

STRENGTHENING WOMEN OF GUJARAT IN THE DIGITAL AGE AGAINST CYBERCRIME TECHNIQUES IN SOCIAL MEDIA

Mr. NIRAJ H. GUPTA

Research Scholar

Discipline/Subject: Law

Dr. Sadananda Anantrao Karhale

Guide

Abstract

Cybercrimes on social media platforms pose an increasing threat to women as the digital landscape continues to change. This research examines the various obstacles that women experience in the digital sphere and suggests empowering tactics to successfully fight against cybercrimes. The research investigation explores the frequency of social media threats that specifically target women, such as cyberbullying, stalking, identity theft, and harassment. The study highlights the necessity of customized combat strategies, acknowledging the critical role that social media plays in women's life. The suggested tactics include community support networks, legislative frameworks, improved cyber security measures, and digital literacy campaigns. The subject matter seeks to support the development of a more secure and welcoming online community for women of Gujarat by providing them with information and tools.

Keywords: Social media, cybercrime, techniques, legal framework, and strengthening women's.

Introduction

The significant influence of social media of Gujarat has permeated everyday life in the ever-changing digital ecosystem. As more women embrace the opportunities and connections made possible by these platforms, they also have to deal with the increased threat of cybercrimes. This investigation aims to examine the complex obstacles that women face when traversing the digital landscape and, more importantly, to suggest comprehensive solutions for reducing cybercrimes that target

them. As we witness an unprecedented increase in online interactions, the vulnerabilities embedded in this digital space require a strategy strengthened by empowerment. In order to create a more safe and welcoming digital environment for women in Gujarat, this research will examine and promote strong tactics that make use of awareness, technological resilience, legal frameworks, and community support. This research aims to add to the ongoing discussion on strengthening the digital future for everyone by exploring the unique nuances of cyber dangers experienced by women and promoting empowerment.

The literature offers a thorough examination of the digital environment and how it interacts with harassment of women. Key conclusions and insights from numerous studies and papers are summarized in the review that follows.

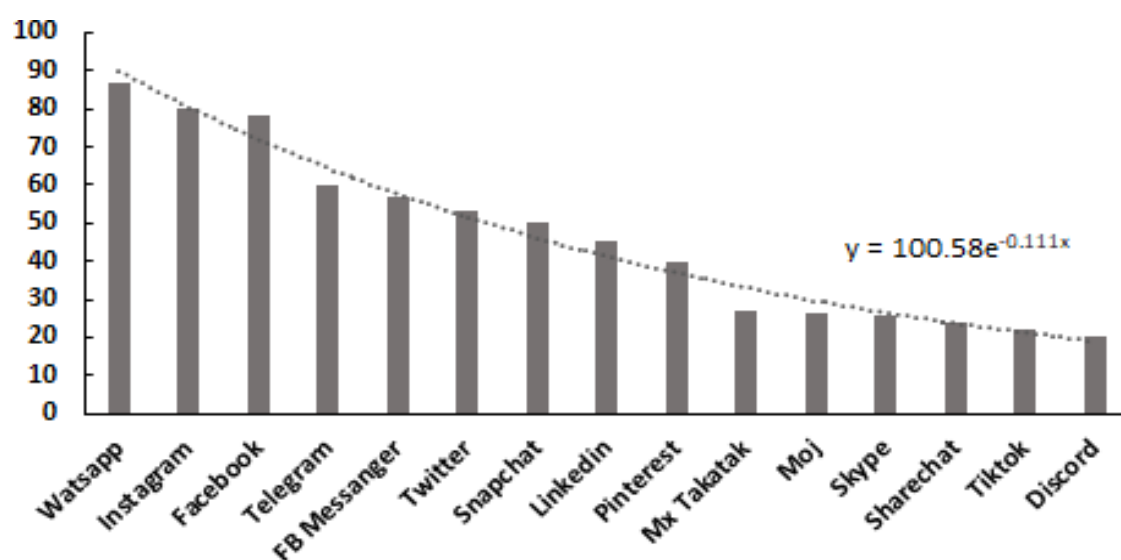
Adriane van der Wilk (2021) highlighted the importance of worldwide laws in tackling digital harassment against women, particularly the Budapest Framework Convention on Cybercrime and the Istanbul Convention. The article offers a legal framework for comprehending and addressing violence enabled by technology. The Cybercrime Investigation handbook provides useful information about investigating cybercrimes. It is an invaluable tool for comprehending the technical facets of cybercrimes, which is essential in the fight against digital harassment against women. A baseline survey on WhatsApp harassment in rural and urban India was presented by **Halder & Jaishankar (2015)**. In addition to providing a contextual understanding of the frequency and type of online violence against women, the report explores the subtleties of digital harassment.

