and videos may be accessible, downloaded, and utilized by others without your awareness. Ensure you choose the right privacy settings and content sharing filters on social media platforms to share your information, photos, and videos exclusively with trusted individuals. Exercise caution when accepting friend requests from strangers on social media. Learn how to block individuals causing discomfort. Understand the process of removing someone from your friends list. Always log out from social media websites after use. Implement password protection on your phone for added security. If you observe the creation of a fake account, promptly notify the social media service provider to block the account.

Stay Attentive to Your Presence in Video Chats and Calls

Your video chats on social media platforms may be recorded by the individual on the opposite end. Instances exist where supposedly private video chats have been recorded and disseminated on social media groups and websites. Exercise caution when accepting chat requests from unfamiliar individuals.

Use of Smartphones to Report Sensitive Content

Avoid using smartphones for capturing sensitive personal photos and videos. Since most smartphones are linked to the internet and cloud storage, images or videos taken with a smartphone connected to the cloud may automatically be saved there. Even if users delete the content from their phones, it could still be recoverable from the cloud account or any other device/PC linked to the cloud with the same account. If someone has taken such photos using a smartphone, treat the matter seriously and ensure that the content is deleted not only from their smartphone but also from the cloud and any other connected devices using the same account.

Protect Yourself from Cyber Stalking: Cyber stalkers show advances on a person repeatedly despite clear indication of disinterest by such person. They use internet, email, social media or any other form of electronic communication for stalking. To avoid stalking following steps shall be taken.

- Disable location services for social media sites, mobile devices etc.
- Refrain from sharing your personal information like Phone number, e-mail address, photographs with unknown persons.
- Consult your relatives and friends, if you think you are a victim of Cyber stalking.

Table 2.Data recovery software's and the supporting digital devices

Sr. No.	Data Recovery Software	Devices Supported	Ease of Use
1	Recuva	Windows PCs, external drives, memory cards	User-friendly interface
2	EaseUS Data Recovery Wizard	Windows, Mac, external drives, memory cards	Intuitive and straightforward
3	Disk Drill	Windows, Mac, external drives, memory cards	User-friendly with additional tools for disk health
4	PhotoRec	Windows, Mac, Linux, external drives, memory cards	Command-line interface, suitable for advanced users
5	Wondershare Recoverit	Windows, Mac, external drives, memory cards	Intuitive interface with advanced features
6	R-Studio	Windows, Mac, Linux, external drives, memory cards	Professional-grade tool for advanced users
7	Prosoft Data Rescue	Windows, Mac, external drives	User-friendly with advanced features
8	DiskWarrior	Mac, external drives	Mac-specific, known for repairing disk issues
9	Dr.Fone - Data Recovery (Mobile)	iOS, Android	User-friendly for recovering mobile data
10	Tenorshare UltData (iPhone Data Recovery)	iOS	Specialized for iPhone data recovery
11	Disk Digger	Windows, Android	Simple interface for file recovery

Beware of Fake Social Media Accounts: Not all the accounts are real and not all information provided on accounts are true. Be cautious while accepting friend requests from strangers.

Be Cautious with Sensitive Browsing

One should browse shopping or banking websites or apps only on a device that belongs to him/ her or on a trusted network. Avoid using friend's phone, public computer, cyber cafe or free Wi-Fi for sensitive browsing as data can be stolen or copied.

Be Careful While you Give your Mobile Devices, Pc's for Servicing /Repairing/ Selling

Personal commuters and mobile devices consist private information's which needs to be erased before sending it for repairing, servicing or selling. The deleted data on your communication devices can be recovered. It is advisable for women's to not to sale their digital devices without doing proper formatting the system. Table-2 describes the data recovery software's available in open market and the devices from which the data can be retrieved.

The data recovery software's can retrieve the data from the devices such as smartphone, tablets, hard disk of computers etc. If the devices are sold or getting repaired with the persons of malicious activity, they can use the data to conduct previously mentioned cyber-crimes. It is advisable to format the devices thoroughly before re-sale of such devices and must locked by strong passwords while giving them for repairing.

