RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

Cyber Harassment and Online Safety of Women in India: Legal Challenges and Policy Responses

Dr. Rahul Tiwari

Assistant Professor,

Atal Bihari Vajpayee School of Legal Studies,

C.S.J.M. University (Formerly Kanpur University),

Kanpur, Uttar Pradesh

Abstract

The blistering development of the use of internet in India has created both chances and obstacles with regard to the security of women in the online worlds. Even though the online platforms have enabled greater involvement in the social, economic and political arena, they have also become the arenas of several forms of gender-based violence and harassment. This research attempts to examine the natures and scale of cyber harassment that is faced by women in India, to assess the current legal provisions and the associated limitations and to review the policy reactions aimed at ensuring internet security. The results indicate that there are extensive gaps between the law and its positive application, leading to the need to make extensive changes, improve digital literacy, and unite the efforts of stakeholders to create safer online experiences of women.

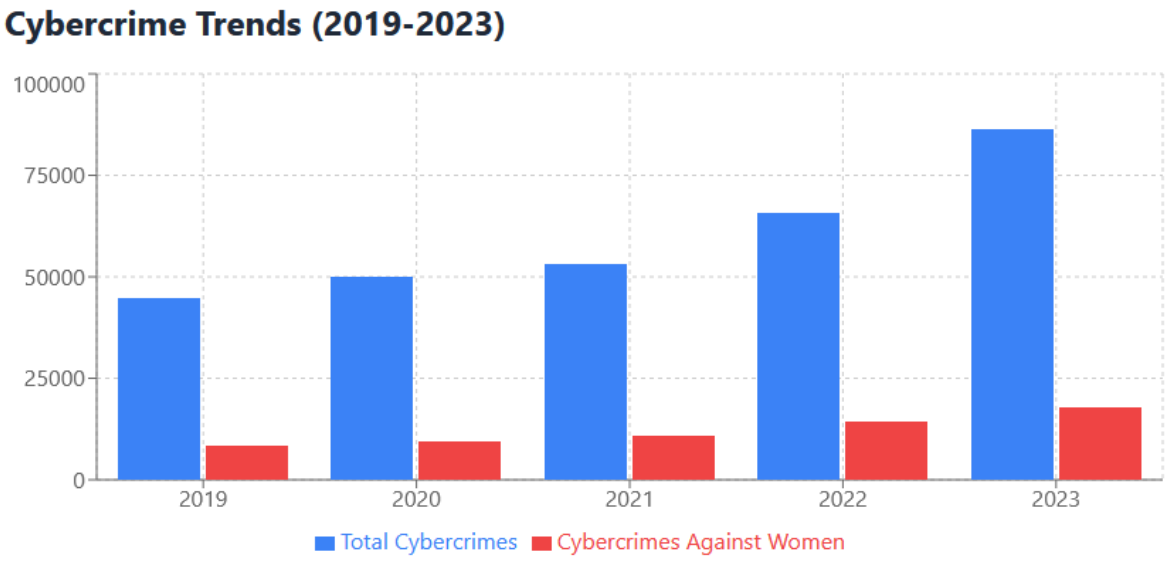
Keywords: Cyber harassment, online safety, women's rights, digital India, IT Act, cybercrime, gender-based violence, legal framework

1. Introduction

In the last ten years, India has gone through a digital revolution that has never been witnessed. The country has over 700 million internet users by the year 2023 and is one of the most populous online users across the world. The women represent a growing portion of this digital community who use the internet to gain an education, take up jobs, engage in social networking, and exercise their civic

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

rights. However, this increased digital footprint has been welcomed by a worrying trend in the online harassment, cyberbullying, online stalking, and other forms of gender-based violence in the online space. Women face cyber harassment not just as a technology problem, but as a symptom of the attitudes of society as a whole to gender and power issues. The anonymity and affordability of the internet has empowered the individuals to attack women without any fear of punishment, which can at times cause catastrophic psychological, social and work related impacts on the victims. The full picture and proper response to this trend require studying the legal context of cybercrimes and the social and institutional processes as a whole that deal with online violence against women. This paper examines the complex issue of cyber harassment against women in India with respect to answering three questions: (1) What is the nature of cyber harassment, and how common is it? (2) How well has the current legal framework had in meeting these challenges? (3) Which policy measures have been taken and which loopholes still exist in making women safe on the Internet?



