ISSN: 3139-3179(Online)
Aviradha International Journal of Law and Legal Studies (AIJLLS)
© AIJLLS | Vol. 2 | Issue 2 | January-March 2026
Available online at: https://aijlls.com/
DOI: https://doi.org/10.65785/aijlls.v2i2.10

Technology-Facilitated Crimes Against Women in India: A Legal Perspective

Dr. G.M. Mamatha [1] and Dr. Manindra Singh Hanspal [2]

[1] *HOD, School of Law, Presidency University, Bengaluru.*

[2] *Assistant Professor, Presidency University, Bengaluru.*

Corresponding Author Email: mhanspal21@gmail.com

ABSTRACT:

The Internet and mobile technology have revolutionized Indian life. It has also brought about new forms of harm against women. Today, online harassment in the form of cyber stalking, sharing of intimate images without consent, online impersonation, sextortion and the dissemination of pornographic images impacts the safety and dignity of women nationwide. This paper discusses the legal regime regulating the technology-enabled crimes committed against women in India. This study adopts a doctrinal approach. It outlines the constitutional pillar, right to life and dignity under Article 21 and right to equality under Article 14, as interpreted by the Supreme Court in the privacy judgement of 2017 in Justice K.S. Puttaswamy v. Union of India. It then looks at the Information Technology Act, 2000, the provisions on identity theft, violation of privacy and obscene content, etc., and the judgment of Shreya Singhal v. Union of India, which invalidated Section 66A of the Information Technology Act, 2000. It examines the criminal law on voyeurism, stalking, and insult to modesty of the Indian Penal Code and their continuation in the Bharatiya Nyaya Sanhita, 2023, which was introduced in 2023. It takes into account special protective laws and the Digital Personal Data Protection Act, 2023. The paper details the common types of harm, links to provisions and highlights gaps in the definition, reporting and enforcement. It ends with suggestions for legal and institutional changes.

Keywords: *Cybercrime, Women, Technology, Privacy, Information Technology Act, Bharatiya Nyaya Sanhita, Online harassment, Data protection.*

1. INTRODUCTION:

The opportunities afforded by digital technology to women in education, work and public life are new. This new technology has also designed new lines of harm. Women are targeted by offenders

through their phones, social media and messaging apps with tools including stalking, threatening, shaming and defrauding. [1] They take 'private' pictures of people without their permission. They disguise themselves using fake names. They are demanding monetary compensation, threatening to expose them if they don't give. Their actions have a profound impact on safety, dignity, and mental health and leave a lasting imprint on the life of the victim, even after the victim logs off the internet. The legal response by India has developed over the course of 20 years. The first guidelines on Internet behaviour were introduced in the Information Technology Act, 2000. [2] Offences related to privacy and obscene content were added in 2008. The reforms in the criminal law in 2013, following a national debate on the safety of women, inserted offences of stalking and voyeurism. These protections were now given a strong constitutional footing in 2017 when privacy was recognized as a fundamental right. Offences safeguarding women were inherited from the Indian Penal Code, which was replaced by the Bharatiya Nyaya Sanhita 2023. [3] The Digital Personal Data Protection Act, 2023, introduced provisions concerning the processing of personal data.

This paper tries to consider this framework. It has three aims. The first goal is to enunciate the constitutional and statutory provisions of technology-facilitated offences against women. The second purpose is to identify principles in the law which address each of the common types of harm. The third goal is to highlight any issues with the definition, reporting and enforcement of the law, as well as provide recommendations for the law's reform. The discussion is confined to the developments through 2024 and is based on the wording of the statutes and the most important judgments. It's important to first define some terms. This paper refers to gender-based harm perpetrated through technology as ‘technology-facilitated crime against women,' and similarly, writers refer to it as ‘cybercrime against women, ‘online gender-based violence,' or ‘image-based abuse. It doesn't matter whether it's a specific name that's used, but indeed whenever it's a technology that targets a woman and causes harm to her safety, dignity and/or property. One reason why the paper does not distinguish between the various types of crimes is that multiple crimes may occur in a course of conduct and multiple statutes may be violated in a single crime. This 'framing' is only to aid later argument, as it becomes clear that there is a need for clarity and coordination throughout the law.