Jenefa S. (2017) investigated the use of social media as a weapon of abuse against women. The study provides a complex understanding of the relationship between technology and gender-based violence by illuminating the different ways that social media platforms both contribute to and occasionally magnify discrimination against women. **Kovacs, Padte, and Shobha SV (2013)** looked into verbal abuse of Indian women over the internet. The study advances knowledge of the nature of gender-based violence in digital environments by investigating the dynamics of online abuse. The legal issues and suggested remedies for cybercrime against women in India were the only emphasis of **Beliriya N K and Abhilasha (2020)**. It offers a legal viewpoint on dealing with cyberviolence, revealing weaknesses and possible solutions in the legal system. **Saumya Uma (2017)** concentrated on making cybercrimes against

women in India illegal, providing a legal analysis and suggesting ways to improve protection. The study adds to the current debates over legislative strategies to stop cyber violence.

Table 1: India's most popular social media sites

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: Percentage of social media users across various channels

An inventive Smartphone app created to gather information on women's safety in Indian cities was examined by **Viswanath and Basu A. (2015)**. It provides insights into the role of technology in reducing violence against women and illuminates technological solutions aimed at improving women's safety. By integrating legal, technical, and sociological viewpoints, these studies significantly advance our knowledge of online violence against women. The literature emphasizes how urgent it is to handle this issue comprehensively, taking into account societal norms, technical advancements, and legal frameworks.

India is an important participant on the international scene thanks to its dynamic social media sector, which has seen significant growth, regulatory actions, and revolutionary changes. India has a very appealing but competitive online market because it is the most populated country in the world and has the second-highest number of internet users. A sizable social media user base spends an average of 2.6 hours a day on various platforms, despite the fact that only 43% of people have access to the internet.

Overview of Social Media

Digital apps or services that enable user-generated content production, sharing, and exchange as well as user networking and engagement are referred to as social media platforms. These platforms offer a virtual environment where people may interact, converse, and exchange text, photos, videos, and links, among other types of content. Social media platforms provide many advantages, but there are drawbacks as well, such as privacy concerns, online harassment, and the dissemination of false information. Users should utilize these sites appropriately and be aware of their online presence.

The utilization of Social Media

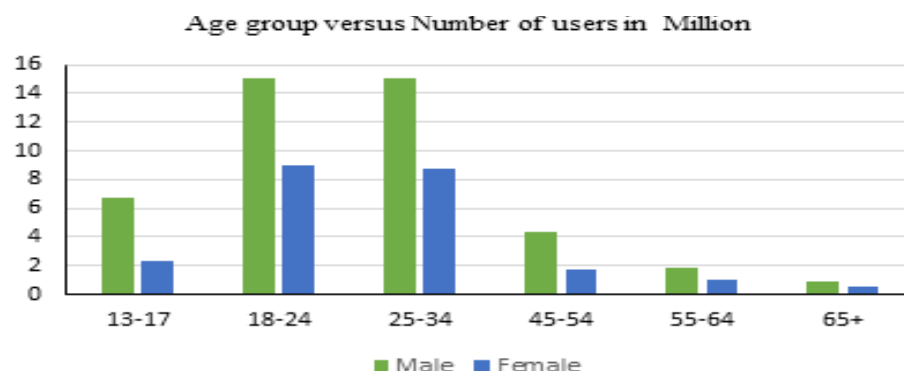
Social media systems are adaptable and can accommodate a wide range of user requirements. Real-time involvement is made possible via communication capabilities like instant messaging and comments. Effective digital networking is facilitated by networking, which enables connections based on common interests, affiliations, or

relationships. Depending on personal privacy settings, content sharing enables users to share updates, images, videos, and articles.

Social media, which provides news and trends, is an essential resource for knowledge discovery. By following pertinent accounts, users curate feeds to stay informed. Videos and memes are examples of entertaining content that offers recreational opportunities. Companies use social media to advertise goods, services, events, and engaging promotional activities. A sense of belonging is fostered by the formation of social media networks around particular subjects. Agencies use social media to share knowledge for educational reasons. They are ideal for activism since they offer a forum for spreading awareness and rallying support. Interactivity encourages participation in the online community by enabling users to offer input. In general, consumers are empowered for a variety of online experiences by social media's versatility.

In the course of the next decade, India is expected to overtake China as the biggest market for social media advertising spending. According to the most recent estimates, there are over 484.2 million Instagram users and 653.6 million Facebook members in India as of 2025.

On Facebook, there are roughly 72.99% male users and 27.01% female users. On Instagram, there are roughly 72.74% male users and 27.26% female users. With a projected compound annual growth rate of 55–60% during FY 2020–2025, social commerce in India is expected to grow from \$1.5–2 billion to \$16–20 billion. According to an Oxford University survey, 54% of Indians use social media to find "truthful" information, which is higher than the global average of 37% and the US average of 29%.



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

Figure 2: Utilization of Social Media by male female according to age group



Figure 3: Diagram showing the progression of cybercrime

Statistics on Cybercrime against Women in Gujarat

Cyber extortion, threats, cyber pornography, the distribution of explicit pornographic material, stalking, bullying, defamation, morphing, and the creation of false profiles are among the common cybercrimes that target women. In Appendix table indicates advantages and disadvantages of using social media.

Cybercrime incidences have increased by 20% overall as of 2023. However, according to the National Crime Record Bureau, the number of specific cybercrimes against women has increased more sharply, rising by 30%.