Protect your communication devices: Prevent others from accessing your devices by providing password, PIN, Pattern or bio-metric information. Always install applications to your mobile phones, computers, etc. from a trusted source only e.g., Play store, App store or from official company websites

Report if you find content related to of Child Pornography: (CP)/Child Sexual Abuse Material (CSAM) or sexually explicit material

- Any content related to of Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material such as Rape/ Gang Rape (CP/RGR) content should be report to the concerned social media website
- If anybody of your acquaintance shares Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material with you, it is your duty as a responsible citizen to inform the concerned person that publication, collection and distribution of Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material is illegal and he should refrain from doing such activities.
- You can also report it on National Cyber Crime Reporting Portal (www.cybercrime.gov.in)

Ipc For Cyber Crime Against Women

All cyberspace users are bound by global laws governing legal aspects arising from networked computer technology and digital platforms. These laws serve to safeguard individuals from cybercrimes, offering protection and justice for victims. Specific crimes punishable under the law with rigorous imprisonment and fines are outlined in the Indian Penal Code (IPC, 1860), specifically in sections 354, added as a result of the 2013 Criminal Amendment Act.

Section 292: The purpose of this section was to address the sale of obscene materials, however, in this digital age, it has evolved to deal with various cybercrimes as well. A manner in which obscene material or sexually explicit acts or exploits of children are published or transmitted electronically is also governed by this provision. The penalty for such acts is imprisonment and fines up to 2 years and Rs. 2000, respectively. The punishment for any of the above crimes may be up to five years of imprisonment and a fine of up to Rs. 5000 for repeat (second-time) offenders.

Section 354A: This section addresses sexual harassment, defining acts such as demanding or pleading for sexual favours, displaying pornography against a woman's will, or making sexual remarks as punishable offenses. Offenders may face rigorous imprisonment for up to three years, a fine, or both. In the first two cases, there is a possibility of up to one year of imprisonment, a fine, or both.

Section 354C: Voyeurism, as per Section 354C, involves taking a photograph of a woman engaged in a private act and/or publishing it without her consent. For an act to qualify as "voyeurism," the circumstances must be such that the woman would usually expect not to be seen. Offenders found guilty may be fined and sentenced to up to three years in prison for the first conviction and up to seven years on subsequent convictions.

Section 354D: The addition of Section 354D addresses stalking prohibition, encompassing online stalking. Stalking is defined as pursuing or approaching a woman despite her obvious disinterest or observing a woman's online behaviour, internet usage, or electronic communication. Convictions for stalking may result in up to three years in jail and a fine, with subsequent convictions potentially leading to up to five years in prison and additional fines.

Section 379: The punishment involved under this section, for theft, can be up to three years in addition to the fine. The IPC Section comes into play in part because many cybercrimes involve hijacked electronic devices, stolen data, or stolen computers.

IT ACT

Offenses outlined in the IT Act 2000 encompass a range of activities, such as tampering with computer source documents. These offenses are detailed in specific sections:

Table 3.Section of the IT act and concern offense

Section No.	Offense Description
Section 65	Hacking of computer systems
Section 66	Publishing of information that is obscene in electronic form
Section 67	Unauthorized access to a protected system
Section 70	Breach of confidentiality and privacy

The sub section of the IT Act 2000 described below with respect to the type of offence, and the magnitude of punishment. Changes made under the IT Amendment Act,2008.

Section 66B contains punishment for deceitfully receiving stolen computer or communication devices.

Section 66C: Identity theft constitutes a punishable offense under Section 66C of the IT Act, particularly in cases of cyber hacking. This clause stipulates that individuals who falsely or dishonestly use another person's electronic signature, password, or distinctive identifying feature may face a maximum penalty of three years in prison and a fine of up to Rs. 1 lakh.

Section 66D contains penalty for cheating by personation.

Section 66E: Section 66E addresses breaches of privacy rights. Anyone found guilty of taking, sharing, or sending a picture of another person's private area without their consent, thereby violating their privacy, can face up to three years of imprisonment and/or a fine.

