

Cyber Crimes Against Women in India: An Analysis of Emerging Trends

¹Ms. Dilpreet Kaur, ²Dr. Mohleen Kaur

¹LL.M. student, ²Assistant Professor

¹²University School of Law

¹²SGGSWU, Fatehgarh Sahib, Punjab

Abstract—In a short time, information technology has evolved and now the internet has been widely adopted, changing how people communicate, conduct business, govern, and interact in society around the globe. Technological development has given rise to numerous opportunities but also to new and different types of criminal activity, which are grouped together under the term cyber crimes. With smartphones, social platforms, digital payments and online services becoming more pervasive in Indian society, the scope of cyber crimes is growing at a rapid pace. Women have become one of the most vulnerable groups in cyberspace, exposed to cyber stalking, cyber harassment, cyber bullying, identity theft, revenge pornography and the dissemination of intimate content without consent and the morphing of images, doxxing, impersonation and dissemination of content. These crimes offend not only privacy and dignity, but also have psychological, social and economic implications. This paper reviews cyber crime in India in an analytical way and highlights the emerging trend of cyber crimes against women in India. It examines the legal framework for cyber offences, judicial reactions to cyber offences, practical obstacles and problems in the implementation of the legal framework and existing laws and how effective they are. The study states that there is a strong legal framework and technology skills and also public awareness of the issue, but there is a need to have more effective mechanisms and gender sensitisation to provide better protection of women in cyberspace.

Index Terms—Cyber Crime, Women Cyber Stalking, Cyber Bullying, Revenge Pornography

I. Introduction

The 21st century has seen unprecedented innovation that has changed the way we communicate, do business, find information and engage in social life. The internet has grown into an essential component of everyday life, enabling billions of people to interact and connect through digital channels, and connecting people and processes in ways that were unimaginable until recently. India, home to one of the world's largest internet user base, has seen tremendous progress in digital growth with the introduction of various initiatives such as digital governance, e-commerce, electronic payment systems and internet usage. These advancements have also brought about numerous positive results, but it has also opened the door to crime committed online. Cyber crime is one of the most severe problems which modern laws have to deal with.

A crime involving use of computers, digital devices, networks, or communication technologies as a tool, target, or setting for a crime. Cyber crimes are often cross-border, and can be perpetrated anonymously, making them difficult to detect and prosecute. Advances in technology, increased accessibility and the world-spanning reach of cyberspace have given criminals the opportunity to carry out a variety of illegal acts,

including financial fraud, hacking, identity theft, cyber terrorism, and online harassment.¹ The increasing reliance on digital technology has thus exacerbated the threat of cyber risks to individuals and institutions.

The different types of cyberscrime, in particular crimes against women, have garnered particular attention. The digital world, which affords opportunities for communication and empowerment, is also a context in which women often suffer from harassment, abuse, intimidation and exploitation. Cyber victimization is being used to target women in many ways and increasingly via social media platforms, messaging applications, online forums and digital communication networks. Many times, the anonymity of the internet gives impetus to the criminal, allowing him to behave in a manner which he may not have done in a “real world” situation. As a result, gender-based violence and discrimination have become an important location in cyberspace.

Cyber crimes targeting women come in many different shapes and forms and can constantly be adapted and developed with the advancement of technology. Cyber stalking is a pattern of threatening or harassing a person through electronic communication. Abusive messages, threats, defamatory content, and targeted campaigns of intimidation are all potential forms of online harassment. Women are often the target of cyber bullying, especially on social media, which brings them psychological stress and humiliation. Offenders can use impersonation and identity theft to access personal information, and with morphing of images and the spread of intimate content without consent, there are serious implications for privacy and dignity.² As revenge pornography and the non-consensual sharing of private photos are becoming commonplace, concerns for women's safety in digital environments are growing to new heights.

The consequences of cyber crimes against women do not just stop at the financial or reputational damages. Common feelings of victims are anxiety, depression, social isolation, emotional trauma and fear for personal safety. Online abuse can also impact on professional life, learning and social connections. The psychological effects can be especially harsh as digital content can end up being available for an extended time and could be shared quickly with a wide audience. Cyber offences are different than many traditional forms of harassment in that they persist and can be seen online.³

These problems have been realised and India has put in place several legislations to combat cyber crime and safeguard the individuals against digital victimisation. The main legislation relating to cyber offences and electronic communications is the Information Technology Act, 2000. The Act makes it illegal to use or cause to be used any unauthorized computer, computer system, or network; any account without authorization; impersonation; privacy invasions; and the dissemination of obscene material in electronic transmission.⁴

¹ Talwant Singh, *Cyber Law and Information Technology* 12 (Allahabad Law Agency, Faridabad, 6th edn., 2022).

² Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* 145 (Lexis Nexis, New Delhi, 2012).

³ David Wall, *Cybercrime: The Transformation of Crime in the Information Age* 76 (Polity Press, Cambridge, 2007).

⁴ The Information Technology Act, 2000 (Act 21 of 2000), ss. 66C, 66D, 66E, 67 and 67A.

Further, Bharatiya Nyaya Sanhita, 2023 covers offences like stalking, sexual harassment, criminal intimidation and dissemination of obscene content. Further, the Digital Personal Data Protection Act, 2023 has enhanced the legal protection framework regarding privacy and data protection.

Judicial institutions have also played an important role in shaping cyber law jurisprudence in India. The role of judiciary has also been crucial in developing cyber law jurisprudence in India. In the age of the internet, privacy, dignity, and freedom of expression have all become increasingly important to courts. Judicial rulings on harassment on-line, cyber-stalking, identity theft, and privacy issues have helped shape law principles of cyberspace. In parallel, courts have recognised the challenges of cyber crime investigation and prosecution, especially in relation to the complexity of technology and jurisdictional issues.⁵

Though there have been legislative and judicial advances, there are still obstacles to overcome. A lack of awareness and confidence in enforcement mechanisms, social stigma, fear of retaliation, and the failure to report many incidents are continuing to prevent the reporting of many cyber crimes against women. Whether it's for finding the criminals, preserving digital evidence or dealing with crimes that span state lines, investigative agencies often struggle. Technology changes quickly relative to legal and institutional responses, resulting in gaps in regulation and enforcement. Furthermore, the adoption of fake accounts, encrypted messaging and new technologies is causing challenges within the field of good cyber governance.

An escalating trend of cyber offences against women has caused great concern about digital rights, gender justice and State duty to provide safe online environments. The problem is not only one of criminal law enforcement but also one of developing a legal and institutional structure that can reconcile technology with respect of the fundamental rights. With the ever growing digitization of infrastructure and its services in India, urgent need of efficient cyber law mechanisms becomes more and more important.

This paper attempts to critically analyse the cyber crime phenomenon in India focusing on crimes against women. It examines the nature and development of cyber offences, reviews the current formal structure of the law, explores relevant judicial decisions, looks at practical issues and recommends strengthening measures to protect women in cyberspace. The study concludes that although India has come a long way in the formulation of cyber laws, the laws need to be more comprehensive and sensitive to gender to respond to the changing face of digital victimisation and provide access to justice for women.

II. Concept and Growth of Cyber Crime in India

Cyber crime has become a major legal and social problem in today's digital era. The Internet's proliferation, ubiquity of smart phones, reliance on digital payment systems, and the rise of social media have

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

changed the face of crime around the globe. In India, technological innovation has been key to the flourishing of economic development, digital governance, financial inclusion, and social communication. Meanwhile, the growing digitalization of the society has also provided new opportunities to the offenders to use technologies in an illegal manner. Cyber crime has thus grown from a technological problem to a significant threat to everyone from individuals to businesses, financial institutions and governmental bodies.

Cyber crime is a general term used to describe crimes in which computers, electronic devices, communication systems or electronic systems are involved as either a crime tool, a crime target, or a crime environment. Unlike traditional crimes which are generally restricted to particular geographic areas, cyber crimes can be committed from anywhere in the world. The lawless quality of cyberspace, and the anonymity offered by digital technologies, poses special challenges to law enforcement and legal systems.⁶

The proliferation of cyber crime in India goes hand-in-hand with the incredible growth of Internet use. Digital connectivity in India has witnessed a dramatic change in the past 2 decades with the proliferation of affordable smartphones, low cost internet, expansion of broadband infrastructure and digital inclusion efforts by the Government of India. Citizens have been pushed to use online services in different fields like banking, education, governance, health and commerce through various programmes like Digital India. These advances have brought significant social and economic advantages but have also raised the risk profile of individuals and institutions to cyber threats. With the increasing number of activities that are now available online, there are more chances for cyber criminals to thrive.

