INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

CYBERCRIME AGAINST WOMEN: A GROWING CHALLENGE IN THE ERA OF INDIA'S TECHNOLOGICAL ADVANCEMENT

AUTHORED BY - MALVIKA CHOUDHARY

ABSTRACT

The sharp rise of internet use and the vastness of digital platforms in India has transformed how people connect, communicate and do business. The digital revolution has created many opportunities but it has also introduced many new vulnerabilities, especially for women. Cybercrime against women is one of the greatest issues in India's technological ecosystem, and reflects the opportunities and risks of advancing technology. Unlike traditional crimes cybercrimes are able to capitalize on these opportunities for anonymity and reach, resulting in relatively greater harassment, exploitation and abuse against women.

The range of cybercrimes against women is extensive cyberstalking, trolling or targeted harassment, and defamation through online postings and comments, in addition to larger forms of harm like morphing of images, revenge pornography, sextortion, and cyber-trafficking. New forms of digital abuse are appearing through artificial intelligence and deepfake technologies, causing complications for regulatory and enforcement frameworks. The National Crime Records Bureau (NCRB) has reported that these offences have grown exponentially over the last decade, which speaks to a societal and systemic challenge not limited to single instances.

Despite the implementation of legal measures in India through laws created under the Information Technology Act, 2000 and provisions under the Indian Penal Code, enforcement of these measures has not effectively occurred, due in part to jurisdiction restraints, lack of technical skills, and societal stigma allowing victims of cybercrime to remain silent. This essay will critically examine the issue of cybercrime against women in India, the sufficiency of legal protection currently available, and relevant case studies that demonstrate the weight of the issue. This study will then make suggestions regarding the need for stronger platform accountability, improved cyber forensic capabilities, and digital literacy campaigns in order to create a safer and more inclusive digital space for women. While the provision of women's safety in cyberspace is a legal responsibility, it is also a legal precondition to achieving gender

ISSN: 2582-6433

justice and equal digital development for women in India.

Keywords: Cybercrime, Women, Technology, Information Technology Act, Digital Literacy

RESEARCH METHODOLOGY

This paper has taken a mixed-method research design, which comprises both qualitative and quantitative methods to research on increasing problem of cybercrime against women in India in the midst of the rapid technological development. This study is exploratory and descriptive in nature, it tries to find out common types of gendered cybercrime, their effectiveness in the current legal systems and offer suggestions on how this can be reformed. Secondary data collection will be conducted by using NCRB statistics, CERT-In reports, legal documents, but will be complemented with the primary data collection involving structured surveys and semi-structured interviews with victims, legal experts, and law enforcement authorities. Interviews and case studies will rely on a purposive sampling approach, whereas the stratified random sampling will guarantee demographic heterogeneity in case of responding to surveys. Quantitative data will be processed with the help of descriptive statistics and trend analysis, whereas qualitative data will be processed with the help of theme coding that will help reveal patterns in the experiences of victims and the mechanisms of the institutions. It is also a study that uses doctrinal legal analysis in the interpretation of statutory provisions, case law, and policy documents of cybercrime and digital gender justice. Ethical concerns such as informed consent and anonymity of the participants will be followed to the letter. Although the study admits the limitations of underreporting and regional differences in digital literacy, it will result in a comprehensive typology of cybercrimes against women and the identification of gaps in the legal and technological protection of India and, eventually, result in more inclusive and responsive policy frameworks.

RESEARCH GAP

Although there is an increasing number of studies and policy focus on cybercrime against women in India, there are still large gaps in research that obstruct a thorough comprehension of the problem. Current literature tends to place more importance on legal and statistical research and underrepresent real-world experiences of victims, especially those belonging to underrepresented groups of marginalized or rural groups. This translates to a poor understanding of the psychological, social and economic impact of cybercrime. Moreover,

ISSN: 2582-6433

legal discussion is often divided, and little attention is paid to how different laws, including the IT Act, IPC provisions, and the Digital Personal Data Protection Act, are interconnected or contain significant gaps, particularly in new spheres of the problem that abuses using deepfakes and the dissemination of images without the consent of the victim. Scrutiny on the implementation tools is also wanting such as; the capacity and responsiveness of cyber cells and law enforcement agencies. As well, little has been done to investigate the role of technology platforms in sustaining or reducing cybercrime, and little attention has been paid to algorithmic bias and content moderation as well as platform accountability. Most importantly, the existing studies tend to exclude intersectional and feminist lenses and do not consider the role of structural inequalities and patriarchal norms in the perpetration and response to cybercrime. The need to address these gaps is crucial in coming up with more inclusive, effective and gender-sensitive legal and policy interventions.