Section 67: Under Section 67, the publication, transmission, or distribution of obscene content is prohibited. A first conviction may result in a maximum sentence of three years in prison or a fine, while a second conviction could lead to up to 5 years of imprisonment and an additional fine.

Section 67A: Engaging in the publication, transmission, or assistance in the transfer of sexually explicit material is considered a misdemeanor under Section 67A. A first conviction may lead to a maximum penalty of five years in prison and a fine, and subsequent convictions could result in up to seven years of imprisonment and additional fines.

Section 67B punishment for transmission of sexually explicit materials of children has been included

Government of India Website for Cyber Crime

The government has established the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) to facilitate the reporting of various cybercrimes, particularly those targeting women and children. Additionally, a module of the Citizen Financial Cyber Fraud Reporting and Management System has been incorporated, enabling the prompt reporting of financial frauds and preventing illicit money transfers by fraudsters.

Role of Cyber World to Mitigate the Problem

Social Media Website / Apps – Rules and Regulation

To enhance the security of websites and applications, it is imperative to integrate robust security features that effectively safeguard user information. Employing advanced encryption methods stands as a fundamental step in securing user data, ensuring that sensitive information remains inaccessible to unauthorized entities. The implementation of encryption adds an additional layer of protection, making it significantly challenging for potential threats to compromise the confidentiality of user data. Furthermore, the importance of regularly updating security protocols cannot be overstated. By staying vigilant and proactive in updating security measures, organizations can fortify their defences against emerging cyber threats. This proactive approach not only addresses existing vulnerabilities but also positions websites and apps to tackle new challenges that may arise in the ever-evolving landscape of cybersecurity. In essence, the incorporation of robust security features, advanced encryption, and regular updates collectively forms a comprehensive strategy to bolster the security posture of websites and applications, thereby fostering user trust and safeguarding valuable digital assets.

Security Features into the Website and Apps

Ensuring the security of websites and applications is paramount in safeguarding user information. By integrating robust security features, organizations can create a fortified defence against potential threats. Advanced encryption methods play a pivotal role in protecting user data from unauthorized access, adding an extra layer of security to sensitive information. Regularly updating security protocols is equally essential to stay ahead of emerging cyber threats.

Table-4 Social media App's and their respective security features

Sr. No.	Social Media App	Security Features
1	Facebook	Two-Factor Authentication, Privacy Settings, Account Recovery Options
2	Instagram	Two-Factor Authentication, Private Account Settings, Login Activity Monitoring
3	Twitter	Two-Factor Authentication, Login Verification, Privacy and Safety Settings
4	LinkedIn	Two-Factor Authentication, Privacy Settings, Account Activity Monitoring
5	Snapchat	Two-Factor Authentication, Privacy Settings, Location Sharing Controls

6	WhatsApp	End-to-End Encryption, Two-Step Verification, Privacy Settings
7	Tik Tok	Privacy Settings, Restricted Mode, Account Security Options
8	Pinterest	Two-Factor Authentication, Privacy Settings, Account Activity Tracking

This proactive approach not only addresses existing vulnerabilities but also prepares the digital infrastructure to tackle evolving challenges in the dynamic landscape of cybersecurity. Table-4 delineates the security features available for respective social media applications. Use of security features depends on the proficiency of the user , hence not all user are using security features available to them. Providing awrness regading security features available for respective applications can mitigate the problem of cyber crime significantly. Together, these measures form a comprehensive strategy to enhance the overall security posture of websites and apps, instilling user confidence and trust in the protection of their valuable data.