Sourse: National Crime Record Bureau

1.2 Research Objectives

This paper aims to:

- Break down what cyber harassment against women in India really looks like
- Examine the current legal and regulatory system meant to tackle it

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

- Point out where the laws and policies fall short
- Take a hard look at how well these rules actually work in practice
- Suggest real changes to make the internet safer for women—through legal reforms and better policies

1.3 Methodology

To conduct this study, I have reviewed the legal documents, statutes, case law, and government policies. I used academic articles, reports published by non-governmental organizations, crime statistics provided by the National Crime Records Bureau, and empirical studies about women experience of cyber harassment. To get a wider scope, I have contrasted the Indian legal practice with international legal practices and best practices embraced by other countries of the world.

2. Understanding Cyber Harassment Against Women

2.1 Defining Cyber Harassment

Cyber harassment is the deliberate act of using digital technologies in order to threaten, intimidate, or otherwise cause harm to a person. When targeted at the female gender, it often capitalizes on the existing stereotypes and gender norms about the male gender. Unlike conventional harassment, online abuse is not bound by territorial limits, takes place immediately, and has the capacity to reach out to thousands or even millions of victims in a very limited amount of time. Moreover, the online published material is likely to stay forever and essentially the harassment is perpetuated.

There are certain reasons why cyber harassment is especially vexing:

• Anonymity: It is common to find that abusers hide their identity behind more made-up accounts, making it difficult to trace them down or to punish them.

• Viral potential: Dangerous information can spread to various platforms in a few seconds.

• Permanence: When placed in the virtual world, content may cause a long-term psychological influence on victims.

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

• Availability: Harassment can be done at any time of the day, which is an intrusion in the private space of a woman.

• Group behavior: There are occasions where groups form and gang up to accuse and attack people.

All these features place cyber harassment not only as a legal problem but a social one that requires urgent and innovative solutions.

2.2 Forms and Manifestations

Women are cyber harassed in diverse ways. These manifestations are as described in the following sections:

Cyberstalking: Cyberstalking can be explained as an intruder having incessant and undesired communication with the victim using digital means. This can take the form of constant, unwanted communications, the systematic stalking of social media accounts, or using spyware and GPS tracking to monitor the physical activities of a victim in the real world. This kind of behavior often transpires into offline situations, therefore increasing the fear of physical harm.

Non-consensual Intimate Image Distribution (NCII): More often known as revenge porn, NCII also deals with the unauthorised distribution of personal or erotic photographs or videos. Psychological impact is also huge, as it includes trauma, shame, or, in worst circumstances, self-harm or suicide.

Morphing and Deepfakes: The technologies of morphing and deepfakes have their difficulties. With the use of digital manipulations, a woman can be independently superimposed with the features of her face onto sexual pictures or videos. With the development of these methods, it is becoming hard to tell whether the content is original or fake with disastrous personal errors.

Doxxing: Doxxing is a phenomenon in which one shares private information (residential address, telephone number, professional or career information, contacts) with others. The main motive is normally to cause aggression or threaten the victim.

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

Online Trolling and Abuse: Lastly, there is online trolling and abusive commentary that is quite common especially directed at women in the limelight. Such strategies take the form of aggressive insults, threats, hyper-sexual comments among other degrading messages that are meant to shut down or scare the target.

