

From Surveillance to Cyber Violence: Examining Online Harassment against Women through the Lens of Digital Constitutionalism

Abha Tyagi

Research Scholar

Shobhit University

Meerut

Email: abhatyagi2809@gmail.com

Dr Pallavi Jain

Assistant Professor

Shobhit University

Meerut

Abstract

In this age of digital technology, it is becoming increasingly difficult to combine personal privacy with national security, especially in India, where mass monitoring technologies cause serious concerns. The new Indian government's mass monitoring methods threaten constitutional privacy rights. These technologies' broad communication interception, keyword monitoring, and easy access to user data raise serious issues, especially as India's privacy laws are insufficient for concentrated surveillance. Due to its fast growth, cybercrime in India disproportionately affects women. This study examines cybercrimes against women in India. The legislative structure and enforcement methods for these statutes are given special consideration. Especially about the difficult balance between national security and private rights. Since many government agencies and commercial entities acquire and store enormous amounts of personal data in the digital age, the problem has become worse. India just approved the Digital Personal Data Protection Act 2023 to balance national security and personal rights. Surveillance helps maintain national sovereignty, unity, and integrity. Criminals use privacy settings and data-sharing weaknesses to monitor and influence their targets on digital platforms, emboldened by anonymity. Cyberstalking presents challenging challenges for victims, law enforcement, and lawyers. Many crimes go unreported because victims are unaware of their legal options and distrust law enforcement to investigate and prosecute these crimes. Additionally, the research concluded that India's legal system is unprepared to handle cybercrimes against women.

Keywords

Cybercrime Against Women, Cyberstalking, Mass Surveillance, Right to Privacy, National Security, Digital Personal Data Protection Act, 2023, Online Harassment, Revenge Pornography, Image-Based Sexual Abuse, Women's Digital Rights

Reference to this paper should be made as follows:

Received: 27.05.26

Approved: 15.06.26

**Abha Tyagi
Dr Pallavi Jain**

From Surveillance to Cyber Violence: Examining Online Harassment against Women through the Lens of Digital Constitutionalism

Vol. XVII, No.1
Article No. 21,
Pg. 205-216

Similarity Check: 24%

Online available at

<https://anubooks.com/journal-volume/jgv-vol-xvii-no1-jan-june-2026>

DOI: <https://doi.org/10.31995/jgv.2026.v17i01.021>

**This article has been peer-reviewed by the Review Committee of JGV.*

Introduction

Cybercrime is the term used to describe illicit actions conducted using the internet or any digital technology. Cybercrime is more likely to have detrimental effects on the physical and emotional well-being of Indian women. Cyberbullying and online harassment, which primarily target women, have become more common in India due to the growth of social media and online platforms. Cyberthreats that can cause serious psychological pain and emotional agony, such as identity theft, stalking, and revenge pornography, are particularly dangerous for women. Cybercrimes against women in India include online harassment, cyberbullying, cyberstalking, revenge pornography, and cyber financial fraud. While online harassment is the act of sending threatening or offensive messages or comments on social media platforms, cyberbullying is the use of technology to harass, denigrate, or intimidate someone. Online stalking is a pattern of persistent online harassment that involves monitoring, watching, or tracking someone's online activity. Cyber financial crime includes credit card fraud, phishing, and other online financial crimes. Conversely, the act of sharing sexually explicit pictures or videos without the victim's consent is known as revenge pornography. India ranks among the top five countries in the world for cybercrime. Additionally, the increased use of technology and the internet has led to an increase in cybercrimes, making it challenging to effectively address the problem.

The incidence of cybercrime against women in India is becoming an increasing worry, since it can have significant repercussions for the emotional and physical health of women, as well as for their economic well-being. Cybercrimes, which include online harassment, cyberbullying, online stalking, revenge pornography, and cyber financial fraud, demand rapid action from the government, law enforcement agencies, and civil society groups. These crimes include cyberbullying, cyberstalking, and cyberstalking. In order to effectively combat cybercrime, it is necessary to take a holistic strategy that includes raising awareness among the general public, improving cybersecurity laws and regulations, and offering assistance to those who have been victimized by cybercrime.