The statistics shows that 20.2% of total incidents reported in 2024 were classified as crimes against women. According to the state-by-state distribution, Karnataka had the most cases in last calendar year, followed by Maharashtra and Uttar Pradesh. Gujarat is on seventh position where cases of cyber crimes against women have been registered.

The operational diagram of cybercrime is shown in Figure 3. The availability of gadgets like smart phones, tablets, PCs, and smart TVs is crucial to the rise in cybercrime. Similarly, one of the factors contributing to the rise in cybercrime against women over the past ten years has been the accessibility of internet facilities for both urban and rural populations.

There are several reasons for the increase in cybercrime:

1. An increase in internet traffic.
2. Not enough consciousness.

3. The general public and law enforcement have limited technical knowledge.
4. Difficulties in investigating cybercrime cases.

Cybercrimes against Women: A Guide

- **Cyber-bullying and Digital Harassment:** Cyber-bullying and Digital harassment refer to the use of digital media to send someone frightening, hurtful, or threatening messages. It frequently involves the propagation of unfounded rumors, public humiliation, and continuous attacks. The anonymity of the internet allows perpetrators to repeatedly target victims. This can involve releasing humiliating material, making false profiles to mimic the victim, or making harsh remarks on social media. Digital harassment victims may suffer from anxiety, depression, emotional discomfort, and in severe situations, bodily injury. Relationships both personally and professionally may suffer as a result of reputational harm.
- **Digital Stalking:** Digital stalking is a constant search of an individual via social media, which is frequently characterized by keeping an eye on their digital activities, obtaining confidential data, and harboring unwelcome contact. Stalkers follow and harass their victims using a variety of internet platforms. Sending threatening messages, keeping an eye on social media accounts, and obtaining personal data to use against the victim are a few examples of this. Severe psychological discomfort, worry, and a persistent sense of privacy violation can result from online stalking. In order to prevent more harassment, victims may change how they behave online.
- **Economic Fraud:** This kind of crime is the use of dishonest methods to get economic data and carry out dishonest online actions. Phishing emails, phony websites, and malware are some of the strategies used by criminals to gain private financial data. The stolen information is subsequently utilized for identity theft, unlawful transactions, and bank account depletion. Significant losses in cash, unlawful activities, and difficulties recovering stolen money are all possible outcomes for victims. Reputational harm can also result from financial dishonesty.
- **Personal Information Theft:** Personal information theft is the unlawful use of someone's private data, such as social security numbers or financial data, to assume their identity. Phishing, data breaches, and social engineering are just a

few of the ways that criminals gain personal information. Information that has been stolen is then utilized for illegal activities or financial gain. Identity theft victims may experience serious financial losses, credit score harm, and legal issues. Identity restoration can be a difficult and drawn-out procedure.

- **Digital Grooming:** Developing a relationship with a youngster online, frequently with the goal of sexually abusing them, is known as digital grooming. To win a minor's trust, criminals employ gifts, boasting, and manipulative behavior. The intention is to participate in improper activities that could lead to sexual exploitation. For minors, online grooming can have serious repercussions, such as long-term psychological damage, emotional distress, and sexual exploitation. To avoid injury, early intervention is essential.
- **Revenge Porn:** Unauthorized sharing of private photos or films, usually by someone wishing retribution following a breakup, is known as revenge porn. Without the victim's permission, perpetrators distribute explicit content, frequently with the intention of damaging their reputation. This could be sharing private photos or videos via websites, social media, or other internet channels. Revenge porn victims may suffer from extreme emotional suffering, interpersonal relationship damage, and possible reputational loss. Depending on the jurisdiction, offenders may face different legal repercussions.
- **Hacking and social engineering:** Hacking and social engineering are dishonest methods used to fool people into disclosing private information, frequently via phony emails or websites. To deceive people into divulging private information, perpetrators fabricate phony websites, emails, or communications that look authentic. Social engineering manipulates people into disclosing private information by taking advantage of human psychology. Identity theft, financial fraud, and illegal access to personal data can result from phishing attempts. Passwords, credit card numbers, and other sensitive information may be unintentionally disclosed by victims.
- **Hate Speech and Sexism:** Using digital platforms to disseminate harmful, prejudiced, or sexist content that targets people or groups based on their gender is known as hate speech and sexism. Digital platforms are used by offenders to spread content that encourages acts of violence, or prejudice against people

because of their sex. Threats, damaging stereotypes, and sexist remarks are examples of this. Digital hate speech can cause harm in the real world and contribute to a hostile online environment. Victims may feel alone, afraid, and emotionally distressed.

