NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Special Issue – 1, 2024
E – ISSN – 2583-7559

Legal Framework and AI Strategies in Addressing Cybercrime Against Women in India: Role of intermediaries in the detection of cybercrime against women

Narendra Singh Kushwaha
Research Scholar
Unitedworld School of Law
Karnavati University
Gandhinagar, Gujarat

Dr Pranay Prakash
Assistant Professor
Unitedworld School of Law
Karnavati University
Gandhinagar, Gujarat

***Abstract*—** Cybercrimes are said to be on the rise as a result of the internet's growing reach, the quick spread of mobile information, the growing use of social media, and the increasing integration of the online world into our daily lives. Cybercrime can be broadly defined as any activity that involves the use of computers and the internet to obtain personal information from individuals, either directly or indirectly, and then posting that information online against the law or without the individual's knowledge or consent in order to harm the individual's reputation or cause them physical or emotional distress. The frequency of recorded cybercrimes has sharply increased in tandem with technological advancement. Growing dependence on the Internet is correlated with an increase in cybercrimes targeting women. The main causes of this are that more than 50% of internet users have insufficient training and education, are unaware of technological advancements, and do not understand how online platforms function. For this reason, stopping cybercrime has become the top concern for law enforcement authorities around the world dedicated to protecting women and children who are harassed and mistreated for voyeuristic reasons. Targeting women through impersonation, cyberpornography, cyberstalking, etc. is widespread. India is one of the few countries that has enacted the IT Act 2000 to combat cybercrime and protect women from being exploited by hazardous predators. However, issues impacting women continue to skyrocket, and the act fails to address some of the most serious risks to women's security.

***Keywords*—** *Cybercrime, Online platforms, AI, Cybersecurity laws, Women.*

1. INTRODUCTION-

1.1 BACKGROUND INFORMATION ON THE RISE OF CYBERCRIMES AGAINST WOMEN IN INDIA

Cybercrimes against women in the digital era are concerningly on the rise in India. This increase is a direct result of the nation's increasing internet penetration, which has many advantages but has also made users—particularly women—more vulnerable to various forms of cybercrime. These crimes include identity theft, cyberstalking, cyberbullying, and online harassment.

These types of crimes have significantly increased, according to the "National Crime Records Bureau (NCRB) of India". 2018 saw an 18.4% rise in cybercrimes in 2021, with a significant percentage of the offenses aimed at women. More specifically, 10,730 (or roughly 20.2%) of the 52,974 occurrences that were recorded in 2021 were found to be crimes against women. The most often reported crime categories

are cyberstalking, bullying, defamation, morphing, making up profiles, posting or publishing explicit sexual content, cyber blackmail, threats, and cyberpornography.[1] Additionally, varied degrees of these crimes have been reported from other Indian states. For instance, the NCRB reports that Odisha saw the greatest number of these instances in 2022. The state recorded 542 instances of cybercrime against women that year; 269 of those cases involved the publication or transmission of sexually explicit content, while 273 incidents were classified as other cybercrimes, such as morphing, blackmailing, defamation, and creating false profiles.[2]

1.2. The significance of addressing cybercrimes against women

Because of several crucial factors, addressing cybercrimes against women is crucial. First and foremost, victims of these crimes frequently experience severe psychological, emotional, and sometimes bodily suffering as a result of their actions. Their effects also go beyond the digital sphere. Anxiety, despair, and a feeling of vulnerability are among the mental health and general well-being issues that women who are victims of cybercrimes may face.[3] Further, the frequency of cybercrimes against women can reinforce gender disparities by putting more obstacles in the way of women's full involvement in society and the digital economy. Widening the digital divide even more, threats against women such as cyberstalking and harassment can deter them from participating in online activities.[4] Moreover, these offenses frequently remain unreported because of a variety of reasons, including stigma, ignorance, and apprehension bout not being given proper attention. Effective legislative and policy solutions are hampered by this underreporting, which precludes a thorough grasp of the scope of the issue.[5] Legal changes, technology advancements, and public awareness efforts are some of the many strategies needed to combat cybercrimes that specifically target women. Aiming to particularly address and punish such cybercrimes, legal measures should be implemented. The creation of instruments and systems that improve online safety can be one technological approach. Raising women's awareness of their rights and the resources at their disposal requires advocacy initiatives.[6]