Cyber stalking is another type of cybercrime that women in India face. This term refers to a pattern of persistent harassment that occurs online and involves following, monitoring, or tracking the activities of another person while they are online. Cyber stalkers use various digital platforms like social media, emails, and messaging apps to stalk and harass their victims. According to a study that was compiled by the Cyber Crime Cell of the Mumbai Police, the number of occurrences of cyber stalking that have occurred in India over the

course of the past year has increased by 91%. At this point in time, basic ideals, particularly the concepts of liberty and dignity, are being threatened by the phenomenon of digital harassment. Because technology is becoming more and more intertwined into everyday life, it is essential that constitutional interpretation be able to adapt to the changes that are occurring in society. Together, progressive legislation, judicial activism, and policy execution are necessary to guarantee women's safety and empowerment in online environments.

Technological advancements exacerbate digital domestic abuse by providing abusers with continuous access to their victims, making it harder for victims to find safety. Abusers are able to remotely monitor, harass, and exert control over their victims with the use of tools such as GPS tracking, spyware, and social media surveillance, which are continually being improved and updated over the course of time. Furthermore, because of the anonymity that these online spaces provide, it is much simpler for those who commit acts of cyberstalking, revenge porn, and other types of digital abuse to participate in these activities without being held accountable. Victims often struggle to escape, as technology ensures that abuse can follow them wherever they go, blurring the lines between their public and private lives.

The term "cyberstalking" refers to a more specialized kind of cyberbullying that involves persistent and threatening online behaviors. Cyberstalking is another category of online gender-based violence. Cyberbullying affects people on a global scale, regardless of groups or regions. In the year 2023, one in every five people who used the internet reported feeling threatened by online harassment or abuse.

The presence of communities that hold highly sexist attitudes may also be fostered in online platforms. Anonymous discussion platforms often enable the spread of harmful ideas, reinforcing discrimination and violence against women. The nature of the digital world itself plays a role in this exclusion, as women are discouraged from fully engaging in online spaces due to the presence of threats, harassment, and a lack of safety.

In the process of establishing a legal framework, the United Nations Declaration of Human Rights (UDHR) plays a significant part. This is because it acknowledges that human rights, including as the right to freedom of speech, the right to privacy, and the right to be protected from violence, should be preserved in the realm of the internet. Despite the fact that the Universal Declaration of Human Rights is not a legally binding treaty, it does call for the protection of women and other disadvantaged groups from cyber violence, which includes harassment, threats, and abuse that occurs online.

Conceptual Knowledge of Cyberviolence Against Women

A term that is used to describe acts of violence, harassment, abuse, or intimidation that are carried out via the use of digital technology and online platforms is called cyberviolence. In this day and age, one of the most significant threats to women is the prevalence of gender-based violence that is enabled by technology. When compared to more traditional forms of violence, cyber violence is distinguished by the fact that it enables offenders to target victims anonymously on a global scale and has the ability to transcend geographical borders.

Online harassment of women may take many forms, including cyberstalking, trolling, hate speech, revenge pornography, sextortion, identity theft, non-consensual sharing of private images, impersonation, and doxing, to name just a few of the ways it expresses itself. Female journalists, activists, students, professionals, and political leaders are especially vulnerable to targeted harassment that is created with the intention of silencing their voices and discouraging public participation. Cyberstalking entails ongoing, fear-inducing digital surveillance, monitoring, and unwanted communication.

One of the ways that the development of artificial intelligence has contributed to an increase in internet violence is through the use of deepfake technology. AI-generated deepfakes undermine women's autonomy and dignity by producing fake, sexually graphic photos and videos. This kind of misuse of technology usually leads to severe mental pain, damage to one's reputation, social marginalization, and even physical violence by the perpetrator. Because cyber violence directly impacts women's rights to privacy, equality, dignity, and freedom of speech, it has important constitutional ramifications. Women are often forced to self-censor or completely avoid digital areas out of fear of online abuse, which undermines gender equality and democratic participation.