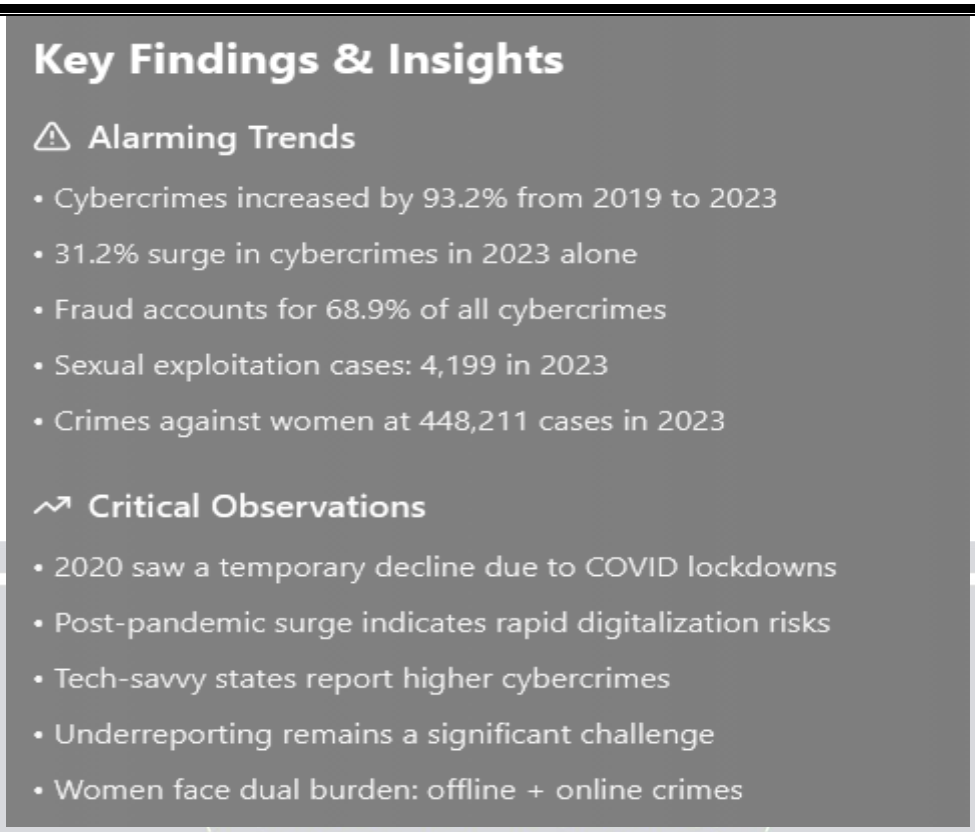
Impersonation and Identity Theft: Fraud and identity theft are two common trends in the modern digital landscape. People tend to obtain photographs and personal information in unauthorized ways and further use it to create fake accounts. Such fabricated identities can spread materials that would undermine the reputation of the target or commit fraudulent request of other users. Blackmail is another negative form of abuse via the web. The offenders might threaten to release intimate photos or confidential data unless the victim fulfills the requirements which might involve giving money, sexual abuse, or provide other embarrassing media. These coercive measures are based on psychological subjugation and terror inculcation.

Year-over-Year Growth Rates (%)

Category	2020 vs 2019	2021 vs 2020	2022 vs 2021	2023 vs 2022
Cybercrimes	+11.8%	+5.9%	+24.4%	+31.2%
Cyber Against Women	+14.5%	+12.9%	+34.7%	+24.5%
Overall Against Women	-8.3%	+15.3%	+4%	+0.7%

Data Source: National Crime Records Bureau (NCRB) - Crime in India Reports (2019-2023)

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL



Data Source: National Crime Records Bureau (NCRB) - Crime in India Reports (2019-2023)

2.3 Impact and Consequences

The adverse effects of cyber harassment also have physical consequences on the daily experiences of women even though this is taking place in an online space. The severity of internet aggression is directly converted into severe damages to not only mental health, career progression, social interactions, but also physical safety. Evidence shows that women victims of digital harassment have significantly increased rates of both anxiety and depression, post-traumatic stress disorder, and sleep disturbance as well as suicidal ideation compared to the general population. The consequences of this aggression continue to exist in the professional realms. Some of the failures women face include limited employment opportunities or exclusion by the society. Journalists, activists, and other professionals can use self-censorship or entirely withdraw themselves to social media platforms to express opposition to the unstoppable internet bullying. This withdrawal does not only slow down

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

individual participation, but also erodes the energy of the public discourse and sustains gender inequality especially in the spheres where inclusion should dominate. Stigmatization also adds to the difficulties of the victims and particularly when the issue concerns non-consentual sharing of intimate pictures. Social prejudice tends to hold the victims of attacks responsible of the injuries they receive hence enabling the real culprits to get away with their deeds. Such social stigma makes silence more real and further perpetuates cyclical dynamics of abuse, since victims have to face embarrassment or fear which stands in the way of seeking help.