Cyber crime is a broad range of crimes. These include hacking, computer system intrusion, identity theft, phishing, financial fraud via the Internet, cyber terrorism, data theft, cyber stalking, cyber bullying, sending inappropriate information, ransomware attack, and online impersonation.⁷ Cyber offences are diverse because digital technologies are diverse and cyber criminals can quickly adjust to new technologies. Cyber crime is not like a traditional crime, it can be complex with advanced technical means that may not be easily seen by the victim nor by investigators.

The pace of Cyber Fraud and Online Financial crimes in India is one of the most outstanding trends. The rapid growth of digital payments, online banking, Unified Payments Interface (UPI) transactions and e-commerce platforms has greatly increased the possibility of financial cybercrime. Phishing tools and techniques, fraudulent links, fake websites and deceptive communications are commonly used for criminals to trick unsuspecting users into providing sensitive financial data. The frauds involving identity theft and

⁶ Talwant Singh, *Cyber Law and Information Technology* 20 (Allahabad Law Agency, Faridabad, 6th edn., 2022).

⁷ *Supra* note 4, ss. 43, 65, 66, 66C, 66D, 66E, 67 and 67A.

impersonation are becoming commonplace and causing significant financial damages for individuals and institutions.⁸

Social media platforms have also contributed to the changing landscape of cyber crime. These platforms provide a means of communication and information sharing, but have now become a breeding ground for different forms of abuse and exploitation. The use of fake profiles, online harassment, misinformation, cyber bullying and sharing of private information are becoming commonplace. When information is spread through social media, the speed at which it can be sent across makes the impact of the cyber offence much greater and often makes it hard to restrict the spread of harmful information once it has been distributed.

With the onset of the COVID-19 pandemic, the rate of cyber crimes in India has further increased. As the world went to a virtual office and digital school, it went to digital health, entertainment and communication. As the world moved to remote work and social distancing, so did people's reliance on digital platforms for work, education, healthcare, entertainment and communication. This quick change opened up new opportunities for cyber criminals, to which they promptly took advantage. There were significant spikes in the number of reports of phishing attacks, fraudulent health-related communication, online scams and unauthorized access to digital systems during this period. The pandemic showed us how technology dependence can lead to innovation and increased cyber risks for people.⁹ The pandemic highlights the opportunities for innovation, while exposing people to greater cyber risks due to technology dependence.

One thing that is very alarming about Cyber crime is its effect on the weak sections of society such as women and children. New opportunities for harassment, intimidation, exploitation and abuse against these groups through digital technologies. Women are often subjected to cyber stalking, threats online, posting of false images, sharing of sexual material without consent, and harassing campaigns. Cyber bullying, online grooming and other digital exploitation are becoming more commonplace with children. The developments highlight the importance of specific legal and institutional responses that are able to deal with the specific nature of cyber victimization.

Advancements in technology like AI, Machine learning, cloud computing and encrypted communication systems have also been a factor in the evolution of cyber crime. These technologies have great advantages but also have the potential to be used for illegal purposes. AI can create fake content, impersonate videos and advanced phishing attacks. Encrypted communication systems can also make it difficult to investigate because

⁸ Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* 160 (Lexis Nexis, New Delhi, 2012).

⁹ Pavan Duggal, *Cyber Law in India* 88 (Saakshar Law Publications, New Delhi, 2021).

of the fact that it is not possible to access digital evidence. Technology constantly evolves and so must the laws and regulations that govern it.¹⁰

India has seen an increase in cyber crime and has introduced the Information Technology Act, 2000, as the main law related to electronic communications and cyber crimes. The Act was enacted to acknowledge electronic records and electronic signatures and to establish penalties for a number of cyber crimes. Later revisions added to the act to cover new technological issues. Moreover, the Bharatiya Nyaya Sanhita, 2023, which enumerates offences related to stalking, criminal intimidation, obscenity and cheating through electronic means, has added to the cyber law provisions.¹¹

Cyber crime is an extremely difficult crime to prevent and prosecute, despite the presence of a law. Police authorities often face challenges in obtaining a trace on an offender, in preserving digital evidence, and in multi-state investigations. Effective enforcement is sometimes difficult because of technical complexity, lack of specialized personnel, and the speed of change in technology. Additionally, numerous victims don't know what remedies are available to them or are afraid to report cyber offenses for reasons of embarrassment, fear, and/or inaction because of the lack of trust in investigative procedures.