Surveillance Technologies and Digital Damage That Is Categorically Individual

One of the most important aspects of contemporary platform capitalism and governance is the presence of digital monitoring. For security, data analytics, targeted advertising, and social monitoring, governments and businesses are depending more and more on surveillance technologies. Biometric identity systems, facial recognition software, malware, algorithmic profiling, metadata tracking, and AI-based monitoring systems are some examples of these technologies.

Although surveillance tactics are usually presented as vital for maintaining public order or national security, excessive monitoring poses major risks to civil liberties and constitutional rights. This is the case despite the fact

that surveillance methods are regularly shown to be necessary. Women are disproportionately affected by digital monitoring due to the fact that surveillance technologies usually intersect with regimes that are patriarchal and discriminatory.

One of the most significant problems associated with surveillance is the extensive collection and processing of personal data without the individual's free and informed permission. It is common practice for governments and commercial organizations to periodically retain and analyze the images, communications, location information, and browsing patterns of women. Spyware and surveillance applications are frequently used in abusive relationships to keep tabs on the activities, social connections, and digital interactions of the women involved. Globally, there is growing concern over intimate partner violence assisted by technology. Through algorithmic tracking and behavioral profiling, social media platforms further support surveillance. Women who express political or feminist opinions online are regularly subjected to coordinated trolling campaigns, threats of sexual assault, and digital intimidation. These tactics are routinely employed against women.

The Difficulties That Women Face Online

Legislative and judicial initiatives have not been successful in removing the various difficulties that Indian women continue to face while attempting to receive protection and remedies from internet harassment. These difficulties come in the form of legal, structural, technological, and sociocultural issues. Within the context of the case of *Sabu Mathew George v. Union of India*, the Supreme Court of India issued an order to search engines, directing them to delete information that violated Indian laws, notably those laws that deal with the determination of prenatal sex. Platform responsibility, a concept that can be applied to content that encourages online violence or misogyny, was established by this ruling.

There is insufficient approval of new-age offenses by the law. Despite the fact that the Information Technology Act and the Indian Penal Code both provide generic remedies, they do not expressly acknowledge new sorts of cybercrimes such as:

1. AI-generated sexual content, Internet impersonation, pornographic deepfakes, and unapproved picture editing. When definitions or categories are ambiguous, judicial decisions and police actions are inconsistent.

2. Underreporting and Fear of Retaliation: A lot of incidents continue to be unreported due to the following reasons:

- The worry that one would be subjected to social stigma
- Not knowing one's legal rights
- A lack of confidence in the work of law enforcement
- The possibility of reprisal from perpetrators, particularly in cases when victims are subjected to abuse in intimate relationships or revenge pornography

Some women are concerned that reporting online abuse might lead to victim-blaming or increased harassment, both online and offline. This is a fear that is generally shared among women.

Taking Responsibility for the Platform and Addressing Bias in Algorithms

Social media companies typically take a long time to delete harmful information, despite requests to do so. The lack of transparency in algorithmic moderation disproportionately affects women, especially those from disadvantaged or minority backgrounds. Even when platforms take action, the effects are typically permanent; content may have already been downloaded or gone viral, harming a person's reputation over time. Even when platforms take action, this is still possible.

The Gender Gap in Digital Access and the Digital Gap

As a result of the digital divide, women also have a more difficult time gaining access to safe technology and filing complaints online. Many women are either controlled by males or do not own personal devices, especially in conservative families. Indian women are 28% less likely than men to own a mobile device with internet access, according to the GSMA Mobile Gender Gap Report 2022.¹⁰ When someone is being abused online, this makes getting help much more challenging.