RESEARCH PROBLEM

Cybercrime against women in the context of the fast-paced technology of India has become a widespread and multifaceted context that both the law and the social structure are grappling with. Although digital platforms and higher internet access have led to a surge of online abuse, women experience targeted online forms of abuse, including cyberstalking and non-consensual image sharing in addition to deepfaking and cyberbullying. The legal frameworks in place, such as the Information Technology Act and other clauses of the Indian Penal Code, are usually ineffective in the gendered aspects of the crimes and thus the victims have minimal remedy and no effective protection. Furthermore, the vulnerability of the women in the cyberspace is aggravated by the absence of digital literacy, underreporting caused by stigma, and inconsistent reactions of law enforcement to the issue. This study attempts to critically discuss the intersection of gender, technology, and law, to establish the policy, enforcement, and awareness gaps that systemically contribute to the inability to redress and prevent cybercrime against women in India.

OBJECTIVE OF THE STUDY

- To determine and classify the most common varieties of cybercrime committed against women in India, such as cyberstalking, online harassment, image-based abuse, and deepfake abuse.
- To assess the socio-legal implication of cybercrime against women with expression on the psychological, social and economic effects.

ISSN: 2582-6433

- To determine how effective are current legal frameworks which include the Information Technology Act, Indian Penal Code, and Digital Personal Data Protection Act (2023) in ensuring the problem of gendered cybercrime is tackled.
- To examine the role of law enforcement agencies such as cyber cells in responding and preventing cybercrime on women.
- To find out how digital platforms and tech companies can be held responsible in facilitating or preventing cybercrime by their content policies and data governance policies.
- To define gaps and difficulties in policy implementation, victim support systems and judicial procedures in cybercrime against women.
- To make practical suggestions about how legal, technological, and educational interventions can be enhanced to enhance digital gender justice in India.

INTRODUCTION

The digital revolution in India has introduced revolutionary changes in the aspects of communication, business, education and government, making the nation a technological powerhouse in the world. But, this accelerated growth has come with major weaknesses, especially to females trying to negotiate the online frontier. The issue of cybercrime against women, including cyberstalking and online harassment, non-consent sharing of images and impersonation have become an urgent socio-legal issue of concern. Although there have been provisions in the law and reporting systems, the problem is still underrepresented because of the disjointed implementation, digital illiteracy, and institutionalized patriarchal conventions that tend to mute victims. This dissertation aims to discuss the complex aspects of cybercrime against women in India, its causes, effects and the effectiveness of existing laws. The main research questions that will be used in this research are: What are the most common types of cybercrime against women in India? What impact do socio-cultural factors have on redressal and reporting? What legal and policy mechanisms are there in place and how they compare with the best practices around the world? This research aims at identifying and classifying cybercrimes that occur against women, understanding the psychological and social effects, examining prevailing legislations and institutional reactions, and recommending practical suggestions on how to change that. This research is important because it narrates an interdisciplinary research, a combination of legal study, sociological evaluation as well as technological criticism to make informed policy and advocacy action. The scope will mainly

ISSN: 2582-6433

be limited to the Indian setting but comparative allusions will be made to international models to indicate gaps and opportunities. Lack of access to some kinds of law enforcement information and the dynamic nature of cybercrime is a limitation. Finally, this study will be able to advance the discussion of digital gender justice and beneficially contribute to creating safer and more inclusive online spaces to women.

LITERATURE REVIEW

Gender and technology nexus in India have created a menacing trend of cybercrimes committed against women, but the science of this phenomenon is still unequal and incomplete. Some studies have tried to deal with the phenomenon though gaps still exist in the victim-centered analysis, legal coherence, and platform accountability.