Challenge Against Dark Web and Hackers

Combating cybercrime against women in Indian social media, particularly the challenges posed by the dark web and hackers, requires a multifaceted approach. Detailed strategies to address this issue involve developing and implementing robust cybersecurity measures tailored for countering dark web activities, including advanced encryption, firewalls, and intrusion detection systems. Additionally, there is a need to enhance collaboration between cybersecurity experts, government agencies, and technology companies to establish a proactive information-sharing mechanism for swift responses to hacking attempts. Allocating resources for cutting-edge technologies, such as artificial intelligence and machine learning, is crucial to monitor and neutralize threats originating from the dark web. Public awareness campaigns are essential to educate users, especially women, about the risks associated with the dark web and hacking activities, promoting safe online practices and providing resources to recognize and report suspicious activities. Strengthening legislation related to cybercrimes against women, with a focus on activities from the dark web, is imperative, empowering law enforcement agencies with the necessary tools and training for investigation and prosecution. International cooperation is vital to combat cross-border cybercrimes, involving partnerships with global cybersecurity organizations and law enforcement agencies for intelligence sharing and coordinated efforts against transnational threats. Encouraging ethical hacking initiatives and implementing continuous monitoring of online platforms, along with a robust incident response plan, further contribute to strengthening the defence against cybercrimes on the dark web and mitigating risks faced by women in the Indian social media landscape.

Case Studies

Case Study on Cyber Stalking

The first conviction in a cyber stalking case against a woman in Maharashtra took place in July 2015 in the case of Yogesh Prabhu v. State of Maharashtra, decided by the Additional Chief Metropolitan Magistrate M.R. Natu.11 In 2009, the woman initially chatted with Yogesh Prabhu online. When he made a marriage proposal to her, she turned it down. Thereafter she stopped responding to his messages as she found his behavior suspicious. She also removed him from her friends' list. However, Prabhu continued to keep an eye on her profile and her whereabouts, and stalk her through the internet. Some months later, she received mails from an unknown email account, containing obscene images and video clips.

She initially ignored them, but when the obscene mails did not stop, she lodged a police complaint, and the Cyber Crime Investigation Cell took over the investigation. Internet Protocol (IP) address of the computer was traced to a Vashi firm where Yogesh Prabhu worked. The cyber cell filed a 200 paged charge sheet in Sep 2009, after which trial began. During the trial, eight witnesses, including the aggrieved woman, Prabhu's colleagues, cyber experts and police officials were examined by the Public Prosecutor. The magistrate's court convicted Prabhu under S. 509 IPC (words, gestures or acts intended to insult the modesty of a woman) and S. 66E of the Information Technology Act, 2008 (punishment for violation of privacy). This was because the cyber stalking provision - S. 354D of the IPC - was enacted in 2013 and could not be applied retrospectively to a crime committed in 2009.

Cyber Pornography

The first ever conviction in India for cyber pornography, was in the case of Suhas Katti v. State of Tamil Nadu, decided by a Chennai court in 2004.12 The woman, a divorcee, complained to the police about a man who was sending her obscene, defamatory and annoying messages in a Yahoo message group, after she turned down his proposal for a marriage. The accused opened a fake email account in the name of the woman, and forwarded emails received in that account. The victim also received phone calls by people who believed that she was soliciting for sex work. The police complaint was lodged in February 2004 and within a short span of seven months from the filing of the First Information Report, the Chennai Cyber Crime Cell achieved a conviction. Katti was punished with two years' rigorous imprisonment and Rs. 500 fine under S. 469 IPC (forgery for the purpose of harming reputation), one year's simple

imprisonment and Rs. 500 for offence under S. 509 IPC ((words, gestures or acts intended to insult the modesty of a woman) and two years' rigorous imprisonment and Rs. 4000 fine for offence under S. 67 of IT Act 2000(punishment for publishing or transmitting obscene material in electronic form).

Circulation of Private Images and Video

One of the most well-known incidents of voyeurism was the Delhi Public School MMS incident of 2004, which involved the creation of a pornographic MMS of two students of Delhi Public School in a sexual act, and its illegal distribution as well as bid to auction on