The significance of digital constitutionalism, as well as its emergence and development

The application of democratic ideals, human rights standards, and constitutional values to the regulation of digital technology and cyberspace is known as "digital constitutionalism." Concerns about algorithmic discrimination, mass surveillance, digital power concentration, data exploitation, and a lack of responsibility among internet companies gave rise to the idea.

Historically, the primary objective of constitutional frameworks was to exercise control over the authority of the state. In spite of this, private technology companies have a tremendous influence on public discourse, communication, and the dissemination of information in the digital era. AI systems, search

engines, and social media platforms are progressively influencing how people engage in society and obtain information.

The objective of digital constitutionalism is to ensure that essential principles, such as liberty, equality, dignity, transparency, accountability, and the rule of law, are safeguarded within the realm of digital technology. It seeks to stop corporations and governments from arbitrarily using digital power.

As an additional point of interest, the concept emphasizes the relevance of data security, algorithmic fairness, intermediary responsibility, informational privacy, and democratic oversight of surveillance technology. It is for this reason that digital constitutionalism provides a normative framework that may be utilized to achieve a balance between the growth of technology and the protection of human dignity and constitutional rights.

It is especially important for women to have a digital constitutionalism since the constitutional guarantees of equality, privacy, and freedom of speech are directly violated by online abuse. It acknowledges that cyberspace must continue to be secure, inclusive, and available to everyone and that digital rights are an extension of fundamental human rights.

India's Constitutional Protection of Women's Digital Rights

Article 14 of the Constitution ensures that all individuals are eligible for equal protection under the law and are treated equally before the law. As a result of the fact that women are disproportionately affected by online harassment, it is difficult for them to engage equally in digital contexts. Due to the fact that they restrict women's ability to express themselves freely, gender-based harassment, sexist trolling, and online intimidation are all examples of behaviors that violate the principle of substantive equality. The State must implement affirmative action to shield women against discrimination and cyberviolence in accordance with the Constitution's guarantee of equality. Within the context of the case of *Rekha Sharma v. State of the National Capital Territory of Delhi*, the court brought attention to the role that law enforcement and intermediaries play in protecting women from cyberbullying and threats.

The legal framework of laws aimed at preventing cybercrime against women

The Indecent Representation of Women (Prohibition) Act of 1986 ought to be updated to encompass virtual settings. This is because the Information Technology Act of 2000 and the Information Technology Rules of 2021 provide a legal foundation for punitive actions against offenders. This proposal has been before Parliament for almost ten years. Additionally, it is believed that Indian courts assign more weight to offline offenses committed against women than

they do to online offenses made against women. When a person is charged with both online and offline offenses, there is a tendency to focus more on the offline offenses, according to the allegations. If such an imbalance exists, it should be corrected so that justice is administered equitably regardless of the location of the offence.

Section 66A: This section covers transmitting inflammatory communications through communication services, creating irritation, etc., or sending an email that misleads or deceives the recipient about its origin a practice known as IP or email spoofing. It is possible to get a maximum term of three years in prison or a fine for these offenses.

Forfeiting a computer resource or communication equipment is a violation of Section 66B, which carries a maximum punishment of three years in jail and a fine of one lakh rupees, or both, depending on the circumstances.

Electronic signature and other kinds of identity theft, such as using the password or electronic signature of another person, are covered by Section 66C of the statute.

Sector communication device faces up to three years in jail of any kind and a fine of up to one lakh rupees.

The violation of privacy is defined as the act of disseminating or publicizing the private information of another individual without first obtaining that other's consent, among other things. It is possible that the accused will be sentenced to three years in prison, a fine of two lakh rupees, or both.

Section 66F: Cyberterrorism is the deliberate attempt to undermine the nation's unity, integrity, security, or sovereignty by preventing anybody who is authorised from using a computer resource or by trying to breach or gain unauthorised access to one.

The use of confidentiality diaries was one of the penalties that were included in Section 72 for breaking privacy and secrecy.