Thus, the rise of cyber crime in India is indicative of the opportunities and challenges that come with technological advancements. The need for cyber security and legal regulation is more important as digital technology becomes more prevalent in daily life. The development of the laws is only the first step in a good response, which also needs technical capabilities, awareness-raising, institutional cooperation, and international collaboration. To create a strategy that can protect people and foster a safe cyber world, it is important to understand what cyber crime is and how it develops.

It is important to put crimes against women into a broader context of the increasing prevalence of cyber offences. Digital victimization of women is a specific form of electronic victimization, and frequently consists of a mix of technology abuse and gender-based discrimination and violence. Such offences involve different legal and social challenges and need to be addressed differently from the perspective of cyber law.

III. Cyber Crimes Against Women: Nature, Forms and Emerging Trends

Digital technology has had unprecedented opportunities for communication, education, employment and social interaction as a result of its rapid expansion. Meanwhile, it is created new opportunities for gender based victimisation and abuse. Women are becoming more and more active on the internet via social media, professional networking, e-commerce, knowledge sharing and communication apps. This involvement has helped to improve the opportunities for women to be empowered and to express themselves but has also

¹⁰ David Wall, *Cybercrime: The Transformation of Crime in the Information Age* 102 (Polity Press, Cambridge, 2007).

¹¹ Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 75, 76, 78, 79, 294 and 351.

brought them into contact with several different types of cybercrime that are directed at their exploitation, intimidation, harassment or humiliation. Cyber crimes against women are now a major issue as they are a blend of traditional gender discrimination and the special features of cyber, which are anonymity, speed, permanence and global reach.

Cyber stalking is one of the most common types of cybercrime that can be committed against women. Cyber stalking is defined as the intentional use of electronic communication technology to monitor, contact, threaten, harass or intimidate another person. However, cyber stalking is different from the old fashioned stalking, and it allows the perpetrators to keep tabs on their victims' social media profiles, emails, messaging apps and other online accounts without being physically in the same vicinity. Persistent unwanted communication and surveillance can cause victims to feel fear, anxiety and psychological distress. A cyber stalker might gather information, track what people are doing online, or persist in making contact in spite of the person's refusal to allow such contact.¹² Cyber stalking can have serious psychological effects as victims may feel they are constantly being monitored and attacked.

Another common type of cyber victimization is online harassment. Social media and communication networks are often sources of abusive messages, sexually explicit comments, threats of violence, defamatory statements or offensive content sent to women. This harassment could be based on gender, occupation, political views, social position or public presence. Women journalists, activists, politicians and public figures are especially at risk of coordinated campaigns of online abuse. Digital platforms provide anonymity which can encourage a more extreme form of behaviour that may not happen in real life.¹³

Cyber-bullying is an increasingly serious issue, especially for younger women and girls. Cyber bullying is when someone is repeatedly harassed, intimidated, embarrassed or humiliated using digital technology. Online abuse can be constant, occur to many people in a short time and is not the typical bullying. Emotional symptoms include emotional distress, social isolation, depression and decreased self-esteem in victims. The use of social networking has increased the impact of cyber bullying and its influence throughout society, making it one of the biggest threats to women's safety in the online world.

Revenge pornography is one of the most damaging cybercrimes faced by women today, and it occurs when someone uses an intimate image of a victim without their consent. This offense is committed when someone posts or shares intimate photos, videos or private information about someone without that person's permission. The material is often shared by former partners wanting revenge, humiliation or coercion. This can have serious repercussions, such as embarrassment, emotional harm, isolation, career difficulties, and mental

¹² *Supra* note 4, ss. 66E and 72.

¹³ Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* 174 (LexisNexis, New Delhi, 2012).

anguish.¹⁴ The offense that is committed using the digital medium can be difficult to completely disappear once it has spread, continuing the victim's suffering.

Similar to revenge porn is the image morphing. Technological tools can be used by perpetrators to alter and make fake or pornographic pictures of women. The distorted photos are often shared via social media, messaging apps, or websites, usually to embarrass or blackmail the victim. One of the more extreme examples of an invasion of dignity and privacy is morphing, which can lead to the creation of an impression that harms the reputation of an individual and/or their organisation. As AI has progressed, image manipulation technology has also become more sophisticated, and detecting and preventing have become more difficult.