2. Understanding Cybercrime

Cybercrimes are defined as *"offenses that are committed against individuals or groups of individuals with a criminal motive to direct or indirectly cause physical or mental harm, or loss, to the victim, or to intentionally harm the victim's reputation using modern telecommunication networks such as chat rooms, emails, notice boards and groups, and mobile phones"*.[7]
Cybercrime includes computer and internet usage. By revealing or publishing someone else's private or sensitive information online, it violates their right to privacy and may result in reputational damage, physical or psychological harm, or both. Women are usually the victims of these crimes because they have less expertise and information about the internet, which makes them easy targets for technological fads.

2.1. Cybercrime victims

During the epidemic, women and children were the most vulnerable segments of society, making

them easy targets for cybercriminals. In contrast, men and adults fell prey to multiple cybercrime schemes. During the epidemic, women were particularly vulnerable to these crimes if they were housewives or used social media. Data from the National Commission for Women in 2021 indicates that the frequency of cybercrime incidents against women declines during a lockdown. Cybercrimes against women surged sharply in March and persisted thereafter, especially when India was severely impacted by the second wave of COVID-19 and nearly the whole nation was placed under harsh lockdown measures in April and May of 2021. Eventually, the number of cyberattacks also began to decline as the second pandemic wave subsided and the lockdown limitations were lifted in June. This situation persisted until the lockdown limitations were removed in July. The number of female victims of cybercrime grew dramatically during the epidemic and shutdown, compared to previous years when this number was quite low.

2.2. Women as a victim of cybercrime

Cybercrime against women is defined as *"crimes against women committed with the intent to cause the victim intentional psychological and physical harm, through the use of contemporary telecommunication networks like the internet and mobile phones"* Debarati Halder and K. Jaishankar go on to define cybercrime from a gender perspective.

Individuals were obliged to use the internet for social, work, play, and educational purposes during the pandemic and lockdown. Working women began working from home with the help of laptops, smartphones, and the internet. Women who are currently enrolled in school are forced to utilise the internet for additional academic purposes, such as online homework.

Around this same period, there was a noticeable rise in the rate of cybercrime against women because most women were using social media and one or more online platforms for leisure, work, and education. Since the victim could not be physically harmed because the entire nation was under lockdown, criminals began abusing them mentally and emotionally.

The following cybercrimes most often affect women:

- *Sextortion:* During the pandemic, the most common cybercrime against women was sextortion. Blackmailing their victims with altered or private photos, the perpetrators began requesting money or sexual favours in exchange. To show their frustration with the epidemic, the perpetrators intimidated women and demanded letters or sexual video conferences from them. They also felt emboldened to threaten victims with their manipulated photographs in an attempt to extract money from them because they were penniless.
- *Phishing* is a technique whereby phoney emails with a link to a particular webpage are sent to trick the recipient into divulging personal information, such as passwords and contact details, or infecting the recipient's device with malicious viruses at the moment the link is clicked to take advantage of the lockdown. It looks like these emails and texts are real. Using the victim's bank account and other personal information, the attackers then execute dubious transactions from the victim's bank account to their own.
- *Pornography:* During the pandemic, criminals attacked women online with sexual intent, modifying their photos to be used in explicit content.

- *Cyberstalking:* This type of harassment encompassed various actions, such as reaching out to the victim through social media platforms or phone calls even though it was evident that she was uninterested, leaving threatening messages on her page, and persistently pestering her with emails and phone calls.
- *Cyber hacking:* Amidst the pandemic, individuals began perusing online news sources. More fake news and information is available now than in the past. The women became the targets of cyber hacking after they clicked on fraudulent URLs. All of their personal information was downloaded to their phones by spyware, which also activated the camera and microphone and captured their private images and videos. Then, criminals commit extortion and other crimes using these images and bits of information.
- *Cyberbullying* is the act of sending abusive, deceptive, and fraudulent messages about a victim on social media and requesting payment to have them taken down, sometimes with threats of rape and murder. On the victim's posts, it also entails making offensive remarks. Digital and communication technologies that are used for bullying and harassment include computers, smartphones, and laptops.
- When it comes to *cybersex trafficking*, the victim and the perpetrator do not interact physically as they would in traditional sex trafficking. Intimate or sexual behaviours carried out by the victim are broadcast, recorded, or photographed by a dealer from a central location. This is known as cybersex trafficking, and the content is subsequently sold online to clients and sexual predators[8].