- **Email spoofing:** In order to trick the receiver about the message's origin, emails with a falsified sender address are created. In order to make an email appear to be from a reliable source, perpetrators employ strategies to alter email headers and sender information. This can be used to disseminate malicious content or launch phishing campaigns. Phishing attacks, unauthorized access to private data, and the spread of malware can all result from email spoofing. People and businesses may become targets of fraud or have their cyber security compromised.
- **Taking advantage of others** Creating a false digital identity in order to trick people, usually for intimate connections or financial gain, is known as exploitation of others. False narratives, pictures, and facts are used by perpetrators to gain the confidence of the target. Once targets are trusted, they may take advantage of them financially or emotionally. sufferers frequently suffer from heartbreak, emotional suffering, and money losses. Realizing you've been duped might have long-lasting psychological repercussions.
- **Cyber stalking with GPS and whereabouts Services:** This type of cyber stalking entails tracking a victim's whereabouts in real time using GPS or other location services. Stalkers use technology to keep an eye on their victims' whereabouts. GPS monitoring and location services on smart phones and other devices can provide this information. Location-based cyber stalking victims may lose their privacy, worry about their safety, and maybe suffer bodily damage if the stalker intensifies their actions.

Factors Controlling the Rise of Cybercrimes against Women in Gujarat

There are a number of contributing causes to the rise in cybercrimes against women in Gujarat. These elements create a difficult climate where women are more vulnerable to many types of cybercrimes and threats. Among the crucial elements are:

- Digital Women: Women are especially susceptible to digital victimization due to the current digital gender divide, which limits their access to digital technologies and awareness.
- Social media privacy: privacy makes it possible to create false profiles with the intention of misleading or harassing people. Cybercriminals can simply construct false identities or fake others in order to commit cybercrimes against women. Because of privacy, people can falsely accuse women without worrying about the consequences. Women's privacy may be violated by anonymous people who obtain and distribute personal information without authorization.
- Unlicensed Social Media Activity: Before registration, social media platforms provide guidance and warnings against cybercrime. In order to stop any illegal activity against users, they also provide a number of security elements. However, people occasionally fail to employ these security mechanisms, whether intentionally or unintentionally. One of the main reasons why women are targeted by cybercrime is this.
- Lack of information: Women are more vulnerable since they are unaware of the possible dangers and safety precautions in the digital world.
- Lack of Judicial Regulation: The administration of justice is hampered by loopholes and inadequacies in its legal structure pertaining to cybercrimes against women as well as sluggish judicial procedures.
- Criminal's territorial position: In the world of cyberspace, a criminal may come from any nation, state, religion, group, etc., which is difficult to track down digitally. The current global system makes it practically hard to punish such criminals through international laws and courts, which is why cybercrime against women is on the rise simply due to the offenders' territorial position.
- Social Media Impersonation and phony Profiles: Women's reputations are frequently harmed by the deliberate creation of phony profiles and impersonation on social media sites.
- Privacy Problems: Women are particularly vulnerable to data breaches and digital privacy violations, making it difficult to preserve personal information and privacy in the digital age.
- Technological improvements: Although there are many advantages to technological improvements, they have also given cybercriminals more advanced tools and techniques to target women digitally.

Addressing Cybercrime against Gujarat's Women Stopping Cybercrime against Gujarat's Women

The internet has completely changed the way individuals connect with each other, interact with friends, share updates, play games, and shop online, making it an essential part of our everyday life. It significantly affects many facets of our daily lives.

Humans are digitally connected to millions of people globally in the huge span of cyberspace. Cybercrimes, especially those that target women and children, such as cyber-stalking, cyber-bullying, cyber-harassment, child pornography, and the spread of improper content, are increasing along with the usage of online. Adopting specific cyber safety measures that help make our online interactions safe and productive is essential to ensuring a secure digital environment. There are two components to the cybercrime prevention strategy for women. One is about the involvement of parents in crimes against girls, and the other is about security measures for women in the teen to adult age range.

Encouraging Parents' Cyber Consciousness and Hygiene

Start having candid discussions with the women's about possible digital risks like stalking, bullying, and grooming. Keep track on their digital activities and set explicit rules for using the internet and playing online games.

- **Keep an eye out for behavioral changes:** Women may be engaging in cyber bullying if you notice that they are spending more time online and that they are becoming defensive or secretive about what they are doing. Encourage them to take part in other activities and have frank conversations with them. Protect women's against the dishonest practice of "cyber grooming," in which an individual uses social media or chat platforms to build an emotional bond with a woman in order to potentially exploit them sexually. In an attempt to make more friends on social media, women's may inadvertently delete their privacy settings. Family should help them to set up strong privacy settings and teach them how to use social media responsibly.

- **Be cautious while opening attachments and links:** Refrain from opening files or links that you receive over social media, text messages, or emails from unidentified sources. Taking this precaution is essential to protecting the device from possible malware attacks.
- **Cover personal cameras:** When not in use, especially on laptops, cover your webcams to protect confidentiality. This safeguard aids in preventing any unauthorized use of hacked cameras to observe, record, or exploit everyday activities.
- **Put family control measures into place:** On their devices, install control software or antivirus software with control features. Examine their social media networks' privacy settings on a regular basis.
- **Give upgrades to the software top priority:** Update the software and operating system that individuals use to fix vulnerabilities that hackers might target. To reduce security concerns, stay away from downloading apps, games, software, or music from unreliable sites.
- **Secure browser settings:** To guard against malware and hackers, install secure browsing tools and choose the most recent browser versions. Update these tools frequently to guarantee ongoing defense against possible dangers.