Deepfake technology has ushered in new forms of cyber victimization. Deepfakes are synthetic, AI-generated audio, video, or imagery that appears realistic but is in-factual. Women are especially targeted by deepfake porn – when their faces are digitally grafted onto sexually explicit material without their consent.¹⁵ This can be used for harassment, extortion, reputation downfall or entertainment. With the growing prevalence of deepfake technology, there are serious issues of privacy, consent, and digital safety to consider, especially for women who actively engage with the online community.

Online impersonation and identity theft are other types of cyber crime that impact women. Offenders might establish fake social media accounts, use personal pictures or pretend to be females for scams or malicious intents. Such activities can lead to damage to the reputation, monetary loss, harassment or social embarrassment. Impersonation can be a huge issue as it allows the offender to use the victim's identity to perpetrate acts of impersonation while leaving the victim's identity hidden. Many times, victims find out about fake profiles when a significant amount of damage has been done.

In digital spaces, another key danger has emerged, known as Doxxing. Doxxing means revealing an individual's private address, phone number, place of work, financial information, financial information, or family information online without their consent. The goal is to frighten, threaten or subject the victim to harassment and/or physical violence. Women involved in public debate, activism, journalism or political activity are especially targets of such attacks. The release of personal information can create risks to victims online and off, making the difference between victimisation offline and online less distinct.¹⁶

Online sexual harassment is a wider concept that includes many types of damaging behaviours towards women that are done via electronic methods. Some examples of this include sexually explicit messages, sexually explicit pictures, threats of sexual violence, unwanted sexual advances, and repeated unwanted

¹⁴ *Supra* note 4, ss. 67 and 67A.

¹⁵ Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 85 (Harvard University Press, Cambridge, Massachusetts, 2018).

¹⁶ Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity and Love in the Digital Age* 120 (W.W. Norton & Company, New York, 2022).

advances. This not only brings the dignity of the person under question into disrepute but also dissuades women from engaging in digital spaces. Online sexual harassment is not new and reflects the ongoing gender disparities in the technology landscape, and the importance of robust legal responses.

There has also been a sharp rise in financial cyber-crimes against women. Many women and those who are less technologically savvy end up getting targeted in many ways for fraudulent investment schemes, online scams, phishing attacks, and deceptive financial transactions. Emotional vulnerability, social engineering and trust are common methods used to trick people. Such crimes show that cyber victimisation affects more than just privacy and dignity issues; they also have significant economic impacts.

As social media develops, it has increasingly made women targets for cyber crime attacks. Digital platforms allow the sharing of personal information, photos, views and experiences, which can provide opportunities for abuse by offenders. Personal information is widely available and can enable stalking and blackmail, as well as impersonation, and other types of cyber victimisation. Social media platforms focus on user engagement and visibility, which can inadvertently drive the spread of harmful content and abusive practices.

The implications of cyber crimes committed against women are not just for the individual victim, but also issues of gender equality and digital rights. The anxiety of being abused online can lead women to avoid public discussion, employment, voicing opinions, and using digital technologies. As a result, cyber crime has also a socio-political dimension for democratic participation, freedom of expression and social inclusion. The challenge calls for a legal, technological, educational, and institutional response that is comprehensive enough to tackle the root causes and effects of digital victimization.

More and more, cyber crimes against women are becoming commonplace and complex, highlighting the need for strong legal frameworks and enforcement. It is important to define the nature and shape of these offences to assess the need for reform of the current legislation. The next step of analysis, therefore, is to examine the current legal regime for cyber offences against women in India, and how well the laws are functioning in an increasingly digital environment.

IV. Legal Framework in India for Protection of Women in Cyberspace

As cyber crimes against women are on the rise, the Indian legal system has been compelled to devise mechanisms to tackle new types of digital victimization. The legal regime for cyber offences in India is not based on a single legislation but is formed of cyber laws, criminal laws, data protection laws and judicariums. These legal measures all aim to provide privacy, dignity, personal security, and freedom from digital exploitation. A lot of progress has been made in the legislative field, but its effectiveness relies on enforcement, technological capacity and awareness among the public.