3. Legal Frameworks in India

3.1. Detailed analysis of existing laws

The Internet has two distinct qualities. First of all, cybercrime is not limited to any one location, and it may be perpetrated by someone from anywhere in the world. Its ability to offer users anonymity, which has advantages and disadvantages of its own, is its second distinctive trait. Anonymity is a blessing for those who use it to voice their opinions to the public, but it is a curse for those who commit crimes using it as cover. As a result, these characteristics make it difficult to both prevent crime and execute the law. Cybercrime against women is not now covered by any specific laws. The majority of women are unaware of other laws that may be applicable in this particular situation. Women are unaware of their rights or even that they exist. Cybercrime is punishable by a number of statutes, rules, and laws. However, the most bulk of legislation are contained in the "Information Technology Act (IT Act) of 2000 and the Indian Penal Code (IPC), 1860".The Indian Penal Code, often known as the General Criminal Code, lists crimes and their associated punishments. The Indian Penal Code, which covers laws and punishments relating to the physical world, is now applicable to cybercriminals due to legislative modifications and careful interpretations. The IT Act, on the other hand, is a unique piece of legislation that addresses offenses involving the use of technology. The 2008 IT Amendment Act was passed, encompassing several cybercrimes. Regarding cybercrime against women, the IT Act and IPC complement one another. The table below was extracted from an IT for Change

discussion paper. It displays the laws that can be brought against an online criminal who violates women. then an analysis of the laws' shortcomings is conducted.

Act & Clause	Forms of Online VAW Addressed	Details of the Offence
IT Act Section 66E	Capture and transmission of images of private parts	sexually explicit photo and video content that is maliciously distributed and circulated without consent. on social internet, graphic sexual abuse.
IT Act Section 67	Publishing/transmission of obscene material in electronic form	sending, without consent, emails or social media communications with pictures and other sexually explicit content.
IT Act Section 67A	Publishing/transmission of sexually explicit content	Transgressive sexual harassment on blogs and social media; unsolicited emails and messages on social media with explicit sexual content.
IT Act Section 67B	Material depicting children in an obscene manner	Child pornography's dissemination.
IPC Section 354A	Sexual harassment	sending a woman sexually explicit material and photographs against her will; displaying pornography on her request.
IPC Section 354C	Voyeurism	Witnessing or recording a woman doing a private act; sharing such photographs without the woman's permission.
IPC Section 354D	Cyber-stalking	tracing a lady, reaching out to her to promote a personal relationship in spite of obvious indifference, or keeping an eye on her use of social media. Victims were only identified as women.
IPC Section 499	Criminal defamation	Damage to one's reputation, which affects women who blog and use social media to combat libel and slander.
IPC Section 507	Criminal intimidation by anonymous communication	can be used by females battling hostile trolls to their advantage.
IPC Section 509	Insult to the modesty of a woman	can be used in incidents of online sexual abuse and harassment.

Table 1: Important legal clauses that can be used to stop online violence against women[9]

3.2. Challenges and gaps in the current legal framework

States nationwide are deeply troubled by the increase in crimes against women; nevertheless, cybercrimes exacerbate the situation by providing offenders with the opportunity to create false identities before committing crimes. To address this, the government should adopt strict rules, as "Internet service providers (ISPs)" are the only institutions that have a complete record of all the data accessible by everybody using the internet. Early crime prevention can be achieved by encouraging ISPs to report any questionable behavior that an individual participates in.

Stricter laws must be passed to govern cybercafes, which must keep a complete and accurate record of every consumer who uses their internet services. People frequently engage in illicit conduct at cyber cafes to hide their IP addresses from potential investigations. Here's another technique to keep your identity a secret.