2. THE NATURE OF TECHNOLOGY-FACILITATED CRIME AGAINST WOMEN

Technology-facilitated crimes against women are crimes committed against a woman, in which technology plays a key role. These tools comprise social media, messaging, email, cameras and

financial technology. [4] This can be sexual, financial, reputational, and/or psychological and is often a combination of these. The online environment enables the offenders to have reach, speed and anonymity. It also enables the dissemination of harmful content in a widespread manner, and to stay accessible for a long time after the initial act. [5]

There are a number of typical forms of these crimes. The chief categories are listed below and in Figure-1. Cyber stalking/harassment is when someone engages in unwanted contact and monitoring over an extended period of time. [6] Non-consensual sharing of intimate images, sometimes known as 'image-based abuse,' is the taking or posting of private images. [7] Online impersonation and identity theft are the acts of creating a fake profile or using another person's identity. [8] Sextortion and financial fraud are threats, and the fabrication of sexual content and/or money. [9] The publishing of content that is obscene or sexually explicit is a form of obscene or sexually explicit content. Defamation and morphed images are the damage to reputation caused by false and/or altered content.[10] There are three aspects to these crimes that make them different from harm that is done offline. The first one is reached. The reach of a single post to a huge audience can be achieved within minutes and can transcend state and national boundaries. The second is the permanence: Online content can be copied and stored numerous times, which means that if it is deleted from one location, it doesn't stop the harm. Thirdly, anonymity. Offenders may be behind fake accounts, and it is difficult to trace, making abuse easier. These characteristics make one thing clear: One event can lead to a lasting and widespread impact, and a quick legal response is more crucial than in the offline environment.

Figure 1. Common forms of technology-facilitated crime against women.

The impact is not limited to the person. Women fear that online abuse can discourage their participation in public discussions and in spaces where there is social and economic value. But equality is not only damaged, but also safety. [11] Legislation to safeguard women online enables

them to be able to fully participate in public life. The National Crime Records Bureau (NCRB) data reveals that the incidence of cybercrimes against women has increased over the years in the country, highlighting the need to take a decisive step towards combating such offences. [12] There are also differences in the effect amongst women's groups. Both young women and young girls are at risk as a result of the use of social media, and also at school and college. There is concerted abuse of women in public positions, including journalists, activists and politicians, to silence them. Women who lack resources may not be able to get legal assistance or have the resources to remove harmful content. There will be instances where one response won't apply to everyone due to the differences. They also bring this issue into the foreground of the broader issue of the safety and dignity of women, both of which have always been part of the focus of the Constitution and the criminal law. An effective framework should be able to be implemented among the most vulnerable population, not just those who are able to protect themselves.

3. THE CONSTITUTIONAL FOUNDATION

This is based on two rights, both outlined in the Constitution. The first one is the right to life and personal liberty guaranteed in Article 21 of the Indian Constitution. This right includes dignity and privacy, which have been read into the Supreme Court. In the case of Justice K.S. Puttaswamy v. Union of India, 2017[13], it was a nine-judge bench which declared privacy as a fundamental right guaranteed under Article 21 of the Indian Constitution. For technology-facilitated crime, it is important as images of the intimate body are perceived as attacks on privacy and dignity. Article 14, with the protection against discrimination under Article 15, is the second right. Crimes committed against a woman for being a woman are related not only to equality issues but also to issues of liberty. Such rights place a duty on the State to ensure that women are not harmed by private individuals/actors, not by the State itself. The duty is in keeping with the criminal law, punishing the offenders and the platforms and data regulatory law. It also leads the way for courts in the interpretation of statutes, as the words of a statute are interpreted in the light of constitutional values such as dignity, privacy and equality. The constitutional structure thus permeates the entire structure that is described in the subsequent sections.