3. Legal Framework Addressing Cyber Harassment in India

3.1 Constitutional Protections

India has provided substantive protection against cyber harassment of women in the Constitution of India. Article 14 requires equal treatment in the law hence obligating the state to provide protection to women in cyberspace in a similar way as other citizens. Article 15 forbids the discrimination based on sex and permits the legislature to adopt special provisions with regard to safeguarding women and hence a legal basis of gender specific legislation is well-founded. Article 19(1)(a) also ensures that there is freedom of expression; however, when harassment forces women to make decisions against participating online, or even silences them, it is not just bullying, but a loss of constitutional rights. Article 21 provides the right of life and individual liberty, and the Supreme Court has stated that the right does include privacy and dignity. The cyber harassment therefore crosses the constitutional limits.

3.2 Information Technology Act, 2000 and Amendments

Section 66C concerns identity theft and impersonation offenses that attract up to three years in jail or a hefty financial penalty against those individuals who masquerade as other individuals online. Section 66D makes it a criminal offense to use computers in misrepresenting oneself under the guise of assuming the identity of another person. In section 66E privacy is protected by disallowing non-consentual capture and sharing of intimate images by providing imprisonment and fines upon their

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

breach. Section 67 punishes the dissemination or release of the obscene content in the digital form by imposing severe penalties to the violators. Section 67A subjects penalties which are more severe in the face of distribution of sexually explicit material, the first time offender and the offender who repeats are treated differently. Section 67B carries harsh punishments to the creation and propagation of child pornography such as long custodial sentences and large fines.

3.3 Bharatiya Nyaya Sanhita, 2023 Provisions

An Indian law Bharatiya Nyaya Sanhita (BNS), which processes replacing the old Indian Penal Code, has been introduced by law to combat cyber harassment and has new provisions in this area. Section 294 makes the distribution or sale of pornography a criminal offense hence substituting the former IPC Section 292. Section 74 concerns sexual harassment, which can be non-consensual touching, requests of sexual favours, distribution of pornographic material and indecent comments; it replaces the previous IPC Section 354A and provides penalties of up to three years of imprisonment or a fine. Section 77 punishes voyeurism by forbidding any recordings or any publication of intimate photographs of women without their permission, and the custodial sentence is between three and seven years and fines. Section 78 is a criminal act against stalking which includes monitoring the use or conversations of a person on the internet; first offenders can serve up to three years in prison and repeat offenders can serve up to five years in prison and receive a fine. In sections 356 and 357, the case of defamation is covered with the corresponding equally severe punishment. Section 351(2) is the issue of criminal intimidation, punishable to not more than two years of imprisonment or a fine, whereas Section 351(3) increases the penalty of more serious cases. Section 79 covers the cases of the offense of offending the modesty of a woman with words, signs, or other actions, including in the form of an online transmission, and the imposition of a sentence of up to three years in prison or fine.

3.4 Specific Legislation

The Protection of Children from Sexual Offences Act (POCSO), 2012 recognizes that child sexual abuse now happens online, too. It includes rules to tackle digital exploitation of children.

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, covers electronic communications, acknowledging that workplace harassment often happens through emails or messages these days.

The Indecent Representation of Women (Prohibition) Act, 1986, bans indecent representation of women across all media, and yes, that includes anything digital.

3.5 Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita (BNSS) that came into effect in 2023 substitutes the previous Code of Criminal Procedure and introduces major changes to the procedure of the adjudication of cases related to cyber harassment. Section 173 streamlines the process of investigating female-related crimes and outlines the measures that have to be followed when dealing with electronic evidence. Section 193 stipulates that, in cases of sexual offence, even with an online element, a woman police officer should be there to record the statement of the victim, or at least to give testimony. Section 230 allows the courts to capture evidence using video conference, hence relieving the victims of cyber harassment otherwise subjected to the stress of in-person testimony.