Several procedural issues, including lack of proof, conflict of jurisdiction, absence of a cyber army, and a judiciary with a keen understanding of cyber crimes against women, are major obstacles to the issue of cybercrimes against women. The enactment of laws designed to address the concerns is shaped in large part by the judiciary. Due to the expanding reach of cyberspace, territorial boundaries no longer seem to have any significance or limitations. As a result, the concept of territorial jurisdiction, as envisioned by "S.16 of the C.P.C. and S.2 of the I.P.C.", will have to make way for alternative dispute resolution methods that place less weight on how relevant the issue is about cybercrime.

Non-sexual online harassment is not adequately addressed. In reference to personal trolls, generic sexist insults have not been covered by Sections 499 and 507 of the IPC, which deal with criminal defamation and criminal intimidation, respectively. Furthermore, doxing that doesn't include distributing sexual content or engaging in intimidation is not included. Although hacking is prohibited by Section 66 of the IT Act, the act makes no mention of doxing by hacking. Internet trolling, verbal abuse, and hacking for doxing are considered individual, personal offenses under Sections 499 and 507 of the IPC and Section 66 of the IT Act. The fact that this abuse is being done against a woman simply because she is a woman should not be overlooked. It is evident from the past that the women's sexual orientation and caste are the basis for the abuse. In contrast to the other provisions of the IT Act and IPC, which describe violence as a trespass on one's bodily integrity and personal autonomy, "Section 66E of the IT Act and provisions 354C and 354D of the Criminal Laws Amendment Act 2013 define violence as physical harm. Additionally, these sections only address physical privacy—not "informational privacy."[10] Though Section 509 of the IPC mentions "privacy," it exclusively discusses women's modesty about privacy. Sexual violence is primarily seen from the perspective of upholding public decency by preventing obscenity and defending women's modesty". Furthermore, withdrawal at any time is evident. The coexistence of sexual abuse and the requirement to control the validation and portrayal of sexuality leads to the perpetuation of gender norms that prioritize safeguarding women's sexuality over their health or privacy. It is an economic violation, not a gender or social offence, to violate Sections 72[11] and 43 read in conjunction with Section 66[12] of the IT Act. Legal recognition of gender-based psychological abuse of women

occurs only within the context of their families. It has not been done to acknowledge psychological violence, which is the sharing of personal information through invasions of privacy that are not sexual. In addition, regulations such as the Protection of Women from Domestic Violence Act of 2005, which addresses situations involving psychological abuse in live-in relationships and at home, do not address cybercrime against women.

3.3. Recent legal developments and amendments

Prohibition-era indecent portrayal of females William (2012): Those who attempt to present an offensive image of women through photographs or recordings face consequences under this statute. The Internet content is now covered by this Bill, which has expanded its purview. India's Cyber Laws for Women, n.d[13].

Section 5: Under this provision, an officer may enter and search any location within the area at any reasonable time. They may also look through and seize any pornographic materials that they believe to be evidence of the offense.

Section 6: Penalties are outlined here, and they can range from ₹ 10,000 to ₹ 50,000 for a fine and from 6 months to 5 years in jail.

3.4. Comparative analysis with international legal frameworks

Diverse strategies and levels of specificity in tackling cybercrimes against women are revealed by a comparative study of the legal systems in India and other countries. With an emphasis on crimes against women, numerous nations throughout the world have created legislative frameworks that expressly target cybercrimes.

One notable move in this direction has been made by the European Union (EU). The European Union's Directive (2008) addresses hate speech and has the potential to encompass specific types of cyberbullying and harassment. It also addresses the use of criminal law to combat certain forms and expressions of racism and xenophobia.)[14] Additionally, the "General Data Protection Regulation (GDPR)" influences the handling of personal data in a big way, which indirectly affects cybercrimes that involve identity theft and invasion of privacy (European Parliament and the Council of the European Union, 2016).[15]

Numerous federal laws, such as the Violence Against Women Act, which addresses online harassment and cyberstalking, are among the many laws that the US government has passed expressly to stop cybercrimes. Furthermore, with indirect benefits for women's protection from cyber risks, the Cybersecurity Information Sharing Act aims to improve cybersecurity measures overall. United States Congress, 2015. [16]

Retaliation porn and other cyberstalking are examples of specific cybercrimes against women that are less specifically covered under India's Information Technology Act and IPC regulations, which are generally more general. As seen in certain Western nations, more focused and specialized legislation is still required even though the legal structure has been improved by recent changes and Supreme Court decisions.