the website eBay India (then known as Bazee.com). The Chief Executive Officer of the website was thereafter prosecuted under various provisions of the Information Technology Act, as the IPC had not criminalized such acts.13 The circulation of video clips of rape and gang rape incidents on the internet would attract these provisions. It is important to note that there may be situations where the victim consents to the capturing of such an image, but does not consent to its dissemination to third persons. If the image is disseminated to such persons, the dissemination will be considered an offence under this section. For example, women have reported that they have sent images of themselves in skimpy clothes or in the nude to their intimate partners through WhatsApp or Instagram, based on the partner's request. In other situations, with the woman's consent, physical intimacy with the partner has been recorded. Subsequently, when the relationship turns bitter, the partner has attempted to take revenge or blackmail the woman by disseminating such images / video clips. Such acts would attract these legal provisions. They could also attract the provision of criminal breach of trust (S. 406 IPC), which involves dishonesty misappropriating or converting to his own use property that had been entrusted in him.

Morphing

Morphing involves editing the original picture by an unauthorized user - when an unauthorized user with fake identity downloads the victim's pictures and then uploads or reloads them after editing. It is a common phenomenon that women's pictures are downloaded from websites by fake users and again reposted/ uploaded on different websites by creating fake profiles after editing them. Very often, morphing involves attaching an image of the face of a woman, who is being targeted, with that of the naked or skimpily clad body of another through the use of image-editing software. Such morphed images are intended to tarnish the image of the victim woman and malign her character. Cybercrimes against women involving morphed photographs are reportedly on the rise in India. While celebrities are often an easy prey to this crime, an ordinary woman too is targeted by a man who may seek to take revenge on her for rejecting his proposal for an intimate relationship, or to blackmail her or to otherwise harass her/ tarnish her image among her circle of family and friends for a real/perceived harm caused by her to the abuser.

Such an act could attract offences under S.43 (which includes acts of unauthorized downloading/copying/extracting and destroying/altering data) and S.66 of the IT Act (which spells out various computer-related offences). Additionally, the violator can be booked under various provisions of the IPC such as sexual harassment under S.354A, public nuisance under S. 290, obscenity under S. 292A and S. 501 for defamation.

Sending Obscene / Defamatory / Annoying Messages

Various legal provisions can be invoked in response to such crimes, encompassing offenses like sexual harassment (S. 354A IPC), defamation (S. 499 IPC), assault or criminal force against a woman with the intent to outrage her modesty (S. 354 IPC), and acts intended to insult the modesty of a woman (S. 509 IPC). Offenses under S. 354 and S. 509 IPC are rooted in colonial and patriarchal notions tied to the sexual assault of women, revolving around public morality, decency, and the modesty of women. The application of these provisions introduces the potential challenge of judicially determining 'modesty' and assessing whether the victim possesses 'modesty' being violated. Nonetheless, these provisions serve a purpose in addressing cybercrimes against women not clearly defined in the IPC and the IT Act. Criminal defamation (S. 499 IPC), involving harm to a person's reputation through words or visible representations, can be particularly pertinent. This provision has the potential to be invoked when women are defamed as sex workers or targeted with sexist abuses, thus tarnishing their reputation in online communities or chatrooms.

Online Trolling / Bullying / Blackmailing / Threat or Intimidation

In Saddam Hussain v. State of M.P., the accused had outraged the modesty of the victim, video recorded the same on his phone and used the same to blackmail her.16 A criminal complaint was lodged under S. 354D IPC (stalking), S. 507 IPC (criminal intimidation by an anonymous communication) of the IPC and S. 66A of the IT Act (which has subsequently been struck down as unconstitutional in Shreya Singhal v. Union of India).17 A petition was filed before the Madhya Pradesh High Court for quashing on the basis of a compromise arrived at between the woman and the accused. The High Court refused to quash the proceedings, stating that the offences were against the society at large and a personal compromise between the parties would not affect the continuation of the prosecution. This case indicates

that courts treat cyber stalking and cyber bullying as very serious offences.