3.6 Recent Legal Developments

Since 1 July 2024, the criminal justice system of India has undergone significant reform as a result of the implementation of the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam, which replace the Indian Penal Code, Code of Criminal Procedure and Indian Evidence Act. These amendments focus on the crimes against women and simplify the manner in which the electronic evidence is processed. The Rules of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) 2021, provide new compliance requirements to social media platforms, which are now mandatory to face infringement on their websites and remove it promptly, have a grievance officer, and make messages traceable. These provisions have however been questionable on the issue of privacy and any misuse. There are a few

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

states, with Maharashtra being the most prominent, that have implemented the lawmaking directly aimed at cyberbullying and online harassment.

4. Judicial Response and Key Judgments

4.1 Landmark Cases

Shreya Singhal v. Union of India (2015): The Supreme Court held that the IT Act Section 66A was unconstitutional and in violation of the freedom of speech as the provision was too vague and created a significant obstacle to free speech. Although it has asserted that online harassment is a severe issue in society, the Court still had other statutory means to protect people against internet abuse.

Justice K.S. Puttaswamy v. Union of India (2017): The Court in this historic decision gave privacy a status that it possesses a fundamental right under Article 21 of the Constitution. These implications of the ruling were significant in terms of protecting women against privacy violation against non-consenting intimate imagery and doxxing.

Kamlesh Vaswani v. Union of India (2018): The Supreme Court found loopholes in the law addressing revenge pornography and instructed the government to create an extensive law on the issue of the non-consenting distribution of intimate pictures.

State of Tamil Nadu v. Suhas Katti (2004): It was the first case that was convicted under the Section 67 of the IT act, in which a woman was defamed and sent obscene messages on the internet. The decision of the Court created a great precedent in the responsibility of cyber bullies under the current statutory laws.

4.2 Judicial Interpretation and Evolution

The judiciary's interpretation and development process is this one. Over the years, the Indian judiciary has increasingly been familiar with the concept of cyber harassment as a severe type of harm that has specific gendered implications that are not limited to the digital world. Misconduct online can never be regarded as virtual, jurists have now realized that it creates long lasting harm, and this is enhanced by the speed and ubiquitous nature of online

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

information. Conceptualizations on privacy and defamation seen as traditional have become seemingly less relevant in dealing with such problems. Moreover, courts are coming to realize the propensity of re-traumatizing victims that come with judicial processes especially in cases where legal practitioners are not sensitive to the experiences of survivors. However, the state of affairs is not even. There are those judicial actors who have taken a technology conscious stance and have expressed an understanding of victims, whilst there are those who continue to use outdated paradigms, or in some cases, victimize the victims by asking about their online activity rather than the actions of the violator.

4.3 Challenges in Judicial Process

There are still a number of hindrances to effective adjudication of cyber-harassment cases. The long litigation times are caused by the overloading of the judicial system and the complexity of technical evidence, the result of which is often insufficient technical understanding of the judges and counsel. Important information can therefore be missed. The process of the courtroom can be an extremely upsetting event to victims, particularly when relating to the non-consensual intimate imagery case, where the reliving of the trauma is usually required to prove liability. Additionally, the courts often provide bail in a very liberal manner without due consideration of the severity of the misdemeanors or the chances of being harassed. Consequently, victims have to wait until the end as the damaging material is still circulating and the image of justice is distorted.

5. Implementation Challenges and Gaps

5.1 Law Enforcement Capabilities

Cyber harassment laws are relatively problematic to enforce in India. It is common to find that police officers do not have the necessary training, technology, and manpower to deal with such crimes. A good number of officers do not have much experience in cybercrime investigations, and a significant percentage of them lack familiarity with the technology behind such a crime, leading to poor evidence acquisition. Cybercrime departments have frequently their hands full, and many jurisdictions do not

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

have specific teams. This means that victims might be forced to move to metropolitan centers just to complain since local law-enforcement agencies are not well established to support them. Besides, complaints are also treated in a biased manner, especially when it comes to women. Victims also complain that they have been dismissed, blamed or just refused to document their complaints, particularly in instances when high level of intimate material is used. The fact that most of the cyber-harassment incidents are trans-regional in nature makes the incidents often cross municipal or state boundaries, which makes it even more difficult to involve the different departments, bring about further confusion and procedural delays.