Encouraging Women (Teens and Young Adults) to Practice Cyber Awareness and Hygiene

Protect Oneself and Your Digital Identity at the Same Time

If one has not set up their social media accounts properly, people may be able to view, download, and use your images and videos without your knowledge. To share personal information, images, and videos only with people you can trust, make sure you select the appropriate privacy settings and content sharing filters on social media platforms. When approving friend requests on social media from unknown individuals proceed with caution. Discover how to block people that are uncomfortable. Recognize how to remove someone from the list of pals. After using social media, always log out. For further security set up password protection on your phone. Notify the social media service provider right away if you see someone creating a phony account so they can block it.

Pay Close Attention to what's happening during Calls and Video Chats

The person on the other end may record video chats on social media platforms. There are instances where purportedly private video conversations have been captured and shared on websites and social media groups. Be cautious when you accept chat invitations from strangers.

Reporting Dangerous Information on Smart phones

Steer clear of taking private, critical pictures and movies using your smart phone. Images or videos taken with a smart phone connected to the cloud may be automatically saved there because the majority of cell phones are connected to the internet and cloud storage. Users may be able to retrieve the content from the cloud account or any other device or PC connected to the cloud using the same account, even if they remove it from their phones. If someone has used a smart phone to capture such pictures, take the situation seriously and make sure the content is removed from their smart phone, the cloud, and any other connected devices that use the same account.

Defend One from Cyber stalking: Regardless a person's obvious signs of aloofness, cyber stalkers persistently make advances on them. They stalk using the internet, email, social media, or any other type of digital communication. The following actions must be performed to prevent stalking.

- Turn off tracking functions on mobile devices, social media platforms, etc.
- Don't give out a cell phone number, email address, or photos to strangers.
- If you believe you are a victim of cyber stalking, speak with your friends and family

Table 2: Software for Retrieving Information from Digital Gadgets

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

Watch Out for False Social Media Platforms: Not all of those profiles are authentic, and not all of the material on them is accurate. When answering friend requests from strangers, exercise caution.

Use Caution When Browsing Sensitively

Usually a personalized device or a reliable network should be used to view banking or shopping websites or apps. For sensitive browsing, stay away from utilizing a friend's phone, a public computer, a cyber cafe, or free Wi-Fi because information can be taken or stolen.

When giving personal computers and mobile devices to be serviced, repaired, or sold, use caution

Mobile devices and personal computers include sensitive details which must be deleted before being sent for maintenance, repair, or sale. It is possible to retrieve erased data from the interactions devices. Women should avoid selling their digital gadgets without properly configuring the system. Table 2 lists the devices that can be used to retrieve data as well as the data recovery software that is available on the open market.

Information can be recovered from devices like smart phones, tablets, computer hard drives, and more using data recovery software. Information can be used by those involved in criminal activity to carry out the aforementioned cybercrimes if the equipment are sold or refurbished. Before reselling such devices, it is advised to fully format them, and they must be secured with strong passwords while they are being repaired.

Safeguard the interactions between gadgets: Use a password, PIN, pattern, or biometric information to keep others from obtaining these devices. Install apps on laptops, smart phones, and other devices only from reliable sources, such as the Play Store, App Store, or official corporate websites.

- Subsequently come across any information pertaining to child/women pornography, child/women sexual abuse material, or sexually explicit material, one should report it to the relevant social media website. If someone who knows who shares women pornography, women sexual abuse material, or sexually explicit material with others, it is one's responsibility as a responsible citizen to let them know that it is illegal to publish, collect, or distribute such content.
- The National Cyber Crime Reporting Portal is another place you can report it. (www.cybercrime.gov.in)

Ipcc for Cybercrime against Women

International rules governing the legal implications of digital platforms and networked computer technologies bind all users of the internet. These laws protect people from cybercrimes and provide victims with justice and security. Section 354 of the Indian Penal Code (IPC, 1860), which was added as a result of the 2013 Criminal Amendment Act, lists particular crimes that are subject to severe imprisonment and fines.

Section 292: Originally designed to deal with the sale of pornographic materials, this section has expanded to handle a variety of cybercrimes in the current digital era. This clause also governs the publication or electronic transmission of pornographic content or sexually explicit acts or exploits of minors. Such activities are punishable by up to two years in prison and a fine of Rs. 2000. Any of the aforementioned offenses have a maximum sentence of five years in prison and a fine of up to Rs. 5,000 for repeat (second-time) offenders.

Section 354A: Sexual harassment is covered in Section 354A, which makes it illegal to show pornography against a woman's consent, demand or beg for sexual favors, or make sexual remarks. Offenders may be fined, imprisoned for a maximum of three years, or both. One year in jail, a fine, or both may be imposed in the first two situations.

Section 354C: Acquiring a picture of a lady performing a private act and/or distributing it without her permission is considered harassment under Section 354C. The situation must be such that the lady would typically expect not to be seen in order for an act to be classified as "voyeurism." If found guilty, the maximum term for a first conviction is three years in jail; for consecutive convictions, the maximum sentence is seven years

Section 354D: The latest amendment of Section 354D deals with the ban of stalking, including internet stalking. Observing a woman's online behavior, internet usage, or electronic communication, or pursuing or visiting her regardless her apparent disinterest, are all considered forms of stalking. Stalking crimes carry a maximum sentence of three years in prison and a fine; further convictions may result in a maximum sentence of five years in prison and supplementary penalties.