Email Spoofing and Impersonation

Impersonation involves representing oneself to be a person one is not. The anonymity of users in the cyber space lends itself easily to impersonation of women. For example, in a reported case, Manish Kathuria impersonated a woman, Ritu Kohli (a married woman) in an internet chat room in 2001, and used obscene language, disseminated her home phone number and invited phone calls. She started receiving numerous phone calls at odd hours. He was arrested by the Delhi police, and charged with 'outrage of modesty' (S. 354 IPC) & S. 509 – which had nothing to do with cyber-crimes he had committed – due to want of appropriate legal provisions. There was no progress in the case, and the frustrated woman reportedly moved out of India. Email spoofing and impersonation could attract offences under cheating (S. 415 IPC) and cheating by personation (S. 416 IPC). 'Cheating by personation' entails cheating by pretending to be some other person, or representing himself to be a person that he is not. The law explains that the offence of cheating by personation is committed whether or not the individual who is personated is a real or imaginary person. S. 66D of the IT Act also provides for punishment for cheating by personation by using a communication device or a computer resource. It is an offence punishable with up to three years imprisonment and fine of up to Rupees one lakh under the IT Act.

Discussion

The escalating prevalence of cybercrime against women underscores the critical need for robust legal frameworks. Existing laws often fall short in addressing the nuanced nature of gender-specific cyber threats. Cybercrimes, including online harassment, stalking, and revenge porn, require specific attention due to their disproportionate impact on women. Legislation tailored to these offenses is crucial for providing adequate protection, ensuring justice, and deterring potential perpetrators. Moreover, legal measures need to evolve alongside emerging cyber threats to effectively address the ever-changing landscape of online crimes against women.

Despite the existence of laws, on-ground challenges impede the effective handling of cybercrimes against women. Limited awareness among law enforcement agencies and the judiciary regarding the intricacies of cyber offenses poses a significant hurdle. Insufficient technical expertise further complicates the investigation and prosecution processes. The underreporting of incidents due to social stigma and fear of retaliation adds to the complexity. Addressing these challenges requires comprehensive training for law enforcement, streamlined reporting mechanisms, and efforts to destigmatize victimhood, fostering a more supportive environment for reporting cybercrimes.

As artificial intelligence (AI) continues to advance, it introduces new challenges in combating cybercrime against women. AI-driven tools can be exploited to automate and amplify cyber threats, making them more sophisticated and challenging to detect. Deep fakes, for instance, pose a growing concern, enabling the creation of realistic yet fabricated content, including explicit material. Moreover, biased algorithms may perpetuate gender-based discrimination, influencing the severity of cybercrimes. Tackling these challenges necessitates a proactive approach, including the development of AI-driven countermeasures, ethical AI guidelines, and continuous monitoring to mitigate the evolving risks associated with AI in the realm of cybercrimes against women.

Conclusion

The study underscores the imperative for comprehensive strategies to counter cybercrimes targeting women in the realm of Indian social media. It places a strong emphasis on the following key components:

- **Awareness and Digital Literacy:** The need to empower women through initiatives focused on awareness and digital literacy to enhance their comprehension of online threats.
- **Technological Fortification:** Advocating for heightened cybersecurity measures to shield women from the ever-evolving landscape of cyber threats in the digital sphere.
- **Legal Frameworks:** Acknowledging the importance of gender-specific legal frameworks to address cybercrimes and urging policymakers to adapt legislation to the dynamic digital environment.
- **Community Support:** Highlighting the pivotal role of community support in establishing a secure digital space for women, both in online and offline contexts.

The recommended holistic approach integrates awareness, technology, legal safeguards, and community resilience. The implementation of these strategies by stakeholders can contribute significantly to creating an inclusive and secure digital environment, allowing women to derive the benefits of social media without compromising their safety. The research aspires to stimulate discussions, influence policies, and prompt actions that propel India towards a future where women can confidently and securely thrive in the digital realm.