It's important to emphasize this concept of dignity. The Supreme Court has made dignity one of the fundamental aspects of the right to life of a person as enshrined in Article 21.[14] The use of images together with sexual harassment is a clear assault on dignity as it involves exposure and degradation of the person against her will. A court reading a statute in this context will take heed of the protection of the dignity, and that will help inform the statute's reading to include new

types of digital harm. This connection of the technical provisions of the statutes with a deeper constitutional purpose. The international law obligations of India are in the same direction. India is a signatory to the Convention on the Elimination of All Forms of Discrimination against Women, which requires it to take steps to address violence and discrimination against women, including through the use of technology, which is now being included in the international guidance on the issue. These are not instruments that, on their own, make offences, but they can help in interpreting statutes and in the drafting of policies. They have reaffirmed the importance of protecting women online not only for the sake of their safety but also for their equality and human rights.

4. THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000, is the main law regarding online practices in India. It regulates electronic documents, digital signatures, and a variety of cyber offences. The Act, which was amended in 2008, dealt with various harms suffered by women. The provision of Section 66C is on the subject of identity theft, which is the unauthorized use of someone else's identity information.[15] The provisions of section 66D (Cheating by personation using a computer resource) apply to many online fraud schemes.[16] Section 66E is the section that covers the area of privacy that concerns the taking or publishing of photographs of a private part of the body without permission. [17] The Act's protection is illustrated in the context of the larger protection in Figure 2.

Figure 2. The layered legal framework for technology-facilitated crimes against women.

Obscene and sexually explicit material is also covered in the Act. Section 67 is about the dissemination/printing of obscene material through electronic means. The material in section 67A

is material which contains a sexually explicit act. The provisions of section 67B protect minors, specifically relating to child sexual abuse material. These provisions contain the potential to take action against the sharing of intimate images and material of a pornographic nature which targets women, but require careful interpretation to ensure it is applied in this context. These provisions have limitations which impact women in particular. Some of these have been written to address obscene content in general and not to refer to the specific abuse of a particular woman; therefore, these do not necessarily reflect the harm of non-consensual sharing, which is that the use of private or consented-to content is not done with their consent. The focus of the violation-of-privacy provision is on images of private areas, which may not apply to all images of intimacy or all morphed images. This raises the possibility that prosecutors will try to "cobble together" provisions to fit the facts. A provision solely and specifically based on consent and image-based abuse will fill a portion of this gap, and the name of evil will be more apt.

Part of the Act was Section 66A, which sparked a substantial constitutional challenge. Section 66A was designed to cover sending messages via a computer or communication device which were offensive or menacing. In Shreya Singhal v. Union of India, 2015, the Supreme Court had invalidated Section 66A.[18] The Court, in its ruling, concluded that the provision was ambiguous and too wide, and that it infringed the right to freedom of speech, under Article 19(1)(a). The ruling upholds freedom of expression on the Internet, but it also eliminates a provision that some had been able to leverage against online abuse. The remaining provisions of the act were given more weight, and so too was the criminal law. The Act also extends to the duties of intermediaries such as platforms for hosting content. Section 79 provides a degree of protection for intermediaries in respect of content provided by their users, subject to the satisfaction of a number of duties. These duties have been elaborated upon under the Act in 2021. They need big intermediaries to have grievance officers and to act on grievances within a stipulated time. They also need to remove some content which reveals a private area, displays nudity or a sexual act or impersonates a person within a short time after receiving a complaint. These responsibilities provide victims with a path to have harmful content removed, but in reality, how quickly and consistently harmful content is removed is a concern.

5. CRIMINAL LAW: THE INDIAN PENAL CODE AND THE BHARATIYA NYAYA SANHITA, 2023

There has been a long history of general criminal law protecting women from harm, and changes have been made to the general criminal law to protect women in the digital world. Justice J.S.