Section 379: Along with to the penalty, the maximum sentence for theft under this provision is three years. Because many cybercrimes include stolen computers, stolen data, or hijacked electronic devices, the IPC Section is relevant.

Information technology (IT) ACT

The IT Act 2000 lists a variety of criminal acts, including tampering with computer source documents. These transgressions are described in depth in the following sections:

Table 3: A section of the IT Act that addresses offenses

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 IT Act 2000's paragraph regarding the kind of offense and the severity of the penalty is explained below modifications brought about by the 2008 IT Amendment Act.

Section 66B: Punishment for dishonestly obtaining stolen computers or communication devices is outlined in Section 66B.

Section 66C: Theft of identities is criminalized under Section 66C of the IT Act, especially in cases of cyber hacking. This section provides that anyone who falsely or dishonestly uses another person's electronic signature, pass-word, or unique identification characteristics may face maximum penalties of three years in prison and an administrative fee of up to Rs. 1 lakh.

Section 66D: It contains the penalty for cheating by impersonation.

Section 66E: It deals with violations of privacy

Section 67: It is forbidden to publish, transmit, or distribute pornographic material. A primary offense has a potential sentence of three years in jail or a financial penalty; a second conviction carries a possible sentence of five years in prison and an additional financial penalty.

Section 67A: It is a criminal to publish, transmit, or participate in the transfer of sexually explicit content. The maximum punishment for a primary offense is five years in jail and a fine; subsequent convictions carry a maximum sentence of seven years in prison and extra financial penalties.

Section 67B: Distribution of women's sexually explicit material is now punishable under Section 67B.

Cybercrime Website of the Government of India

The National Cyber Crime Reporting Portal (www.cybercrime.gov.in) was created by the government to make it easier to report different cybercrimes, especially those that target women and children. Furthermore, a module of the Citizen Financial Cyber Fraud Reporting and Management System has been included, facilitating the timely reporting of financial frauds and stopping criminals from transferring money illegally.

The Cyber Community's Function in Reducing the Issue Rules and Regulations for Social Media Websites and Apps

It is essential to have strong security features that successfully protect user data in order to improve the security of websites and applications. One of the most important

steps in protecting user data is to utilize sophisticated encryption techniques, which guarantee that private information cannot be accessed by unauthorized parties. By adding an extra layer of security, encryption makes it far more difficult for potential attackers to jeopardize user data confidentially. It is also impossible to overestimate the significance of updating security protocols on a frequent basis. Organizations can strengthen their defenses against new cyber threats by being watchful and proactive in updating security measures. In addition to fixing current issues, this proactive strategy puts websites and apps in a position to handle any new problems in the constantly changing field of cyber security. To put it simply, the combination of strong security features, sophisticated encryption, and frequent updates creates an all-encompassing approach to strengthen the security posture of websites and applications, promoting user confidence and protecting priceless digital assets.

Integrating Security Features into Websites and Applications

Maintaining the security of websites and applications is essential to protecting user data. Organizations can build a stronger defense against possible attacks by incorporating strong security measures. Sensitive data is further secured by advanced encryption techniques, which are essential in preventing unwanted access to user data. To keep abreast of new cyber threats, security systems must be updated on a regular basis.

Table-4 Social media platforms and safety elements that go with them

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

In addition to fixing current issues, this preventive approach equips the digital infrastructure to handle new challenges in the ever-changing cyber security landscape. The security elements that are available for each social media program are listed in Table 4. The degree to which a user is proficient determines whether or not they employ the security mechanisms that are accessible to them. The issue of cybercrime can be considerably reduced by raising awareness of the security features that are available for specific applications. When combined, these steps provide a thorough approach to improve the entire security posture of websites and applications, giving users peace of mind and confidence regarding the security of their important data.

The Dark Web and Hackers: A Challenge

Fighting cybercrime against women on social media, especially the problems caused by hackers and the dark web, calls for a multipronged strategy; Strong cyber security solutions designed to block dark web activity, such as intrusion detection systems, firewalls, and advanced encryption, must be developed and put into place. In order to create a preventive information-sharing system for quick reactions to hacking efforts, cooperation between cyber-security specialists, governmental organizations, and tech firms must be improved. Finding resources for cutting-edge technology, like machine learning and artificial intelligence, is essential to tracking and eliminating threats coming from the dark web. Awareness raising efforts are crucial for educating users—particularly women—about the dangers of hacking and the dark web, encouraging safe online conduct, and offering tools for recognizing and reporting unusual behaviors. It is crucial to strengthen laws pertaining to cybercrimes against women, with an emphasis on dark web activity, and to provide criminal justice agencies with the resources and training they need for investigation and enforcement. In order to tackle cross-border cybercrimes, multilateral collaboration is essential. This includes collaborations with multilateral cybersecurity groups and regulation authorities to share intelligence and coordinate actions against multinational criminals. Strengthening the defense against cybercrimes on the dark web and reducing the risks faced by women in the social media landscape can also be achieved by supporting ethical hacking initiatives, putting in place ongoing platform monitoring, and developing a strong incident response plan.