5.2 Technical and Evidentiary Challenges

Cyber-harassments are facing serious evidentiary challenges during prosecution. It is known that digital evidence is not very strong and can be easily tampered with; inadequate methods of collecting or retaining it can destroy its value as evidence in court. A huge percentage of police departments do not have sophisticated forensic equipment or do not have the necessary training. Attackers also hinder the investigation process by using encryption, virtual private networks (VPNs) and anonymizing browsers to hide their identities, thus triggering an investigative standoff. Matters are compounded by the fact that the suspected criminal may be located in a different country; conflicting legal systems and the concerns of sovereignty make it difficult to collaborate and impossible to hold anyone accountable. The assistance given by social media platforms is often scarce considering that they often take long to respond to evidence requests, thus giving offenders a greater chance to delete their posts or otherwise obscure their actions.

5.3 Underreporting and Social Stigma

There is a large amount of unreported cyber-harassment. Social stigma is an influential deterrent especially where intimacy imagery is non-consensual. Victims are usually afraid of being ostracised, creating a negative reputation of the family, or compromising marriage prospects and hence a culture

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

of silence that lets offenders get away with it. The unawareness of the population makes the problem even worse; women, in their turn, might be completely unaware of the legal options, or support. Along with the available digital literacy programs, cyber-harassment laws are rarely covered. There is a lack of trust, which is caused by the negative experience of interacting with the police in the past, lengthy court processes, and poor conviction rates, which further deteriorates reporting. Also, there is a fear of retaliation that may follow, additional harassment, or even the consequences at work, which strengthen passive compliance in victims.

5.4 Legal Gaps and Ambiguities

Even after the enactment of statutory provisions, there are substantive laws gaps. India currently does not have a specific law that pays particular attention to the criminalization of non-consenting communication of intimate images. This means that the law enforcers have to make use of fragmented applications of irrelevant laws, which is inadequate. The punishments tend to be out of proportion to the extent of damage committing, which means that a first-time criminal does not go through serious punitive measures. Civil penalties are never so much; victims have weak sources of compensation, injunctions, or forced removal of content. The current legal emphasis is too much on criminal liability, at the cost of full victim support. Weak regulatory measures of social media sites are, however, inconsistently applied; common businesses have been using safe harbour exemptions without properly mitigating the filtering of the harmful content. Finally, the laws are not effective to combat coordinated harassment efforts; strategic campaigns that will target to crush victims through group efforts are mostly uninterrupted and unchecked.

6. Policy Responses and Initiatives

6.1 Government Initiatives

The Indian government has carried out a set of measures to prevent cyber harassment. The key place of filing complaints related to different types of cybercrimes, specifically to women and children is on the National Cybercrime Reporting Portal (cybercrime.gov.in). Although the portal has simplified

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

reporting, the portal has weak areas in the follow-up procedures and the overall quality of response. Nevertheless, the resources are limited and limit its ability to reach the whole range of victims. To supplement these initiatives, there is Women Helpline (181) that works 24/7 and provides emergency aid to women who have fallen victim to cyber harassment and helps to connect with the police and other related services.

6.2 Awareness and Capacity Building

The Ministry of Home Affairs conducts police officer training related to cybercrime investigation, however, it is not frequent enough and not extensive. Digital literacy measures have been implemented to encourage online safety measures, including Digital India and liaisons with civil society organizations, but priority is not given to the issue of risks that are unique to women. Some schools have also introduced courses on cyber-safety in their curriculum but there is not much institutional uptake.

6.3 Role of Civil Society

The civil society organisations play a vital mediatory role of counselling, legal and technical aid to the victims, thus alleviating governmental provision gaps. These groups promote legislative and policy tightening and research and documentation of the trends of cyber-harassment, thus impacting the policy discussion. Campaigns that are conducted by using social media, workshops, and educating the public spread the information about the character of cyber harassment and possible reactions of a victim.

6.4 Private Sector Role

The policy execution is taken up considerably by technology companies. They create anti-harassment policies, the implementation of which is significantly inconsistent. The majority of large platforms allow their users to report abuse, though the time of response and the gravity with which they receive treatment varies. The introduction of blocking and muting features on platforms, as well as privacy controls, has not involved most security measures being proactive measures to avert harassment,

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

instead shifting most of these protective tasks to the victims. Other companies also release transparency reports about the content removal and government requests, the specificity and usefulness of such reports varies among corporate organizations.