Verma chaired an expert committee which, after a nationwide debate on the safety of women, recommended adding specific offences to the Indian Penal Code for which the Act was passed in 2013. Section 354A was for sexual harassment, which is defined as any unwelcome sexual remarks or demands. The proposed Section 354C was about voyeurism, visualizing or disseminating pictures of a woman while she is engaged in a private act. The provisions of Section 354D related to stalking and specifically included monitoring a woman electronically. Section 509 was for insulting a woman's modesty by words, gestures or acts. [19] The Indian Penal Code was replaced by the Bharatiya Nyaya Sanhita, 2023, from 1st July 2024, and these protections were continued. Voyeurism is included in section 77; Stalking is included in section 78; Insult to a woman's modesty is included in section 79; and Sexual harassment is included in section 75. The new wording basically preserved the nature of the original crimes, such as the explicit mention of electronic means in the offence of stalking. [20] For practice purposes, the continuity is important as conduct before the end of 2024 is governed by the Penal Code, conduct after the end of 2024 is governed by the new Penal Code, but the basic protections are retained.

The Information Technology Act is supplemental to these criminal provisions. One incident of abuse could trigger multiple provisions. The capture and circulation of an intimate image could, for instance, constitute voyeurism under the criminal law, infringement of privacy under Section 66E of the Information Technology Act, as well as the distribution of obscene material under Section 67. The overlap provides prosecutors with a variety of tools, but also requires careful charge construction to ensure the provisions are accurate in light of the facts.

The crimes have actual consequences and significant procedural elements. Stalking (including the act of monitoring a woman through electronic devices) is punishable by imprisonment, which is extended in case of repeat offences. Voyeurism is punishable by imprisonment and/or a fine, and will be more severe in case of a second offence. Many of these crimes are cognizable, and under the procedural law, the police can register a case and investigate without the permission of the court. There are also several crimes committed against women that enable a woman officer to lodge a complaint and enable the victim's identity to be protected. These features will help to reduce the obstacles that victims may encounter in seeking assistance. These crimes require electronic evidence for proof and thus have their own rules. Information, photos, call information and account information should be gathered and given in a court-acceptable format. The law on electronic evidence has been provided in section 65B of the Evidence Act, 1872 and in the Bharatiya Sakshya Adhiniyam, 2023, for a long time, which requires a certificate in support of the

admissibility of an electronic record. So the way digital evidence is handled has an impact on the successful prosecution. It's as important as the offences themselves to provide clear procedures and training, or the strong case can be defeated by weak collection or a faulty certificate.

6. SPECIAL PROTECTIVE LAWS, DATA PROTECTION AND LEGAL MAPPING

In addition to the provisions in the general criminal law and the Information Technology Act, there are some laws specifically safeguarding women in certain contexts. The Indecent Representation of Women (Prohibition) Act of 1986 bans the indecent representation of women in publications and other media, which also covers digital content.[21] There is a legislation that provides for the prevention, prohibition and redressal of sexual harassment at workplaces, including through electronic communication (The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013).[22] Minors are also covered by the Protection of Children from Sexual Offences Act, 2012, which also covers online sexual abuse.[23] There's another layer for data protection. The Digital Personal Data Protection Act, 2023, regulates the processing of digital personal data and provides rights to individuals related to their personal data.[24] Robust data protection lowers the likelihood that any personal information will be revealed or misused, which would allow for the stalking, impersonation and fraud. While the Act is not a criminal law, it is nevertheless a law which advances the protection of women, even if it is not aimed specifically at gender-based harm. Table 1 is a correlation of common forms of harm and the related legal provisions. A closer note should be taken of the workplace law, as work has shifted somewhat to the online realm. The Sexual Harassment of Women at Workplace Act 2013 considers unwelcome sexual conduct to be harassment and extends that to conduct made by electronic communications, including messages and emails. Employers must establish an internal committee and offer a complaints procedure, as required by the Act. With the rise of remote and hybrid work, harassment via digital means has become a problem, and the Act provides a remedy in addition to the criminal law. Minors are also well protected under the Protection of Children from Sexual Offences Act 2012, including from the online sexual abuse of children, which overlaps with the provisions of the Information Technology Act on child sexual abuse material.