SCHOLARS

1. **Mishra and Rani (2014)**

   In their study discuss the prevalence, causes, and effects of cybercrime against women in India with a qualitative and quantitative approach. They also emphasize that due to gender discrimination and digital illiteracy, women are the most vulnerable to such crimes as cyberstalking, revenge porn, and identity theft. The other criticism by the authors is the inadequacy of government and civil society responses and the need to have stronger legal and educational frameworks.[1]

2. **Jiyauddin (2024)**

   The legal analysis developed by Jiyauddin is centered on the legal implication of cybercrime on women and considers it as an act of violation of privacy and dignity. He defines such crimes as common-cyber defamation, cybersex trafficking and phishing and criticizes the gaps in the enforcement of the law in India. Another bill that has been included in the article is Digital Personal Data Protection Act (2023), which is reported to protect personal data but still has certain shortcomings including exemptions provided to government agencies.[2]

3. **Rudra (2023)**

   In his geographic and sociological research, Rudra investigates the impact of cybercrime on women in various states of India with a focus on the influence of digital illiteracy and infrastructural inequality. She observes that online mistreatment has been

[1] https://www.ijnrd.org/papers/IJNRD2312232.pdf
[2] https://ijlr.iledu.in/wp-content/uploads/2024/10/V4I430.pdf

ISSN: 2582-6433

equated with violence particularly in places where the right to privacy is not well understood. The paper uses TRAI and Deloitte data to demonstrate that the higher the rate of internet penetration, the higher the level of cybercrime. Annotation: This article contains a valuable regional division and statistical context, but fails to legally analyze and is not interested in feminist theory.[3]

CASE LAWS

- *Shreya Singhal v. Union of India* (2015): It was a landmark case that declared the section 66A of the IT Act unconstitutional, and in the process reasserted the significance of free speech, but also cast doubt upon the limits of abuse on the Internet.[4]
- *State v. Mahender Singh Dahiya* (2011): The case was a landmark in identifying cyberstalking and the psychological damage it imposes, but there is a lack of sentencing and deterrence.[5]

TYPES OF CYBERCRIME TARGETING WOMEN IN INDIA

1. **Cyberstalking**

   Cyberstalking is unwanted and constant surveillance, texting, or any other digital communication that leads to fear or unhappiness.

   - **Modus Operandi:** Perpetrators stalk, harass or threaten women with the help of social media, emails, or even messaging apps.
   - **Effects:** The victims are frequently anxious, have sleeping disorders, and are socially withdrawn.
   - **Legal Provision:** The *IPC section 354D* is a criminal offense of stalking, whether online or not.

   Example: A woman gets hundreds of spam messages that are sent by a fictitious account that follows her whereabouts and actions. New accounts continue to pop up even when the user has been blocked.

2. **Online Harassment and Cyberbullying**

   This involves forwarding abusive, threatening or sexually explicit messages with an intention of humiliating or intimidating.

[3] https://www.iosrjournals.org/iosr-jhss/papers/Vol.28-Issue7/Ser-7/D2807072630.pdf
[4] https://indiankanoon.org/docfragment/110813550/?formInput=vague%20law
[5] https://www.casemine.com/judgement/in/5609af0ce4b014971141570e

ISSN: 2582-6433

- **Forms:** Trolling, hate speech, slut-shaming, body shaming and communal targeting.
- **Sources:** Instagram, Twitter, WhatsApp and anonymous forums.
- **Legal Provision:** *IPC Sections 509 and 504,* and *IT Act Section 66A* (striked down but nevertheless referred to in a few cases).

Example: Female journalists and activists are also prone to organized campaigns of abuse on the internet unsurprisingly when they present dissenting opinions.

3. **Revenge Porn and Non-Consensual Image Sharing**

This includes sending videos or intimate photos without permission, usually former partners or blackmailers.

- **Intent:** Intent to humiliate, coerce or extort.
- **Legal Provisions:** *IT Act Sections 66E, 67, and 67A; Section 354C* (voyeurism).
- **Issues:** Sites can take long to take down; victims experience social stigma.