Provisions made by the Bharatiya Nyaya Sanhita regarding cybercrimes committed against women

Section 75 regulates sexual harassment. (1) A man is guilty of sexual harassment if he engages in any of the following behaviors: (i) initiating physical contact and making advances that involve unwelcome and explicit sexual overtures; (ii) making a demand or request for sexual favors; (iii) showing pornography against the will of a woman; or (iv) making remarks that are sexually coloured. Every one of these behaviors constitutes sexual harassment.

Voyeurism: Section 77: Anyone who witnesses or records a woman performing a private act in a situation where she would typically expect to be unobserved by the perpetrator or by anyone else acting on the perpetrator's behalf, or who shares such footage, faces imprisonment of any kind for a minimum of one year, but up to three years, and a fine. In the event of a second or subsequent conviction, the punishment is imprisonment of any kind for a minimum of three years, but up to seven years, and a fine.

Section 78 regulates stalking. (1) A man is guilty of stalking if he: (i) follows a woman and contacts, or makes repeated attempts to contact a woman to establish a personal relationship, even when the woman clearly shows no interest in him; or (ii) keeps tabs on a woman's use of the internet, email, or any other form of electronic communication without her permission.

Organized crime: Section 111(1) Any continuing unlawful activity, including kidnapping, robbery, vehicle theft, extortion, land grabbing, contract killing, economic offence, cybercrimes, trafficking of persons, drugs, weapons, or illicit goods or services, human trafficking for prostitution or ransom, by any person or group of persons acting in concert, singly or jointly, either as a member of an organised crime syndicate or on behalf of such syndicate, by use of violence, threat of violence.

Defamation: Section 356. (1) Any person who, through words that are either spoken or intended to be read, or through signs or visible representations, makes or publishes in any manner any imputation concerning any person with the intention of harming, or knowing or having reason to believe that such imputation will harm, the reputation of such a person is said to defame that person, with the exception of the cases that will be discussed further below.

Methods of Excellence for the Prevention of Cybercrimes Committed Against Women: India is experiencing an increase in the number of cybercrimes committed against women, and it is imperative that women take precautions to prevent themselves from being victims of these crimes. The following are some of the most effective strategies that women may use to protect themselves from becoming victims of cybercrime.

When it comes to protecting oneself against cybercrime, one of the most effective and straightforward strategies is to make use of robust passwords. In addition to this, it is one of the most basic methods of safeguarding oneself.

It is of the utmost importance that you make certain that your passwords have at least of twelve characters, which should include a combination of

uppercase and lowercase letters, numbers, and special characters, respectively. If you want to protect your account, you should avoid choosing passwords that are easy to guess, such as your name, your birthdate, or the name of your pet.

Maintain the Confidentiality of Your Personal Information: When you disclose personal information online, particularly on social media platforms, use caution and choose your words carefully. Please take care not to reveal any private information, such as your home address, phone number, or any other facts that may be considered very sensitive. The use of phishing emails or phone calls that beg for personal information is another thing that you should be cautious of.

It is important to exercise caution while using social media since it may be a double-edged sword. It is possible that it will help you keep connected with friends and family, but it also has the potential to be a breeding ground for cybercrime. Be mindful of the individuals you add as friends, and avoid putting anything on the internet that may be construed as private or sensitive as much as possible.

In addition to forcing you to enter your password, two-factor authentication adds an extra layer of security to your online accounts by requiring you to provide a second form of verification, such as a code that is sent to your phone. As a means of accomplishing this, a second form of authentication is required in addition to your password. This feature is accessible on a broad range of well-known online services, including social networking platforms and email service providers, amongst others.

Make Sure That Your Software Is Always Up-to-Date: It is of the utmost importance that you make sure that all of your software, including your operating system and antivirus software, is always upgraded. The majority of the time, software updates include security patches that take care of vulnerabilities that cybercriminals may potentially exploit.

Antivirus software should be utilized. Malware and other types of hazardous software may be prevented from infecting your device on your computer with the use of antivirus software, which may also aid in the identification of existing malware. Make sure that the antivirus software you use comes from a reputable development business.