Information Technology Act 2000 is the main legislation in India that regulates cyber offences. The Act was introduced to recognise electronic transactions and electronic communications and developed into the key piece of legislation for cyber crimes. The following are some provisions of the Act which are relevant to offences against women. Section 66C makes it a crime to use another person's identity and prescribes penalties for using another person's electronic signature, password or other identifying characteristic to commit a crime.¹⁷ This clause is often used in situations of false social media accounts, impersonation and misuse of personal information. Section 66D covers the issue of cheating by personation by computer and is frequently used when there is digital fraud, deceptive communications and an online impersonation of a woman.

The protection of privacy constitutes a significant aspect of cyber law. Section 66E of the Information Technology Act makes it an offence to capture, publish or transmit images of an individual's private part of the body without their permission.¹⁸ This provision is especially important when they come to the issue of voyeurism, photography without consent, sharing of photographs, and publishing of private photographs online. Increasingly, non-consensual image distribution is a necessary part of cyber law enforcement, as it requires protection of privacy.

The publication and transmission of obscene and sexually explicit material in electronic form is covered by Sections 67 and 67A of the Information Technology Act. These provisions are commonly used for revenge pornography, the dissemination of naked photos, sexually explicit material and sexual exploitation in the online environment.¹⁹ The law acknowledges that harmful material can be spread quickly in the internet, and therefore also criminal responsibility of persons responsible for such dissemination. Section 67B further addresses content involving children and seeks to combat online child exploitation. These collectively are key provisions to safeguard women and children from digital abuse and exploitation.

With the emergence of criminal activities on digital platforms, the Bharatiya Nyaya Sanhita, 2023 complements the Information Technology Act by providing relevant regulations on criminal conduct. Important protection against the offences against women which are enabled by technology is offered by Section 75 (sexual harassment), Section 76 (assault or use of criminal force with intent to disrobe a woman) and Section 78 (stalking) and Section 79 (voyeurism).²⁰ These are not only cyber specific provisions, but are often used in connection with offences that occur via social networking, messages, and other digital communications. The inclusion of cyber-type behaviour in general criminal law is testament to the understanding that there is a relationship between victimization in the physical and cyber world.

¹⁷ *Supra* note 4, s. 66C.

¹⁸ *Id.*, s. 66E.

¹⁹ *Id.*, ss. 67, 67A and 67B.

²⁰ Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 75, 76, 78 and 79.

Another significant piece of legislation is the Digital Personal Data Protection Act, 2023. The digital age of collection, storage and processing of personal information has raised questions about privacy and misuse of information. Women are often the victims of identity theft, unauthorized disclosure of personal information, and misuse of sensitive information. Digital Personal Data Protection Act aims to set a framework for the processing of personal data and lays obligations on those who process the same.²¹ While the law is aimed at data governance, and not criminal activity, it plays an important role in achieving the overall goal of safeguarding individuals from digital harms.

The Indecent Representation of Women (Prohibition) Act, 1986 is also relevant in the context of the cyberspace. The Act does not allow for print, advertisements, writing, painting, figures or other materials that depict women in an indecent manner.²² It was originally adopted prior to the advent of digital technologies, but its principles remain relevant for the discussion of women objectified, exploited or degraded content online. As images are increasingly manipulated, women's identities and dignity are being exploited and legislation against such activities is becoming more important with the rise of deepfake content and sexually explicit images.

Judicial interpretation has contributed greatly to the implementation of cyber laws. The case of *Shreya Singhal v Union of India* is one of the most crucial case in Indian cyber jurisprudence.²³ The Supreme Court unconstitutionally struck down Section 66A of the Information Technology Act arguing that it violated the constitutional right to freedom of speech and expression. The decision was primarily about free speech but also outlined the constitutional boundaries of cyber regulation and set down some key principles on the constitutional limits of online speech. The ruling highlighted the importance of striking a balance between cyber security and individual rights in a constitutional framework.

*State of Tamilnadu v Suhas Katti*²⁴ is a landmark case in Indian Cyber Crime Law. The case was related to the posting of obscene and defamatory messages against a woman in an online discussion forum. The prosecution of the accused was one of the first successful cases under the Information Technology Act and showed how cyber laws could help tackle harassment and abuse of women on the Internet. The case is still important as it set a precedent for practical investigations and prosecution of cyber offences.

The other important judgment is *Kalandi Charan Lenka v the State of Odisha*²⁵, in which the victim was harassed online by fake profiles and obscene messages and manipulated images were circulated on the internet. The court highlighted the gravity of cyber harassment and stressed the importance of legal action to

²¹ Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 4, 5, 8 and 11.