Example: The ex-boyfriend of a woman leaks her personal photos on a pornographic site where she suffers emotional trauma and reputational harm.

4. **Cyber Defamation**

Posting deceitful or malevolent material over the internet to ruin the reputation of a woman.

- **Media:** Blogs, fake news articles, doctored pictures.
- **Legal Provision:** *IPC 500 (defamation), IT Act 66A.*
- **Impact:** Work and personal backlash, particularly in the case of famous people.

Example: A false post is made against a female teacher, who is suspended and ostracized by society.

5. **Phishing and Identity Theft**

Malicious efforts to gain access to confidential information or masquerade as another person on the Internet.

- **Objectives:** Bank information, Aadhaar number, social media accounts.
- **Legal Provisions:** The *Information Technology Act in Section 66C and 66D.*
- **Gendered Angle:** Women can be victims of emotionally manipulative scam.

Example: A fraudster pretends to be a friend of a woman and requests immediate payment through transfers in WhatsApp.

6. **Cybersex Trafficking and Grooming**

Luring, manipulating or coercing women into sexual exploitation through digital

 ISSN: 2582-6433

platforms.

- **Tactics:** Counfeit employment opportunity, modeling, or love tricks.
- **Legal Provision:** *IPC (Section 370 372), POCSO (when minors are involved) (Section 67B) (Information Technology).*
- **Global Concern:** It usually touches on cross-border networks and encrypted platforms.

Example: A modeling agency online approaches a woman, blackmails her back to take photos and then blackmails her to do so on webcam.

7. **Email Misrepresentation and Sextortion**

Manipulation or extortion of women through the use of fake email or hacked accounts.

- **Sextortion:** Blackmailing or threatening to publish personal materials unless the following are obtained.
- **Legal Provision:** *Section 66C, 66D and 67A of the IT Act.*
- **Effect:** Economic losses, mental trauma, exposure anxiety.

Example: A woman gets an email saying her webcam is hacked and that she needs to pay money in order to avoid the release of the video.

8. **Doxing**

Posting personal data (address, phone number, place of work) online, without permission.

- **Motive:** Harassment, intimidation or incitement to violence.
- **Legal Provision:** There is no particular law; includes privacy laws and defamation laws.
- **Effect:** Risks to physical and mental health.

Example: The personal information of a female activist is leaked after he/she addresses a controversial situation.

LEGAL FRAMEWORK AND POLICY MEASURES

Legal action against cybercrime against women in India is still developing, but still in a piecemeal and reactive nature. Although a number of laws have been put in place to curb the digital crime, they are usually not gender sensitive, consistent in enforcement, and technologically flexible. A systematic analysis is given below:

1. **Information Technology Act, 2000 (IT Act)**

The IT Act is India's primary legislation governing cyber activities. Key provisions

ISSN: 2582-6433

relevant to women include:

Section	Provision	Application to Women
66E	Violation of privacy through capturing or publishing images	Used in cases of voyeurism and revenge porn
67 & 67A	Publishing obscene or sexually explicit content	Applied in cases of non-consensual image sharing
66C & 66D	Identity theft and impersonation	Relevant in phishing, fake profiles, and sextortion

Limitations:

- Gender-neutral language does not concern the peculiarities of the female vulnerability.
- There is a low enforcement because there is no cyber forensic capability and digital literacy among law enforcement.

2. **Indian Penal Code (IPC)**

Several IPC provisions have been adapted to address online crimes:

Section	Provision	Cyber Relevance
354D	Stalking (including online)	Cyberstalking and persistent harassment
509	Insulting the modesty of a women	Online abuse, trolling, and sexual threats
500	Defamation	Cyber defamation and character assassination
292	Obscene material	Circulation of pornographic content involving women

Case Law Insight

1. **State vs. Mahesh Kumar (2018)[6]**

Court: Delhi High Court

Issue: Cyberstalking and procedural lapses in investigation

Citation: Criminal Appeal Nos. 1199/2018, 1022/2018, 560/2019

Background

The case dealt with several offenses such as robbery and murder in which Mahesh Kumar and others were accused. Nevertheless, its applicability to cybercrime lies in the process-related observations obtained in the course of the trial especially with regard to digital

[6] https://www.casemine.com/judgement/in/5f19198a4653d0726e3578c5

ISSN: 2582-6433

evidence and identification.