Case Studies

Case Study on Cyber Stalking

In the July 2015 case of Yogesh Prabhu v. State of Maharashtra, Additional Chief Metropolitan Magistrate M.R. Natu rendered the first conviction in a cyber stalking case against a woman in Maharashtra. The woman first had an online conversation with Yogesh Prabhu in 2009. She declined his proposal of marriage. She stopped answering his texts after that since she thought his actions were odd. She took him off her list of pals as well. Prabhu, however, persisted in following her online and monitoring her profile and locations. A few months later, she started receiving emails with explicit photos and videos from an unidentified email address.

When the pornographic emails continued, she filed a police report, and the Cyber Crime probe Cell took over the probe. At first, she chose to ignore them. The computer's Internet Protocol (IP) address was linked to a Vashi company where Yogesh Prabhu was employed. The trial started in September 2009 after the cyber cell submitted a 200-page charge sheet. The Public Prosecutor questioned eight witnesses during the trial, including the irate woman, Prabhu's coworkers, cyber specialists, and police officers. Prabhu was found guilty by the magistrate's court under S. 509 IPC (words, gestures, or acts intended to offend a woman's modesty) and S. 66E of the Information Technology Act, 2008 (penalty for infringement of privacy). This was due to the fact that S. 354D of the IPC, which addresses cyberstalking, was passed in 2013 and could not be applied retroactively to a crime that was committed in 2009.

Cyber Pornography

In Suhas Katti v. State of Tamil Nadu, a Chennai court rendered an initial verdict for cyberpornography in India in 2004. After she rejected the proposal to get married, the divorced woman reported to the police about a man who was sending her offensive, slanderous, and obnoxious comments in a Yahoo messaging group. In the woman's identity, the accused created a fictitious email account and transmitted correspondence from that account. People who thought the victim was looking for sex work also called her. The police case was filed in February 2004, and the Chennai Cyber Crime Cell obtained a conviction just seven months after the First Information Report was filed. Katti was sentenced to two years of rigorous imprisonment and a

fine of Rs. 500 under S. 469 IPC (forgery for the purpose of harming reputation), one year of simple imprisonment and a fine of Rs. 500 under S. 509 IPC (words, gestures, or acts intended to insult the modesty of a woman), and two years of rigorous imprisonment and a fine of Rs. 4000 under S. 67 of the IT Act 2000 (punishment for publishing or transmitting obscene material in electronic form).

Forwarding Private Photographs and Videos

The Delhi Public School MMS incident of 2004, that comprises the production of a pornographic MMS of two Delhi Public School students engaging in sexual activity, its illicit circulation, and the sale of it on the website eBay India (formerly known as Baze.com), is one of the most well-known instances of the practice. Since the IPC had not made such conduct illegal, the website's CEO was subsequently charged under several sections of the Information Technology Act. These regulations will be triggered by the online distribution of video footage of rape and gang rape events. It is crucial to remember that there can be circumstances in which the victim gives permission for such an image to be taken but not for it to be shared with other parties. Under this clause, it will be illegal to distribute the image to such individuals. For instance, women have reported sending pictures of themselves naked or in skimpy clothing to their intimate relationships over Instagram or Whatsapp at the partner's request. In other cases, physical intimacy with the spouse has been documented with the woman's permission. The boyfriend has then tried to exact revenge or blackmail the woman by sharing these pictures and videos when the relationship deteriorates. These legal laws would apply to such acts. Additionally, they can be charged with criminal breach of trust (S. 406 IPC), which is defined as dishonestly misappropriating or converting property entrusted to one's own use.

Morphing

When an unauthorized user using a false identity takes the victim's photos and then uploads or reloads them after making changes, this is known as morphing. Women's photos are frequently copied from websites by fictitious users, who then modify them and republish or upload them on other websites. Morphing frequently entails using picture-editing software to affix an image of the targeted woman's face to that of another person's nude or skimpily dressed body. These altered pictures are meant to

damage the victim woman's reputation and character. In India, there is a reported increase in cybercrimes against women using altered photos. Celebrities are frequently the easy targets of this crime, but a regular woman can also be the target of a man who wants to exact revenge on her for turning down his proposal of an intimate relationship, blackmail her, harass her in other ways, or damage her reputation among her friends and family for perceived or actual harm she has caused to the abuser.

Such an act could result in offenses under S.66 of the IT Act (which lists several computer-related offenses) and S.43 (which covers acts of illegally transferring, replicating, gathering, eliminating, and changing data). Furthermore, the offender may be charged under a number of IPC laws, including S. 354A for sexual harassment, S. 290 for public annoyance, S. 292A for obscenity, and S. 501 for defamation.