²² Indecent Representation of Women (Prohibition) Act, 1986 (Act 60 of 1986), ss. 3 and 4.

²³ *Supra* note 5.

²⁴ C.C. No. 4680 of 2004 (Court of the Chief Metropolitan Magistrate, Egmore, Chennai).

²⁵ 2017 SCC OnLine Ori 552.

shield victims from online abuse. The judgment reflects an awareness of the psychological and social impact of cyber crimes against women, which the judiciary is becoming more aware of.

Although there is a substantial legal framework, there are still a number of difficulties involved in its enforcement. Issues like collection of digital evidence, technological skills, multi-jurisdictional investigations and identifying anonymous criminals can plague investigative agencies. Legislative action often falls short of fast-paced technological progress, resulting in gaps in legislation and enforcement. In addition, many victims are not aware of legal options or are afraid to report crimes because of stigma, fear of privacy, or other reasons.

However, the Indian law system shows a positive approach towards women's cyber crime. The judiciary, along with the Information Technology Act, the Bharatiya Nyaya Sanhita and data protection laws, has paved a path for safeguarding women in the digital space. Further reform, effective implementation, targeted training and increased public awareness are all critical for the realization of women's safety and justice in an increasingly digital world.

V. Cyber Crimes Against Women : Enforcement Challenges

Cyber crime against women is on a continuous rise despite the availability of a well-drafted legislation. With the increasing sophistication of technology, and the fast growth of digital communication platforms, the current array of preventive, investigative and enforcement mechanisms has proven to be severely challenged. Legislative changes have been made to bolster legal protections, but practical obstacles often compromise those laws. Accordingly, the recognition vs protection issue is one of the most pressing issues in the area of cyber law.

Underreporting is one of the most critical issues. A number of female victims of cyber crime do not report to the police for fear of social stigma, damage to reputation, victim blaming, or privacy concerns. For victims of revenge pornography, online sexual harassment and the sharing of intimate content, the prospect of legal action could lead to additional unwanted attention from others. This means that many offences go unreported and the perpetrators are able to operate with relative impunity.²⁶

This is yet another challenge, as the Internet is anonymous. Cyber criminals often use fake profiles, virtual private networks, encrypted communications and sophisticated technological tools to hide their identity. The process of identification of the offenders is thus a complex and time-consuming procedure that requires special technical expertise. Often perpetrators are living out of state, or even in a foreign country, making

²⁶ Aparna Viswanathan, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* 201 (Lexis Nexis, New Delhi, 2012).

investigations and prosecutions far more difficult. International cooperation is often required in cases of cyber crime, but may be delayed because of jurisdictional and procedural issues.

There are extra challenges when it comes to digital evidence. Electronic records are different from traditional records in that they can be easily altered, deleted, encrypted, or manipulated within a short period of time. Investigating agencies need to therefore have the technical skills to gather, preserve and analyze digital evidence in compliance with the law. However, the large numbers of the unskilled cyber forensic experts and lack of adequate technological infrastructure often prevent an effective investigation.²⁷ These activities are further complicated by the rate at which technology is changing, requiring investigators to have to keep up with new technologies and new ways cyber criminals are using them.

One major issue is related to the deepfake technology and cybercrimes using artificial intelligence. AI can produce extremely realistic fake images, video and audio recordings which could be used to harass, blackmail or defame women. Current legislation generally dates from a time when these types of technologies were not broadly adopted and may not always adequately meet the specific needs of these technologies. As deepfake technology evolves in sophistication, it becomes harder to identify these fake images and poses significant issues about privacy and consent, as well as evidentiary requirements.

Another huge challenge is still the insufficient cyber awareness of the users. Far too many people are still sharing personal information, photos and other sensitive information through digital platforms without realising the potential risks. This is a blind spot that is often targeted by cyber criminals with a phishing fraud, social engineering, fake messaging and identity theft attacks. S. privacy settings, cybersecurity measures or legal options may leave some women more vulnerable to cyber exploitation, especially if they are not familiar with them.²⁸

Finally, institutional constraints also play a role in how effective cyber law enforcement is. While some jurisdictions have cyber crime units in place, there are a shortage of personnel, technical resources and training opportunities in many jurisdictions. Investigating officers do not always have the needed skills in the fields of digital forensics, cyber security or electronic evidence management. As a result, investigation and prosecution can be delayed, minimizing the impact of available legal remedies for victims.