4. Cybercrimes Against Women: Case Studies

i. Ritu Kohli Case[17]:

In India's first reported case of cyberstalking, Ritu Kohli filed a complaint against an individual who impersonated her online, engaging in obscene conversations and disclosing her personal

contact information, leading to numerous harassing phone calls. The offender was traced through IP addresses and arrested. This lawsuit was filed under the Indian Penal Code's Section 509, which addresses actions or gestures meant to offend a woman's modesty. The offender was subsequently released on bail. This case set a precedent for addressing cyberstalking in India and highlighted the need for specific laws to combat such cybercrimes.

ii. DPS MMS Scandal[18]:

An MMS clip showing a schoolgirl in a compromising circumstance was distributed across multiple internet networks, which led to the DPS MMS scandal. In a related incident in Mumbai, a Swiss couple was arrested for creating child pornography by forcing slum children to pose for obscene photographs and uploading them to websites catering to pedophiles. While the specific judgments in these cases are not detailed in the document, they underscore the severity of cybercrimes involving sexual exploitation and the legal actions taken under various sections of the Indian Penal Code and the Information Technology Act.

iii. SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra[19]:

In India, this case is the first instance of internet defamation. A SMC Pneumatics employee wrote their business associates lurid and offensive emails regarding the Managing Director of the company. Following the company's identification of the perpetrator with the aid of a computer specialist, the Delhi High Court ordered an ad-interim injunction that forbade the employee from writing, publishing, or otherwise spreading emails that were defamatory. The court's readiness to step in to stop additional reputational injury and the availability of civil remedies in cyber defamation cases were both made clear by this case.

iv. The State of Tamil Nadu Vs Suhas Katti (Case of Obscene Messages in Yahoo Group) [20]:

This case concerned the posting of obscene, libelous, and irritating statements about a divorced woman in a Yahoo messaging group, which resulted in repeated harassing phone calls. The mails were sent from a fake email address created in the victim's name. The case demonstrated the misuse of online platforms for character assassination and the legal implications of such acts under the IT Act and IPC. However, the specific judgment or legal outcome of this case is not provided in the document.

v. Air Force Balbharati School Case (Delhi)[21]:

In this case, a student at Delhi's Air Force Balbharati School, fed up with being taunted for his pockmarked face, altered photographs of his classmates and teachers into naked images and submitted them to a website. This act was reported to the police by a parent. The case was addressed under the IT Act 2000, specifically Sections 43 and 66, which deal with computer-related offenses and data protection, and Section 509 of the IPC. This case serves as an example of the legal consequences of cyberbullying and the misuse of digital platforms for harassment.

vi. Jibin Babu v. State of Kerala

In her statement, the victim stated that she had been in love with the accused for a few years. When the accused traveled to India in February

2019 from the Gulf, they would meet up. The accused then took the victim to a hotel where they had sex. The accused then shared the graphic photo of the victim with their friends. The Information Technology Act's sections 66 E, 67, and 67 A were used to register the case[22].

vii. Sazzadur Rahman v. The State of Assam and Ors.

The accused created a fake Facebook account for the victim, using the victim's name, posted a pornographic photograph, and used abusive comments. Trial court found accused guilty in accordance with IT Act Section 66 E and IPC Section 354 D.The trial court rejected the accused's application made in accordance with section 311 of the CRPC . Following that, an application was filed under section 482 of the CRPC, but the Gauhati High Court rejected it[23].

5. Role of AI in Addressing Cybercrimes Against Women

The issues AI brings to law enforcement are made clear by the Octopus Conferences on Cooperation against Cybercrime in 2018 and 2021.These obstacles include obtaining and keeping electronic evidence, as well as issues in making video and document forgeries illegal. These presentations emphasize how understanding the nuances of artificial intelligence (AI) and identifying and apprehending those who abuse AI systems need measured risks and coalition building. The management and operation of AI systems raises significant technological and legal difficulties, particularly when examining cases where it is necessary to hunt down fraudsters utilizing internet data. In this sense, international service providers are crucial to the assistance of law enforcement agencies. As seen by the current trends in cybercrime, criminals are increasingly relying on artificial intelligence (AI) to enhance their illicit activities, especially when it comes to the spread of malware and ransomware attacks. In response to these challenges, UNICRI's Centre for Artificial Intelligence and Robotics is creating a Toolkit for Responsible AI Innovation in Law Enforcement. To give law enforcement organisations throughout the globe the essential insights, use cases, guidelines, suggestions, and best practices for utilising AI technologies responsibly, this toolkit intends to offer them useful advice.