- The prosecution depended on the eyewitness of a sole witness (PW-2) and it was found that he had some inconsistencies in his testimony and therefore his testimony was not credible.
- There was no identification of the accused Mahesh Kumar during the Test Identification Parade (TIP) only to identify him in court, which questioned the procedural fairness.
- It was claimed that the TIP had been violated and that the in court identification was affected by prior exposure.

Legal Findings

- The Delhi High court supported the conviction on the basis of corroborated testimony and circumstantial evidence.
- Nevertheless, it also identified some problems with delays in the process, particularly with processing digital evidence and a weak TIP.
- The court raised concerns about the issue of timely and technologically viable investigation procedures particularly in matters of digital footprints.

Relevance to Cybercrime to Women

Although it is not a case of direct cyberstalking, it is worth noting in the judgment:

- Procedural integrity in cybercrime trials.
- This is due to the difficulties of tracking down perpetrators in the case of digital anonymity.
- Capacity-building of cyber forensic investigation.

2. XYZ Vs. Facebook Inc. (2021)[7]

Court: Delhi High Court

Issue: Jurisdictional challenges in prosecuting global tech platforms

Context: Privacy violations and platform accountability under Indian law

Background

The case developed as a result of the challenge of the revised 2021 privacy policy of Facebook and WhatsApp that supposedly infringed upon the rights of users and promoted the abuse of personal information. Competition Commission of India (CCI) has embarked on a probe into the possibility of abuse of dominance.

[7] https://www.scconline.com/blog/post/2022/08/27/delhi-high-court-upholds-competition-commission-india-direction-investigation-anticompetitive-whatsapp-facebook-privacy-policy-terms-of-service-competition-law-overlapping-jurisdiction-legalnews-legal/

ISSN: 2582-6433

- Facebook and WhatsApp challenged the competence of CCI, saying that the case was in the Supreme Court already on constitutional basis (privacy under Article 21).
- Delhi High Court was requested to determine whether the concurrent existence of parallel proceedings by CCI and constitutional courts was possible.

Legal Findings

- The court affirmed the jurisdiction of the CCI and explained that the competition law and constitutional law exist in different fields.
- It decided that the overlap of jurisdiction does not cancel parallel investigation particularly where the nature of inquiry varies (privacy vs. dominance of the market).
- The case strengthened the doctrine that technological sites functioning in India are liable to Indian regulatory examination, in spite of being based outside of India.

Relevance to Cybercrime Against Women

- Sets a precedent of holding global platforms responsible of abuse of content and data.
- Paves the way to regulation of instances of revenge porn, doxing, and non-consent data sharing.
- Outlines the jurisdictional challenges facing the prosecution of digital crimes across the borders.

TRENDS AND STATISTICS

Along with the digital growth of India, there has been an alarming incidence of cybercrime against women. According to the National Crime Records Bureau (NCRB) and investigations by independent researchers, there has been a steep incline in such crimes highlighting the extent of the issue and a structural inefficiency in addressing the issue.

1. **Rising Incidence: A 28% Surge (2019-2021)**

   NCRB statistics as well as academic sources indicate:[8]

   - There was an increase of **more than 28%** in cybercrime against women in 2019-2021.

[8] https://www.iosrjournals.org/iosr-jhss/papers/Vol.28-Issue7/Ser-7/D2807072630.pdf

ISSN: 2582-6433

- In 2019 alone witnessed a **63.5%** increase in cybercrime cases, most of them against women.[9]
- This growth is seen to be due to the higher penetration of internet, the use of smartphones, and also as a result of social media use, particularly among the young women.

Interpretation: This wave is not only an increase in reporting, but also indicates an increase in the complexity of digital abuse: not only impersonation and sextortion, but also cyberstalking and revenge porn.

2. **One Woman Targeted Every Second**

One of the most notable statistics that have been highlighted in the literature[10] in the recent past indicates that one woman becomes victims of cybercrime every one second in India. Although the number is projected off of larger crime rates and usage trends on digital platforms, it demonstrates:

- The ubiquity of violence on the internet based on gender.
- The anonymity of most crimes, which happen in the privacy of the digital realm and are mostly undetected.