Form of harm	Key legal provisions	Nature of protection
Cyber stalking and harassment	Section 78 BNS (stalking) and Section 75 BNS (harassment)	Criminal penalty for unwanted monitoring and contact
Non-consensual intimate imagery	Section 77 BNS (voyeurism) and Section 66E IT Act	Penalty for capture and circulation of private images

Form of harm	Key legal provisions	Nature of protection
Obscene or explicit content	Sections 67 and 67A IT Act	Penalty for publishing obscene or explicit material
Online impersonation	Sections 66C and 66D IT Act	Penalty for identity theft and cheating by personation
Insult to dignity	Section 79 BNS	Penalty for acts intended to insult a woman's modesty
Misuse of personal data	Digital Personal Data Protection Act, 2023	Rights and duties on the handling of personal data

Table 1. Mapping common forms of harm to legal provisions.

To enable the framework to be viewed on a whole, Table 2 provides an overview of the main instruments in this field and their year, as well as their relevance. The instruments include both the Constitution and the latest legislation, reflecting the evolution of the protection itself. The table also shows an aspect of the Indian approach. There is no single Act in India which explicitly defines and talks about technology-mediated gender-based violence. Protection is, on the contrary, distributed throughout the Constitution, the Information Technology Act, the criminal law, special protection legislation and the data protection statute. Yes, this spread has an upside since it gives several provisions to apply to one act and provides prosecutors with options. It also involves a cost, since a victim and an investigating officer have to read many laws to find the appropriate provision, and there are gaps which occur where none of the laws provide a specific provision for a new form of harm. It is the pattern that provides the motivation for the reforms set out below. The rationale for the reforms below is the pattern.

Instrument	Year	Relevance
Constitution of India (Articles 14, 21)	1950	Rights to equality, life, dignity and privacy
Information Technology Act	2000	Core offences on identity, privacy and obscene content
Protection of Children from Sexual Offences Act	2012	Protection of minors, including online
Criminal Law (Amendment) Act	2013	Added stalking, voyeurism and harassment offences
Sexual Harassment of Women at Workplace Act	2013	Workplace harassment, including electronic forms
Puttaswamy judgment	2017	Privacy is recognized as a fundamental right
Digital Personal Data Protection Act	2023	Rights and duties on personal data
Bharatiya Nyaya Sanhita	2023	Carries forward offences protecting women

Table 2. Key legal instruments and their relevance.

7. THE JUDICIAL RESPONSE

It is this area that has been influenced in two respects by the courts. They have established the constitutional foundation first of all. The Puttaswamy judgement of 2017 put privacy at the centre of the protection of women in the digital space. The Court's determination that privacy is a fundamental right provided image-based abuse and surveillance victims a strong constitutional argument and the State a clear obligation to safeguard privacy under the law. Later benches have been influenced by this holding in considering the scope of State and private interests in respect of personal information. Secondly, the courts have regulated the balance between protection and free speech. The Court, in Shreya Singhal (2015), ruled a general law permitting arrest for offensive messages to be unconstitutional. The ruling safeguarded freedom of expression in the digital world and ruled that any limitation on speech needs to be clearly and precisely defined. The two taken together establish the context for this field. It is the State's duty to keep women safe from actual harm, but the State has to do this by means of measures that are unambiguous enough to allow for freedom of speech. The rest of the provisions are designed and implemented in light of this balance. Courts have also given guidelines on the timely action to be taken on complaints, such as removing harmful information and ensuring that the identity of victims is not exposed. These directions are important because they can exacerbate the harm if delayed or not followed. Overall, the judiciary's actions have enhanced the rights of women and the rules of online activity.

Another area of development relates to the deletion and eradication of harmful material. Courts have acknowledged that there is a strong interest in the removal of content from all platforms and authorities that host the images, and have ordered them to do so when a victim has fallen victim to image-based abuse. Because of the recognition of privacy as a fundamental right, one can argue that the further dissemination of material published with his consent should be restricted. In addressing the feature of permanence as mentioned above, this developing method is that of a one-time removal order that is of little value if the content is being duplicated elsewhere. It is for this reason that the courts have turned towards remedies to fight the dissemination of content, rather than the initial act.