The other challenge is related to the velocity of spreading of harmful contents in digital platforms. Within minutes, the information can be shared with thousands of people through manipulated content, defamatory statements, private information and obscene images. Authorities can quickly remove such content, but copies may still be shared through various platforms and communication channels. This often hinders the effective

²⁷ Pavan Duggal, *Cyber Law in India* 118 (Saakshar Law Publications, New Delhi, 2021).

²⁸ Talwant Singh, *Cyber Law and Information Technology* 212 (Allahabad Law Agency, Faridabad, 6th edn., 2022).

use of law enforcement response following a crime in cyberspace and underscores the need for preventive action.

The intermediary role of social media continues to be discussed. In addition to the reporting systems and content moderation policies that are new to digital platforms, there are worries about the slow time it takes to eradicate harmful content, differences in enforcement, and limited victim support systems. The issue of free speech and abuse protection continues to be a complex legal and policy problem.

The challenges highlight the need to tackle cyber crimes targeting women through a multi-faceted strategy that goes beyond the scope of criminal law. A more robust protection regime is reliant on better enforcement, technological development, public awareness and awareness-raising, institutional capacity development, and inter-institutional partnerships between government, technologists, and civil society organizations. Legal measures alone might not be effective to provide meaningful protection in the cyberspace without addressing these structural issues.

VI. Conclusion and Suggestions

Cyber crime is emerging as one of the biggest challenges faced by contemporary legal systems. The evolution of digital technologies into daily life has led to a growing in volume and complexity of cyber offences. The rapid digitalization of India has created tremendous opportunities for social and economic empowerment but also put people at the risk of being victims of new kinds of victimization. Women are especially targeted for cyber stalking, online harassment, cyber bullying, revenge pornography, identity theft, morphing of images and deep fake exploitation and abuse of technology. Not only are these crimes committed to the detriment of privacy and dignity but they also have severe psychological, social and economic implications.

It is a study that shows that India has provided a significant legal framework to tackle cases of cyber crimes. A combination of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and other laws can be used to tackle cyber victimization in various ways. Judicial rulings have also helped shape the jurisprudence in the field of cyber law and upheld the constitutional values of privacy, dignity, and personal liberty. There is however, an increasing trend of cyber offending of women that suggests that recognition is not enough for effective protection.

The critical analysis shows that one of the greatest challenges in enforcement. Reporting continues to be underreported, technologies are still complex, and awareness of the problem is not widespread enough, jurisdictional issues remain, there is a lack of cyber forensic capability, and new technologies are emerging. Legislative and institutional reaction to cyber crime often lags behind its development, allowing criminals to

take advantage of the shortcomings. Therefore, it is important to improve the preventive and remedial measures in the cyber law framework.

Ensuring the safety and security of women in cyber space is not just a technological or legal problem, but a human rights, gender justice and social equality problem. Women are able to access digital spaces without being harmed, intimidated or feared in digital environments. The expansion of India's digitalization efforts is an ongoing process, and both cyber security and the rights of women must be priorities for the development of laws and policies.

To wrap up, the cyber crimes targeting women is a multifaceted problem that needs a cooperative legal, technological, institutional, and social solution. India has taken steps to evolve cyber laws but further evolution and implementation is crucial to fight the ever-changing threats. Technology and technological advance must be complemented by strengthened legal protection, effective enforcement and shared responsibility for safeguarding the dignity, privacy and rights of women in cyberspace.

A number of strategies can improve the existing protection. First, the special units of cyber crimes must be strengthened with the state-of-the-art technological infrastructure and regular professional training. Second, public awareness programs are to be run to make citizens, especially women and youth, aware about cyber security practices, protection of privacy and the available legal avenues for redress. Third, laws ought to be reviewed on a regular basis, to include new technologies like artificial intelligence and deepfakes. Finally, enhanced collaboration between law enforcement, social media sites and technology firms should be encouraged to ensure that harmful material is identified and removed in a timely manner. Fifth, there should be convenient mechanisms for victim assistance, such as counselling and legal aid, to help women victims of cyber offences. Last but not least, schools need to establish digital literacy and cyber safety programs to raise awareness of cyber dangers and responsible online use.