Conclusion

Since the advent of the digital era, there has been a substantial shift in the form of violence against women. The growth of new forms of cyberviolence that threaten democratic participation and constitutional rights has been facilitated by a number of factors, including artificial intelligence, social media,

surveillance technologies, and a government that is driven by data. Online harassment of women is a constitutional issue that affects privacy, equality, autonomy, dignity, and freedom of expression in addition to being a technology issue. The growing overlap between cyberviolence and surveillance highlights the critical need for rights-based digital governance. Digital constitutionalism offers a solid basis for extending constitutional norms into cyberspace and limiting the use of digital power by governments and enterprises. This foundation is supplied by digital constitutionalism. Through the promotion of accountability, transparency, privacy, and human dignity, digital constitutionalism has the potential to make significant contributions to the development of digital environments that are more secure and hospitable for women. For the purpose of protecting women from being subjected to cyberattacks, India has to strengthen its legislative framework, exercise control over surveillance technologies, ensure that intermediaries are held accountable, and establish gender-sensitive digital policies. It is very necessary for the preservation of constitutional democracy to ensure that human rights are protected in the digital arena, which is where modern social and political activity is taking place with growing prevalence.

References

1. National Crime Records Bureau. (2020). Crime in India. Retrieved from <https://ncrb.gov.in/en/crime-india>
2. Sharma, R. (2018). Cyber Crimes Against Women in India: An Analysis. *Journal of Information Technology and Economic Development*, 9(2), 18-33. Retrieved from <https://www.jited.org/index.php/jited/article/view/128/79>
3. National Crime Records Bureau, Crime in India-2021, Ministry of Home Affairs, Government of India(2022),available at: <https://ncrb.gov.in/en/en/crime-india>
4. Lorna Christie – Susie Wright, Technology and domestic abuse, UK Parliament, 2020, <https://post.parliament.uk/technology-and-domestic-abuse/>
5. Lorna Christie – Susie Wright, Technology and domestic abuse, UK Parliament, 2020, <https://post.parliament.uk/technology-and-domestic-abuse/>
6. Stacy Jo Dixon, *Cyberbullying – statistics & facts*, Statista, 2024 October 24, <https://www.statista.com/topics/1809/cyber-bullying/#topicOverview>
7. Wikipedia, *Online gender-based violence*

8. United Nations, *Universal Declaration of Human Rights (UDHR)*, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>
9. Enock, F. E., Stevens, F., Bright, J., Cross, M., Johansson, P., Wajcman, J., & Margetts, H. Z. (2024). Women are less comfortable expressing opinions online than men and report heightened fears for safety: Surveying gender <https://arxiv.org/abs/2403.19037>
10. Safiya Noble ,*Algorithms of Oppression:How Search Engines Reinforce Racism*, NYU Press,2018
11. Rekha Sharma v. State of NCT of Delhi,2020 SCC Online Del 1110
12. G.B. Reddy, *Women & The Law including Law Relating to Children* (Lex Worth, Gogia Law Publication, 10th edu., 2021).
13. Vaishali, *Bharatiya Nyay Sanhita & provisions regarding cyber-crimes*, 2024 <https://www.linkedin.com/pulse/bharatiya-nyay-sanhita-provisions-regarding-cyber-shintre-bhagwat-69fjff#:~:text=Whoever%20has%20in%20his%20possession,Sanhita%2C%20be%20punished%20with%20imprisonment> (last visited May. 06, 2026).
14. The Bharatiya Nyaya (Second) Sanhita, 2023, <https://prsindia.org/billtrack/the-bharatiya-nyaya-second-sanhita-2023> (last visited May. 07, 2026).
15. Gupta, S., & Kapoor, M. (2018). Cyber Crime in India: An Empirical Study on Cyber Crime Awareness among Women. *International Journal of Management Studies*, 5(4), 106-111. Retrieved from http://www.aarf.asia/images/short_pdf/1538513964_12.%20PAPER%203