Posting Horrible, Insulting, or Pornographic Messages

Such offenses include sexual harassment (S. 354A IPC), insulting another person (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 a woman's modesty (S. 509 IPC). S. 354 and S. 509 IPC offenses center on public morals, decency, and women's modesty and are based on colonial and patriarchal ideas related to sexual assault of women. The potential difficulty of judicially defining "modesty" and evaluating whether the victim's "modesty" is being violated is introduced by the implementation of these regulations. However, these rules are useful in tackling cybercrimes against women that are not well defined in the IT Act and the IPC. Particularly relevant is criminal defamation (S. 499 IPC), which involves damaging someone's reputation by words or outward manifestations. When women are subjected to sexist abuse or are falsely accused of being sex workers, this clause may be used to damage their reputation in online forums or groups.

Digital Threats, Assault, Blackmail, Bullying, and Trolling

In *Saddam Hussain v. State of M.P.*, the accused violated the victim's modesty by filming it on his phone and using it as leverage. A charge of criminal conspiracy was filed under S. 66A of the IT Act (which was later declared illegal in *Shreya Singhal v. Union of India*), S. 507 IPC (criminal intimidation by anonymous speech), and S.

354D IPC (stalking). The Madhya Pradesh High Court received a plea for quashing based on an agreement reached between the accused and the woman. Because the offenses were against humanity as a whole and a personal agreement between the parties would not influence the case from continuing, the High Court declined to halt the proceedings. This case shows that courts view cyberbullying and cyberstalking as extremely severe crimes.

Email fraud and fraudulent activity

Representing oneself as someone one is not is known as fraud. Because people can remain anonymous online, it is easy to impersonate women. For instance, in a documented instance in 2001, Manish Kathuria pretended to be a married woman named Ritu Kohli in an online chat room, using foul language, sharing her place of residence phone number, and accepting calls. She began to get a lot of calls at strange times. Due to a lack of relevant legal requirements, he was detained by the Delhi police and charged with "outrage of modesty" (S. 354 IPC) and S. 509, which had nothing to do with the cybercrimes he performed. The investigation was made little further, and the irate woman reportedly left India. Email fraud and fake news may be prosecuted under S. 415 IPC for cheating and S. 416 IPC for cheating by personation. Endeavoring to be someone else or portraying oneself as someone he is not is known as "cheating by personation." According to the law, cheating by personation is illegal regardless of whether the person being personated is a real or imagined person. Additionally, cheating by personation through the use of a computer resource or communication device is punishable under S. 66D of the IT Act. According to the IT Act, it is a crime that carries a maximum sentence of three years in prison and a fine of Rupees one lakh.

Discussion

The growing incidence of cybercrime against women emphasizes how important it is to have strong legal frameworks. The complexity of gender-specific cyber threats is often not adequately addressed by current legislation. Because they disproportionately affect women, cybercrimes—such as online harassment, stalking, and revenge porn—need special attention. For these crimes to be adequately protected, justice must be served, and potential offenders must be discouraged. Furthermore, in order to

effectively combat the constantly shifting panorama of online crimes against women, legislative measures must adapt to new cyber threats.

Even with regulations in place, practical difficulties make it difficult to effectively address cybercrimes against women. One major obstacle is the judiciary's and law enforcement organizations' lack of knowledge about the complexities of cybercrimes. The investigation and prosecution procedures are made more difficult by a lack of technical expertise. The intricacy is increased by the underreporting of incidences because of social stigma and fear of reprisals. In order to overcome these obstacles, law enforcement must receive thorough training, reporting procedures must be expedited, and victimization must be de-stigmatized in order to create a more encouraging atmosphere for reporting cybercrimes.

Fighting cybercrime against women becomes more difficult as artificial intelligence (AI) develops. Cyber threats can be automated and amplified by AI-driven systems, making them more complex and difficult to identify. For example, deep fakes are a developing problem since they make it possible to create realistic-looking but fake content, including pornographic stuff. Furthermore, gender-based prejudice may be sustained by biased algorithms, which could affect the seriousness of cybercrimes. In order to address these issues, a proactive.

Conclusion

The report emphasizes the need for all-encompassing tactics to combat cybercrimes that target women on social media. It emphasizes the following crucial elements:

- **Awareness and Digital Literacy:** In order to improve women's understanding of digital hazards, awareness and digital literacy activities are necessary.
- **Digital Protection:** Promoting increased cyber security measures to protect women from the constantly changing array of digital threats.
- **Judicial Procedures:** Encouraging legislators to modify laws to reflect the ever-changing digital landscape and recognizing the significance of gender-specific legal frameworks to combat cybercrimes.
- **Social Assistance:** Emphasizing the critical role which neighborhood support plays in creating a safe online and offline environment for women.

The suggested all-encompassing strategy incorporates social resilience, digital technology, legal protections, and awareness. By putting these tactics into practice, stakeholders can make a substantial contribution to the development of a safe and inclusive digital environment that enables women to profit from social media without jeopardizing their safety. In order to move Gujarat closer to a tomorrow where women can safely and securely prosper in the digital sphere, the research hopes to spark conversations, change laws, and inspire action.

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.dsai.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>

Advantages and Disadvantages of Using Social Media

Advantages of Using Social Media	Disadvantages of Using Social Media
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. Cyber bullying: Women may face online harassment, cyber bullying, 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.