8. CHALLENGES AND GAPS

The framework is not as robust as it could be, and several challenges decrease the protection that the framework would provide.

- **Definitions:** Some harm, like the production of altered or synthetic images, does not fit the traditional technology-based provision. As there are more tools available to generate such realistic false images, the law might be challenged. The lack of a definition for image-based abuse could be the reason.
- **Reporting:** The majority of women who are being abused on the Internet don't report the abuse because of shame, fear of getting more abuse, or not being sure what to do or if their actions will make a difference. Reporting systems are difficult to use, and victims might not know to whom to report. There is low reporting, resulting in many offenders going without any repercussion and in official statistics, being an underestimate of the problem.
- **Enforcement and capacity:** Online crime investigations require expert policing, technology and the involvement of platforms that may own the information required. Many police units do not have this capability, and elements of the cross-border make it more challenging when an offender or a platform is located outside of India. The longer it takes for the investigation to take place, the greater the chance the harmful content will spread and the less chance for a remedy.
- **Platforms:** Many harmful pieces of content exist on private platforms, and how quickly the content can be removed will depend on their systems and desire to do so. The provisions on intermediary duties impose some obligations, but it can take time, and it is uncertain whether victims will be removed. A speedy and straightforward method for eradicating non-consensual intimate content would lessen harm. There can be some confusion around victims and investigators, as there is an overlap between a number of statutes.
- **Social stigma and awareness:** Few women receive support or condolences when reporting online abuse; instead, they feel that they are being blamed for it, leading them not to report it. Lack of knowledge of rights and remedies further compounds the issues, as the victim who is not aware of which law to which he/she can turn or which law enforcement authorities to contact may not take any action. Awareness-raising initiatives, facilities for the victims and a friendly attitude from authorities would assist those who need to avail themselves of the existing protection. This challenge is social as well as legal and demonstrates that there needs to be a change in both the law, practice and attitudes.
- **Jurisdiction:** Investigations are even further hindered, as often the offender and/or platform is located outside the victim's state or country. Requests for data stored overseas may take an extended period of time, and harmful content can travel to services more quickly than the

authorities can react. Effective cooperation between the agencies, unhindered access to platforms and timely mutual assistance are required to ensure the law is effective along the borders. Even if provisions are good in the country, if there is no cooperation, it may not be possible to reach an offender from another country.

9. RECOMMENDATIONS

Based on the analysis, the following recommendations are made:

- Clarify what is meant by image-based abuse and the use of synthetic/altered images, ensuring the law can cover new ways in which images are used for abuse.
- Make reporting easier in one, easy-to-access system and ensure the identity of victims is safeguarded throughout.
- Enhance Police Units' capacity via training, technical tools and special cybercrime cells.
- Assign roles to platforms to swiftly and effectively remove intimate content that is not consensual and to retain evidence.
- Improve the practice of data protection to make it more difficult to abuse personal information for fraud and stalking.
- Provide counselling and legal assistance, and awareness-building programs on remedy options to victims.

These measures are best implemented in combination and not separately. Having a clear definition is of little benefit if reporting is still hindered, and fast removal procedures are of little benefit if police have no means of tracing offenders. The reforms take, therefore, at the same time care of the law, the institution and the support for the victims. They complement the existing legislation and the Constitution, and seek to turn the foundation into protection that women can use every day in their lives.