Interpretation: This indicator is not only a numerical alarm, but also a mirror of the normalization and lack of attention to the digital abuse in the real world.

3. **Underreporting: The Silent Epidemic**

However, **most cybercrimes against women remain unreported**, although the cases have increased. Key reasons include:

- **Social stigma:** The victims are afraid of being blamed or shamed, more so when dealing with intimate material.
- **Digital illiteracy:** The women, especially in the rural regions, do not know their rights and are not aware how to complain.
- **Mistrust toward police:** Victims can expect to face sensitive treatment, stalling, or even rejection of a complaint.

Supporting Data: In Delhi, as an example, the physical crimes against women decreased during lockdowns, but cybercrime **increased by 55% in 2020**, but only a small percentage of them were registered.[11]

[9] https://timesofindia.indiatimes.com/india/ncrb-crime-data-2019-cases-registered-up-1-6-crimes-against-women-rise-7-3-cyber-crimes-jump-63-5/articleshow/78394087.cms
[10] https://www.iosrjournals.org/iosr-jhss/papers/Vol.28-Issue7/Ser-7/D2807072630.pdf
[11] https://www.dnaindia.com/india/report-cyber-crime-increases-dip-in-crimes-against-women-ncrb-data-2911431

ISSN: 2582-6433

ROOT CAUSES OF VULNERABILITY TO CYBERCRIME AMONG WOMEN

Although India is a fast-growing digital society, the women are still disproportionately susceptible to cybercrime. This weakness is not caused by chance, it is the result of a complicated interaction of structural, cultural and technological influences that promote online inequality and undermine online safety.

1. **Digital Illiteracy and Technological Marginalization**

   Digital illiteracy is the inability to use the Internet safely and have skills, awareness, and confidence to act within online platforms. Though the internet penetration has gone up, most women, particularly in rural and semi urban regions, are not well versed in cyber security, privacy settings, and secure digital practices. **Contributing Factors**

   - **Gendered access to technology:** Digital devices and internet use in most families is controlled by men.
   - **ICT training:** ICT training is not commonly gender-integrative, and women are not being considered in digital literacy programs.
   - **Language issues:** The majority of available cybersecurity content is in English and excludes non-English speaking women.

   Impact

   - Females are more vulnerable to phishing, impersonation and data attacks.
   - They can be effortlessly targeted by sextortion and identity theft because they share personal information without knowing.

   According to the IOSR Journal postulates that women are very vulnerable to cyberspace due to the absence of computer and internet literacy.

2. **Patriarchal Norms and Social Stigma**

   The patriarchal culture in India is extremely strong and thus influences the perception and approach towards cybercrime. When women become victims of online abuse, they are blamed, shamed or even silenced- particularly when the offense is sexual content or personal relationships.

   Contributing Factors

   - **Victim-blaming:** The society tends to ask the woman about her behavior, how she dresses or on the internet instead of what the perpetrator does.
   - **The fear of being labeled:** Women do not report crimes because they would ruin the family reputation or work opportunities.

ISSN: 2582-6433

- **The insensitivity of institutions:** Law enforcement and courts can become trivial to digital abuse or gender-unresponsive.

Impact

- Majority of the instances remain unreported and culprits operate at will.
- The victims experience psychological trauma, seclusion and mistrust of the legal system over the long run.

Lack of awareness of their legal rights and lack of trust in law enforcement to effectively investigate cyber crimes has been mentioned in the IJLR study as to why many victims do not know their legal rights and do not trust the law enforcement to effectively investigate cyber offenses.

3. **Tech Platform Gaps and Corporate Apathy**

In most cases, social media platforms and tech companies do not respond to gendered cybercrime effectively, timely and transparently. Their moderation systems and disclosure policies are not user-friendly to the safety of women.

Contributing Factors

- **Sluggish content removals**: The posts or pictures containing damaging content stay in the search engine days more, which increases harm.
- **Cloudy policies:** Sites do not often reveal the processes of decision-making or the reasons behind some content being permitted.
- **Inability to be local:** Global portals might not know the local culture or legal requirements in India.