7. Recommendations

7.1 Legal Reforms

India needs to implement a new law dealing with intimate image sharing that is non-consentual. The criminal behavior proposed in the statute must be clearly defined, be severely punished, make the process of content removal to be easy and ensure victims get support and compensation. Additionally, the legislation must impose greater responsibilities on platforms, including obliging accelerated moderation, quick reaction, and systematic failure repair- whilst preserving privacy and freedom of expression of the users. The civil law should allow the victims to have a wider means of redress, such as injunctions, damages, and removal of the material without criminal proceeding. The dynamic character of organised harassment campaigns creates the need to provide certain provisions to mitigate such vectors. At this point, the statutory protections are rather fragmented, and it would be beneficial to adopt an integrative strategy, i.e. to unite the provisions of the IT Act, IPC, and some other statutes to remove ambiguities and create a harmonious system of regulation.

7.2 Implementation Improvements

Every district is supposed to create a special cybercrime unit, which is to be made up of skilled personnel who have the right tools and adequate resources to deal with cybercrime. Studies Police, prosecutors and judges need regular, compulsory training, which includes not only technical training, but also skills in working with digital evidence and gender sensitivity. Standard, clear procedures ought to be written down to all procedural steps, including the receipt of complaints to the gathering of evidence and support of the victim. Cyber harassment should be dealt with by establishing fast-track courts to ensure that the process does not take too much time. Procedures that are victim-

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

centered like closed-door hearings, remote testimony, as well as provisions against re-traumatization through exposure to unwarranted evidence, are necessary.

7.3 Institutional Mechanisms

A dedicated agency, similar to that of eSafety Commissioner in Australia, would help India coordinate its responses nationally, regulate platforms, assist victims and keep an eye on the big picture trends through research. The National Commission on Women needs to be given more resources and mandate to handle the large number of complaints of cyber harassment. To solve this problem, the active involvement of everyone is required; the institutional measures should be created that would help to unite government, technology firms, civil society, and academic researchers.

7.4 Awareness and Education

The concept of digital safety should be taught in the curriculum of all educational organizations. Students should be taught how to recognize and eliminate, and report abuse on the internet, and what to do when it is occurring in front of them. India needs to carry out long-term national awareness to break the stigma, encourage reporting, and share information on Internet security. It is important to involve communities, especially in rural environments in order to address the issue of shame and support victims. Frontline workers in the case of journalists, teachers and healthcare workers need training on how to best help those who seek their assistance.

7.5 Research and Data Collection

India should enhance its data collection on cybercrime that involve into details, gender-disaggregated statistics, tracking of outcomes of cases and analyzing macro-level trends. Regular appraisal of policies and legislation is required to base the reforms on empirical evidence. National surveys can be regarded as a valuable instrument that cannot be ignored to measure the prevalence, manifestations, and effects of cyber harassment, even those that are not reported. It is possible to constantly improve the efficiency of countermeasures against online abuse through such systematic research.

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

8. Conclusion

Online harassment is not just a worrying menace on the internet, but it is a significant source of danger to the safety, dignity, and inclusion of women in the Indian digital world. Even though India has been enacting numerous laws to deal with this phenomenon, there a lot of gaps in them. The legal provisions are strong on paper, but they often do not work in favor of women who face harassment, which results in the lack of support and neglect on the systemic level. To overcome this challenge, the legal reevaluation of the matter, implementation of efficient measures, and responsibility of the technological platforms should be carried out.

The police and investigators need better investigative instruments and training. Without proper resources and gender-specific procedures, the cases often are not brought to the stage of adjudication. Introduction of special units, as it is practiced in multiple jurisdictions, may make inter-agency coordination more effective and offer more substantive support to survivors.

The technology companies cannot be passive and they need to institute enforceable rules and regulations, apply effective sanctions and increase transparency. They are tasked with the role of building safer such online spaces, investing in more sophisticated content-moderation tools, and working hand in hand with law enforcement organizations when enforcing cases. However, the greatest change should be brought by the change in society.

The silence of too many victims has been caused by shame, or fear; this silence is something that has to be broken. This problem can be reduced by educational programs, community and group discussions, and community support systems. In digital literacy, the curriculum needs to be spread not only to the simple use of applications but also the recognition of harassment, safety precautions, and peer support systems.