6. Combating Cybercrimes Against Women: Strategies, Best Practices, and AI-Based Initiatives

- Legal Awareness: Understanding the legal aspects about cyberspace is crucial. Reporting the incident is imperative, and the victim shouldn't be afraid to do it because doing so could make things worse. For reporting cyber crimes against women, there are dedicated hotlines. where the victims receive free legal aid in 1091/1090. It is now imperative that people be aware of and knowledgeable about cyber regulations.
- Training of Officials: To stop the increase in cybercrimes, members of the court, police officers, and specialists in cyber law must receive training. They need to be informed about how they respond to various cybercrime situations. These days, numerous cybercrime subsets handle various online threats, such as phishing, blackmail, hacking, stalking, morphing, and others.
- Privacy Policies and Guidelines: Before accepting, women should read over all the terms and conditions because certain websites are phoney and vulnerable to

hacking. To be sure that hackers cannot access their social media accounts, the women need to go through the privacy settings. It is important for everyone opening an account on a website to read the terms and conditions since it will assist them prevent future cybercrimes. This is a leisurely process; thorough research should be conducted before accepting any pop-up boxes at random.

- Discourage Information Sharing: To prevent information from being leaked or used against them, women should refrain from disclosing to third parties their passwords, electronic signatures, bank account information, and other personal data.
- Update passwords Frequently: To prevent hacking, one must periodically update their passwords. Passwords must be kept private and not disclosed to those who are closed.
- The importance of raising awareness regarding cybercrimes cannot be overstated. Young boys uninformedly begin committing these crimes, and like most teenagers, young ladies fall victim to such acts. Education institutions need to plan campaigns, seminars, and workshops. Advertising on television and social media helps spread awareness of cybercrime among a large audience.
- Saving the Evidence: If a woman experiences cyberviolence, she should be aware that it's critical to save all documentation of the offense, including offensive texts, explicit recordings, and crude remarks made to her. Threatening calls can be traced back to certain phone numbers. Cyberlaw specialists may use it to uncover information.
- Install Anti-Virus Software: To prevent hackers from trying to steal information, people must install the most recent versions of anti-virus software on their laptops and desktop computers. It is important to know when to use secure URLs and to stay away from unprotected websites. Firewall settings need to be maintained. Better privacy against Trojan and other email infections is ensured.
- Steer clear of unsolicited friend requests and spam calls: Be cautious when using the internet. It is usually best to decline friend invitations from people you do not know and to ignore calls from spammers. It is merely a precautionary measure to ward against cybercrimes.

7. Role of intermediaries in the detection of cybercrime against women

i. Role of Government:

Online harassment of women in India should be punished the same as physical assault against them, according to Union Minister for Women and Child Development Ms. Maneka Gandhi's May 2016 statement. This recognition prompted the National Commission for Women to design a mechanism to combat online harassment of women and resulted in the establishment of a new forum for discussing such matters. This initiative marks a significant step in recognizing and combating the virtual harassment and abuse faced by women.

ii. Role of Intermediaries (ISPs):

Because it's so simple for thieves to fabricate identities and commit crimes online, the rise in cybercrimes targeting women presents a special issue. In response, the paper recommends that governments impose more stringent laws on ISPs because they have extensive logs of everything that is done online. ISPs should be obligated to report any suspicious activities identified during internet usage. This approach aims to curb such crimes at an early stage, emphasizing the crucial role of ISPs in detecting and reporting cybercrimes against women.