References

1. Adriane van der Wilk, (2021), Protecting women and girls from violence in the digital age, the relevance of

the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women, Council of Europe, pp. 1-71.
2. Cyber-crime investigation manual, Data security council of India, (www.dsci.in) pp. 1-137.
3. Halder, Debarati & K. Jaishankar (2015). Harassment via WhatsApp in Urban & Rural India. A Baseline Survey Report (2015).
4. S. Jenefa (2017) Social Media as a tool of violence against women. World Journal of Science and research, (ISSN: 2455-2208), 2(2), pp. 77-82.
5. Kovacs, Anja, Richa Kaul Padte and Shobha SV. (2013). "Don't Let it Stand!" An Exploratory Study of Women and Verbal Online Abuse in India. Internet Democracy Project. New Delhi, India. April 2013. http://Internetdemocracy.in/wp-content/uploads/2013/12/Internet-Democracy-Project-Women-and-Online-Abuse.pdf
6. Nilesh Beliriya K and Abhilasha (2020), Cyber crime against women in India: legal Challenges and solutions, Int. Jour of Law Management and Humanities, [ISSN 2581-5369], Vol.3, Issue5; pp.1012-1022.
7. MS Saumya Uma (2017), Outlawing cyber crimes against women in India, Bharati Law Review, April-June, 2017, pp 103-116.
8. Viswanath, Kalpana and Ashish Basu. (2015). "Safety in an innovative mobile app to collect data on women's safety in Indian cities. "Gender & Development, 2015. Vol.23, No.1, 45-60. Oxfam GB 2015. http://dx.doi.org/10.1080/13552074.2015.1013669
9. UN Women (2014) Technology and Violence Against Women Framework, www.empowerwomen.org/ict4d
10. https://www.mxmindia.com/media/rural-india-outperforms-urban-india-in-social-media-usage/
11. https://www.indiancybersquad.org/
12. https://www.geeksforgeeks.org/cyber-crime-against-women/
13. https://www.indiancybersquad.org/cyber-safety-tips

Abbreviations

AI	: Artificial Intelligence
CP	: Child Pornography
CSAM	: Child Sexual Abuse Material
GPS	: Globle positioning System
IPC	: Indian Penal Code
IP	: Internet Protocol
IT	: Information technology
NCCRP	: National Crime Reporting Portal
PC	: Personal Computer

Pros and Cons of using Social media

Pros of Social Media Usage	Cons of Social Media Usage
1. Connectivity and Networking: Social media enables women to connect with family, friends, and communities, fostering a sense of belonging.	1. Privacy Concerns: Increased online presence can lead to privacy issues, with personal information being vulnerable to misuse.
2. Information and Awareness: Access to information on health, education, and various resources empowers women with knowledge.	2. Cyberbullying: Women may face online harassment, cyberbullying, or trolling, impacting their mental health and well-being.
3. Empowerment and Expression: Social platforms provide a space for women to express their opinions, showcase talents, and advocate for social issues.	3. Unrealistic Beauty Standards: Exposure to curated content can contribute to unrealistic beauty standards, affecting self-esteem and body image.
4. Business and Entrepreneurship: Social media offers opportunities for women entrepreneurs to promote their businesses and reach a broader audience.	4. Time Management: Excessive usage may lead to time-wasting, affecting productivity and real-world relationships.
5. Support Communities: Women can find support networks, share experiences, and engage in discussions on social issues.	5. Spread of Misinformation: Social media can be a source of misinformation, impacting opinions and contributing to the spread of rumors.
6. Educational Resources: Access to educational content and online courses can contribute to skill development and learning.	6. Mental Health Impact: Constant comparison and social pressures can contribute to stress, anxiety, and a fear of missing out (FOMO).
7. Awareness of Social Causes: Women can use social platforms to raise awareness about social causes and participate in movements.	7. Digital Addiction: Excessive use can lead to addiction, affecting physical and mental health negatively.
8. Remote Work Opportunities: Social media serves as a platform for networking and job opportunities, especially in remote work scenarios.	8. Online Predators: There's a risk of encountering online predators, particularly for young women and teenagers.
9. Political Engagement: Women can engage in political discussions, express opinions, and participate in civic activities.	9. Platform Exploitation: Social media platforms may exploit user data for targeted advertising or other purposes.
10. Skill Building and Creativity: Platforms offer avenues for women to showcase creativity, skills, and hobbies.	10. Addiction Impact on Relationships: Excessive social media use can strain relationships due to distractions and lack of real-time communication.