Since India moves to a more digitised future, online safety of women is not about technology or legal matters; it is a fundamental part of the achievement of equality and freedom. The accessibility of the online world by women without any fear of doing it, the capacity to express oneself and to contribute

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

as equals is the key to the inclusivity of the future of the digital India. Finally, technology should empower and not threaten people and the rights of digital subjects should be on the same level as the rights of offline defendants.

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

Work cited

i. Amnesty International. (2018). Toxic Twitter: A Toxic Place for Women. London: Amnesty International.

ii. Chatterjee, R. (2021). "Anonymity and Accountability: Legal Challenges in Prosecuting Cyber Harassment Cases in India." Indian Journal of Gender Studies, 28(2), 188-210.

iii. Citron, D. K. (2014). Hate Crimes in Cyberspace. Cambridge: Harvard University Press.

iv. Gurumurthy, A., & Chami, N. (2019). "Unpacking Digital India: A Feminist Commentary." Economic and Political Weekly, 54(17), 42-50.

v. Henry, N., & Powell, A. (2018). Technology-Facilitated Sexual Violence: A Literature Review. Sydney: Australian Institute of Criminology.

vi. Indian Penal Code, 1860.

vii. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

viii. Information Technology Act, 2000 (as amended by the Information Technology (Amendment) Act, 2008).

ix. Internet and Mobile Association of India. (2023). India Internet Report 2023. Mumbai: IAMAI.

x. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

xi. Kamlesh Vaswani v. Union of India, W.P. (C) No. 177 of 2013.

xii. Kapur, R., & Sharma, M. (2019). "Combating Cyberstalking in India: Legal Provisions and Their Effectiveness." Journal of Constitutional Law and Jurisprudence, 12(3), 445-467.

xiii. Mehra, D., & Jain, S. (2020). "Legal Framework and Challenges in Combating Cyber Violence Against Women in India." NLUJ Law Review, 7(1), 89-112.

xiv. Ministry of Home Affairs, Government of India. (2022). National Crime Records Bureau Annual Report 2021. New Delhi: MHA Publications.

xv. Ministry of Home Affairs. (2022). Guidelines on Cyber Crime Investigation.

xvi. National Commission for Women. (2021). Report on Cyber Crimes Against Women. New Delhi: NCW.

xvii. National Commission for Women. (2023). Annual Reports on Cyber Harassment Cases.

RMSG (Rashtrakavi Maithili Sharan Gupt) PUBLICATION
ISSN:3049-4109
INTERNATIONAL DOUBLE-PEER-REVIEWED MULTIDISCIPLINARY E-RESEARCH JOURNAL

xviii. National Crime Records Bureau. (2023). Crime in India Statistics.

xix. Pavan, E. (2017). "The Integrative Power of Online Collective Action Networks Beyond Protest." Social Movement Studies, 16(5), 571-584.

xx. Point of View. (2018). Digital Harassment of Women in India. Mumbai: Point of View Publications.

xxi. Salter, M. (2016). "Privacy, Power and the Internet: Domestic Violence in the Digital Age." Melbourne University Law Review, 40(2), 347-383.

xxii. Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013. Government of India.

xxiii. Shrewsbury, K. D. (2019). "Cyberstalking and the Law: A Comparative Analysis." International Journal of Cyber Criminology, 13(1), 156-178.

xxiv. Shreya Singhal v. Union of India, (2015) 5 SCC 1.

xxv. Subramanian, S. (2020). "Cyber Crime Against Women in India: A Study of Gender-Based Violence in Digital Spaces." Journal of Criminal Law and Criminology, 42(3), 234-256.

xxvi. The Indian Penal Code, 1860 (with relevant amendments). Government of India.

xxvii. The Information Technology Act, 2000 (as amended in 2008). Government of India.

xxviii. United Nations. (2015). Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call.

xxix. Women and Media Collective. (2021). Online Violence Against Women Journalists in South Asia. Colombo: WMC Publications.

xxx. World Wide Web Foundation. (2020). The Impacts of Online Gender-Based Violence on Women in Asia. Washington: WWW Foundation.