8. Conclusion

Conclusively, the investigation into cyber crimes against women in India, including the legislative structures, the function of artificial intelligence, and different approaches and best practices, highlights a complicated and diverse issue. Although it offers a foundation, the current legal framework has shortcomings and makes it difficult to manage cybercrimes because of their dynamic nature. The legal framework has become more responsive through amendments and judicial interpretations, but stricter and more targeted legislation is still required. India faces unique issues, and the global dimension of the issue is shown by the comparative analysis with international legal frameworks. Lessons and approaches for reforming laws and policies can be learned from this comparison. Case studies that highlight the seriousness and consequences of cybercrimes against women are presented in real-world settings, underscoring the need for prompt and effective action. Cybercrime detection, prevention, and response have all showed potential when facilitated by AI-based projects. Thought must be given to the ethical and privacy implications of these technologies when they are used. An impartial approach is required, even when the assessment of these AI-driven indicators shows a good trendA road map for an all-encompassing response to cybercrimes against women is provided by global strategies and best practices, which include technology advancements, legal reforms, educational programmes, and multi-sectoral partnerships. These tactics ought to be customised for India's unique social, cultural, and legal environment. Fighting cybercrimes that target women involves not only legal action but also social and technological change. To make the internet a safer place for women, governments, courts, tech professionals, educators, and members of civil society must work together consistently. This multimodal strategy would not only tackle the existing issues but also clear the path for women in India and elsewhere to have a more safe and equal digital future.

REFERENCES

1. "Business Standard. (2022). Cybercrime against women up 28% since 2019, Karnataka's share highest: NCRB. Retrieved from https://www.business-standard.com/article/current-affairs/cybercrime-against-women-up-28-since-2019-national-crime-records-bureau-122083001139_1.html"

2. "Telegraph India. (2023). Odisha reports highest cases of cybercrime against women in 2022: NCRB. Retrieved from https://www.telegraphindia.com/india/odisha-reports-highest-cases-of-cybercrime-against-women-in-2022-ncrb/cid/1916672

3. Citron, D. K. (2014). Hate Crimes in Cyberspace. Harvard University Press. https://www.hup.harvard.edu/catalog.php?isbn=9780674368293

4. Bailey, J., & Travers, K. (2017). The Gendered Dimensions of social media. In J. Bailey, V. Steeves, & J. Burkell (Eds.), eGirls, eCitizens. University of Ottawa Press. https://press.uottawa.ca/egirls-ecitizens.html

5. Henry, N., & Powell, A. (2015). Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. Australian & New Zealand Journal of Criminology, 48(1), 104-118. https://journals.sagepub.com/doi/abs/10.1177/0004865814524218

6. West, R., & Lloyd, J. (2017). The Role of Digital Technology in Responding to the Challenge of Cyberbullying. In K. Jaishankar (Ed.), Cyber Criminology. Springer. https://link.springer.com/book/10.1007/978-3-319-72613-8"

7. DEBRATI HALDER & K. JAISHANKAR, CYBER CRIMES AGAINST WOMEN IN INDIA

8. https://www.legalserviceindia.com/legal/article-8918-cyber-crimes-against-women.html

9. "Technology-mediated violence against women in India, IT FOR CHANGE, (Jan 29, 2021), https://itforchange.net/e-vaw/wp-content/uploads/2017/12/DISCUSSIONPAPER.pdf"

10. "Information privacy, or data privacy (or data protection), concerns personally identifiable information or other sensitive information and how it is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. In relation to technology, it pertains to the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them".

11. Breach of privacy and confidentiality

12. Data Theft

13. Women - Cyber Laws in India. (n.d.). Information Security Awareness. All Rights Reserved Ministry of Electronics and Information Technology (MeitY), Govt of India. Retrieved June 15, 2022, from https://www.infosecawareness.in/concept/cyber-laws-inindia/women#:~:text=Section%2066E%20of%20the%20IT,years%2C%20and%2For%20fine.

14. "European Parliament and the Council of the European Union. (2008). Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law".

15. "European Parliament and the Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation).*

16. U.S. Congress. (2015). Cybersecurity Information Sharing Act of 2015. *Public Law 114-113.*

17. http://cyberlaws.net/cyberindia/2CYBER27.html

18. http://en.wikipedia.org/wiki/DPS_MMS_Scandal"

19. http://cyberlaws.net/cyberindia/defamation.ht

20. http://www.naavi.org/cl_editorial_04/suhas_katti_case.htm

21. Abhimanyu Behera, " Cyber Crimes and Law In India," XXXI,IJCC 19 (2010)

22. Decided by Kerala High Court on 26 August, 2020.

23. Criminal Petition No. 654 2019.