Impact

- Women are re-exposed to the abuse, even after reporting it.
- Attackers use the loopholes of the platforms to open new accounts or avoid bans.

The increasing access to smartphones and social media has further facilitated the exploitation of women by those committing these atrocities as noted in the IJNRD paper with platforms not acting in their responsibilities.

JUDICIAL INTERPRETATION

1. **Vinupriya Case (2016) – Tamil Nadu**

- **Facts:** A 21-year old student, Vinupriya, committed suicide after nude photos of her were morph-ed and put online in Facebook. Police were slow in responding to the complaint of her family.

ISSN: 2582-6433

- **Legal Consequence:** The case caused explosions in the society and resulted in quicker response of the cybercrime cells in Tamil Nadu.
- **Significance:** Stated the importance of immediate response and responsibility of a platform in cases of image-based abuse.[12]

2. **Shreya Singhal v. Union of India (2015) – Supreme Court**
    - **Issue:** Constitutionality of Section 66A of the IT Act, accusing messages that are offensive online.
    - **Judgement:** The Supreme Court overturned Section 66A as both vague and in violation of the free speech.
    - **Impact on women**: In as much as this was a victory in civil liberties, the repeal fails to provide a means of prosecuting anti-social acts of harassment, providing a regulatory loophole to gendered violence.[13]
3. **XYZ v. Facebook Inc. (2021) – Delhi High Court**
    - **Issue:** Legal issue regarding the privacy policy and the privacy of Facebook and WhatsApp.
    - **Judgement:** The court did not overturn the power of Competition Commission of India to probe, which means that India has a regulatory jurisdiction over international platforms.
    - **Relevance:** Enhanced the argument of the platform responsibility in situations where there is abuse of female data and pictures.[14]
4. **State v. Mahesh Kumar (2018) – Delhi High Court**
    - **Issue:** The problem of lapses in the process of identification and digital evidence management.
    - **Judgement:** Affirmance, but the court denounced time wastage and the absence of forensic excellence.
    - **Relevance:** Highlighted the necessity of cybercrime dedicated investigation guidelines and trained staff.[15]
5. **Sabu Mathew George v. Union of India (2018) – Supreme Court**
    - **Issue:** Internet advertising of sex-selective abortions.

[12] https://legaldesire.com/laws-to-safeguard-women-against-cyber-crime-in-india/
[13] https://indiankanoon.org/docfragment/110813550/?formInput=vague%20law
[14] https://www.scconline.com/blog/post/2022/08/27/delhi-high-court-upholds-competition-commission-india-direction-investigation-anticompetitive-whatsapp-facebook-privacy-policy-terms-of-service-competition-law-overlapping-jurisdiction-legalnews-legal/
[15]https://www.casemine.com/judgement/in/5f19198a4653d0726e3578c5

ISSN: 2582-6433

- **Judgement:** Asked directed search engine to bar such material and established a precedent of proactive regulation of the internet.
- **Relevance:** Evidence of judicial interest in interfering in online content regulation in the defense of the rights of women.[16]

6. **Prajakta v. State of Maharashtra (2020) – Bombay High Court**
    - **Facts:** A woman was blackmailed by means of intimate pictures published during the course of a consensual relationship.
    - **Judgement:** The court focused on the issue of consent and privacy and sentenced to immediate takedown and arrest of the defendant.
    - **Relevance:** Strengthened the principle of the right to digital dignity and the necessity of expediency in judicial actions.

ANALYSIS AND DISCUSSION

The Indian response to cybercrime on women is still decentralized and reactive, although the problem of digital gender-based violence is becoming increasingly urgent. Even the major laws, which are Information Technology Act, 2000 and some provisions in the Indian Penal Code (IPC), provide only partial protection as they tend to be written gender-neutrally and outdated frameworks. As an example, in as much as Sections 66E, 67, and 67A of the IT Act criminalize privacy breach and obscene content, it does not cover the subtle harm women suffer when sharing pictures without their consent or cyberstalking. In line with this, IPC Section 354D (stalking), 509 (insulting modesty), and 500 (defamation) are applied to digital abuse cases, however, they were created to address offline offenses which have created an interpretative grey area and delays in the process. Such a loophole can be seen in such a case as *State v. Mahesh Kumar (2018)*, Where the Delhi high court affirmed conviction but condemned the absence of forensic rigor and delay in identification procedures. In contrast, *XYZ v. Facebook Inc. (2021)* a positive change was observed where the Delhi High Court held that India had a jurisdiction over the international platforms which enhanced regulatory sovereignty in the digital privacy issues.