10. CONCLUSION

Rape and sex crimes committed via technology are very serious and are on the rise in India. The legal framework has evolved over the past twenty years: beginning with the Information Technology Act 2000, followed by criminal law reforms in 2013, and recognition of privacy as a fundamental right in 2017, with new laws in 2023. These instruments collectively contribute to the security of women in the digital sphere, ensuring their safety, dignity and equality. The strength and direction of the constitutional structure come from the constitutional underpinnings in Articles 21 and 14. However, protection that is on paper is not the same as protection that is in reality. Limits to the impact of the law include gaps in definition, low reporting rates, limited

capacity for enforcement, and delayed removal of harmful content. These gaps may be filled by the proposed reforms here. The law should adapt to technology to ensure that women participate in digital life without fear of harm in the future. The protection of women is combined with the broader principles of privacy, equality and safe public participation in this task. This paper is a snapshot of the framework, and its sources are based on the progress up to 2024. These developments will keep unfolding until the new criminal code is fully in force, the platforms adapt their systems, and courts will interpret it in new cases, in the light of the data protection statute. Future research should examine the implementation of the new provisions, the victim experience of the reporting and removal procedure and the extent to which the reporting and removal tools are pushing the envelope on the current legislation on synthetic images. This study would reveal if the framework accomplishes its goals and would assist in guiding the changes that have been proposed in this paper.

REFERENCES

[1] A., Sabari Deeksha Choudary; SR, Yugandhra; S., Pranesh Raj. (2021). Cyber Crime Targeting Women. Indian JL & Legal Rsch., 3, 1.

[2] The Information Technology Act, No. 21 of 2000, India.

[3] Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023 (India)

[4] Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. The British Journal of Criminology, 59(3), 551-570.

[5] Wall, D. S. (2015). The Internet as a conduit for criminal activity. In A. Pattavina (Ed.), Information technology and the criminal justice system (pp. 77–98). Sage Publications.

[6] Kaplun, K. (2023). Tracking and Trailing Each Other: Tracing Stalking and Harassment Through Time and Technology (Doctoral dissertation, Rutgers The State University of New Jersey, Graduate School-Newark).

[7] Maddocks, S. (2018). From non-consensual pornography to image-based sexual abuse: Charting the course of a problem with many names. Australian Feminist Studies, 33(97), 345-361.

[8] Irshad, S., & Soomro, T. R. (2018). Identity theft and social media. International Journal of Computer Science and Network Security, 18(1), 43-55.

[9] Paquet-Clouston, M., Romiti, M., Haslhofer, B., & Charvat, T. (2019, October). Spams meet cryptocurrencies: Sextortion in the bitcoin ecosystem. In Proceedings of the 1st ACM conference on advances in financial technologies (pp. 76-88).

[10] Henderson, M. S. (2018). Applying Tort Law to Fabricated Digital Content. Utah L. Rev., 1145.

[11] Sobieraj, S. (2020). *Credible threat: Attacks against women online and the future of democracy*. Oxford University Press.

[12] National Crime Records Bureau. (n.d.). *National Crime Records Bureau*. Ministry of Home Affairs, Government of India. National Crime Records Bureau (NCRB)

[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (Supreme Court of India).

[14] Yadav, U. (2021). Article 21: A Comprehensive Journey of Right to Life and Personal Liberty. *Indian J. Integrated Rsch. L.*, *1*, 1.

[15] Information Technology Act, 2000, No. 21 of 2000, § 66C (India).

[16] Information Technology Act, 2000, No. 21 of 2000, § 66D (India).

[17] Information Technology Act, 2000, No. 21 of 2000, § 66E (India).

[18] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 : AIR 2015 SC 1523 (SC).

[19] Verma, J. S., Seth, L., & Subramanium, G. (2013). *Report of the Committee on Amendments to Criminal Law*. Government of India.

[20] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), sections 75, 77, 78 and 79, in force from 1 July 2024.

[21] The Indecent Representation of Women (Prohibition) Act, 1986 (Act No. 60 of 1986).

[22] The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (Act No. 14 of 2013).

[23] The Protection of Children from Sexual Offences Act, 2012 (Act No. 32 of 2012).

[24] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

Cite this Article:

***G.M. Mamatha & Manindra Singh Hanspal, "Technology-Facilitated Crimes Against Women in India: A Legal Perspective"**, Aviradha International Journal of Law and Legal Studies (AIJLLS), ISSN: Applied (Online), Volume 2, Issue 2, pp. 01-14, January-Mach 2026.*

Journal URL: https://aijlls.com/

DOI: https://doi.org/10.65785/aijlls.v2i2.10