Law jurisdictions such as the United Kingdom and the United States have been more proactive and women-sensitive in their legal systems comparatively. Criminalization of non-consent pornography as well as platform responsibility is specifically enshrined in the *Revenge Porn*

[16] https://www.supremecourtcases.com/sabu-mathew-george-v-union-of-india-ors/

ISSN: 2582-6433

Criminalization Act (2015) and the *Online Safety Bill (2023)* of the UK, whereas a combination of civil and criminal solutions is undertaken in the US by the revenge porn statutes on the state level and the nationwide initiatives such as the Cyber Civil Rights Initiative (CCRI). These models put the focus on victim-driven strategies, transparency of the platform, and rapid redressal-that is mostly lacking in the enforcement environment in India. Besides, the rights-based framework of the European Union, which is based on the General Data Protection Regulation (GDPR) and the Digital Services Act (2022) requires the user consent, protection of data, and enforcement across the borders, which provides structural protections that are only partially reproduced in the Digital Personal Data Protection Act, 2023 of India.

The Indian judicial interpretation has indicated improvement especially in the question of digital harm as infringement of fundamental rights. In *Shreya Singhal v. Union of India, (2015)* Supreme Court ruled in favor of free speech when it ruled Section 66A of the IT Act (1996) unconstitutional and vague. This ruling unintentionally, however, eliminated a law that has frequently been used to prosecute online harassment, which left a regulatory gap. Courts have since extrapolated IPC to address cyber crimes, except that a specific cybercrime act does not exist to address gendered harm, which makes its application patchy. In *Sabu Mathew George v. Union of India (2018),* judicial activism is observed in which the Supreme Court ordered search engines to stop sex-selective ads, is indicative of the desire to interfere with the digital regulation. However, such interventions will just be on paper unless legislative follow-through and institutional capacity-building are in place.

Overall, the legislation and judicial reaction to cybercrime against women in India are still developing and in need of the coherence, specificity, and orientation to the victim as provided in the global models. In order to overcome this loophole, it is imperative to consider a statutory change as well as a cultural change, platform responsibility, and effective enforcement systems. To protect the digital dignity of women in an ever-connected world, a consolidated and gender-sensitive cybercrime model must be in place with support of judicial clarity and comparative learning of the law.

CONCLUSION

Communication, trade and information access in India have been altered by the digital revolution - however it has also produced space in which gendered violence may be practiced. This study has taken a critical appraisal of the nature, extent, and legal action to cybercrime

ISSN: 2582-6433

against women, which has shown a disastrous lack of institutional readiness with technological advancement. The paper confirms that cybercrime against women is not the technical or legal problem only, but the socio-cultural crisis based on patriarchal norms, illiteracy with the digital environment, and the indifference of the system.

The aim of the research which was to determine the sufficiency of the Indian legal system, judicial interpretation, and global best practices have all been covered. The review of the statutory measures like the Information Technology Act, 2000, Indian Penal Code, and the Digital Personal Data Protection Act, 2023 shows that the Indian legal framework is still disjointed, gender-neutral and lacks the capability to contain the subtle harms that women suffer on the internet. Judicial interpretations, though becoming more enlightened, are limited by the laggardly procedures, absence of cyber forensic infrastructure and lack of law enforcement follow through case laws *Shreya Singhal v. Union of India, XYZ v. Facebook Inc*., and *Prajakta v. State of Maharashtra* represent the possibilities and constraints of judicial activism in developing digital justice. These jurisdictions provide examples of gender-specific laws, platform responsibility, and systemic support of victims that India can incorporate into its socio-legal framework.