

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

AI-Enabled Harassment: New Challenges in Tackling Cyberstalking in India

NISHA*

ABSTRACT

This paper examines cyberstalking as an emerging form of cybercrime in India and the new challenges that artificial intelligence and rapidly evolving digital technologies pose for its regulation. It situates cyberstalking within the broader landscape of online harassment, conceptualising it as the persistent, unsolicited pursuit, monitoring or threatening of an individual through digital platforms. Adopting a comparative national perspective, the paper analyses the Indian statutory framework, including Section 78 (stalking) and Section 77 (voyeurism) of the Bharatiya Nyaya Sanhita, 2023, and the Information Technology (Amendment) Act, 2008, against the gender-neutral approaches of the United States and the United Kingdom. It traces the legal evolution prompted by early incidents such as the case of Ritu Kohli, considers the psychological and sociological profiles of cyberstalkers, and evaluates the social and psychological impact on victims. The paper concludes by identifying the principal enforcement challenges, including cross-border jurisdiction, technological change, under-reporting and the preservation of digital evidence, and proposes reforms to strengthen cyber security and the protection of women in the digital realm.

Keywords: Cyberstalking, Digital, Harassment, Cybercrimes, Humanity.

I. INTRODUCTION

The digital world is the very medium through which the generation of the twenty-first century leads its life. The digital era is poised to become this generation's greatest legacy, an era marked by the advent of online social networking applications that have evolved into an integral part of everyday life. According to various schools of psychological thought, it is widely accepted that human beings are social by nature; they are perpetually in search of connection, social relationships, interpersonal interaction and networks.

To fulfil these inherent social desires and needs, technology has manifested itself in the form of a diverse array of online applications. These applications have become conduits for establishing connections across vast distances, platforms on which users share their life experiences and forge new relationships. The online posting activities conducted on platforms such as Instagram,

* Author is an Assistant Professor at IIMT University, Meerut, Uttar Pradesh, India.

Facebook and similar applications have, in a sense, become a means of cultivating social status, with individuals engaging through 'liking' or 'following' posts that they perceive as influential or inspiring.

Cyberspace has now evolved into a dynamic platform on which individuals share their personal identities and cultivate social networks and relationships. While this platform offers countless benefits, it simultaneously poses numerous challenges regarding privacy. In this era of the internet and digitisation, the most significant gains realised lie in the realms of communication and global connectivity. However, this connectivity, unfettered by geographical or physical barriers, is increasingly giving rise to cyber-threats in a world where individuals' personal identities exist more prominently within the digital sphere than in their physical lives. The digital revolution has also inadvertently served as an enabler for cyber-criminals lurking within the digital realm; as 'digital shadows', these perpetrators exploit the digital environment to inflict harm upon others. Today, cyberstalking, that is, pursuit over the internet, has emerged as one of the most common forms of cybercrime across the globe. Furthermore, the continuous rise in incidents of cyberstalking is becoming a growing cause for concern, particularly for a developing nation such as India. According to statistics released by Statista in 2022, Maharashtra recorded the highest number of cyberstalking incidents against women and children among all the states in India.¹

II. UNDERSTANDING CYBERSTALKING AND THE PREVAILING PATTERN

In its simplest form, 'cyber' may be defined as anything revolving around virtual reality, that is, the virtual world. Stalking may be described as unwanted, unsolicited and persistent attention that instils fear, anxiety or a sense of impending danger in an individual. As a physical activity, stalking involves the continuous pursuit of a person; it entails physically following someone to such an extent that it creates a psychological apprehension that one is at risk or in danger. It involves subjecting the victim to constant scrutiny, thereby driving the individual into a genuine state of fear or anxiety. When an attempt to stalk is made through a technical device on a digital platform, it constitutes the crime of cyberstalking. For instance, stalking through online social networking applications, sending incessant messages, breaching someone's private information and using that information to intimidate the individual collectively constitute the crime of cyberstalking. Unlike in developed nations, where cyberstalking is a gender-neutral offence, in India it is a gender-specific crime. In India, the crime of cyberstalking is predominantly perpetrated against women. Crimes against women remain a matter of grave concern for the

¹ Cyber Stalking: Number of Victims by State, India 2022, STATISTA (2023).

nation; it is now imperative to ensure the safety and security of women not only in the physical world but also within the digital realm. India is a nation where numerous age-old gender-related stereotypes continue to form an integral part of the socio-cultural fabric, and these stereotypes influence prevailing attitudes regarding how individuals of a specific gender should be treated and what their status within society ought to be.

In India, women constitute 48.41 per cent of the population, according to World Bank statistics, yet they remain the most victimised demographic in the country.² The primary reason for this is their gender identity and society's prevailing attitudes towards their gender. In the United States, 18 U.S.C. Section 2261A defines cyberstalking as the use of electronic means against any individual with the intent to cause emotional distress, or the attempt to do so, or to instil a fear of serious bodily injury or death.³ In the United Kingdom, the law pertaining to cyberstalking is found under Section 2A of the Protection from Harassment Act 1997.⁴ This section defines stalking as following a person, contacting or attempting to contact them through any medium, or monitoring that person's use of the internet, email or any other form of electronic communication, among other acts. In India, under Section 78 of the recently enacted criminal code, the Bharatiya Nyaya Sanhita, 2023, stalking is defined as conduct by any man who follows a woman and, despite her explicit refusal or indication of disinterest, repeatedly contacts or attempts to contact her with the intent of fostering personal interaction, or who monitors a woman's use of the internet, email or any other form of electronic communication.⁵

From the United States perspective, cyberstalking is characterised as the malicious use of electronic means with the specific intent of inflicting emotional distress or issuing threats of physical harm. The definition is confined solely to such malicious usage and the malevolent intent to cause harm, whereas the legislative codes of the United Kingdom and India define cyberstalking within a much broader context, encompassing activities such as the persistent monitoring of internet usage, following a victim or making contact with them. Both the United States and the United Kingdom adopt a gender-neutral approach to cases of cyberstalking. By contrast, within the Indian legislative framework, cyberstalking under Section 78 is categorised under Chapter V of the Bharatiya Nyaya Sanhita, 2023, which deals specifically with offences against women. This arrangement renders cyberstalking a gender-specific offence, defined as the persistent pursuit of a woman by a man, and the monitoring of her internet activities, despite her explicit refusal or expression of disinterest. This situation raises a pertinent question: why,

² Population, Female (% of Total Population) — India, THE WORLD BANK.

³ 18 U.S.C. § 2261A (2018).

⁴ Protection from Harassment Act 1997, c. 40, § 2A (U.K.).

⁵ The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023, § 78 (India).

unlike in other parts of the world, is cyberstalking treated as a gender-specific issue in India? The answer involves various social, cultural and psychological factors intertwined with prevailing societal attitudes towards women. In Indian society, the gender roles and identities of women are often relegated to a secondary status; the prevailing patriarchal system in the country reinforces the entrenched notion that women are mere objects of gratification and that their consent holds no significance.

Cyberstalking has therefore become an easy avenue for perpetrators to fulfil their malicious intentions. Cyberspace facilitates cyberstalkers in sexually harassing victims, ensnaring them in their traps, intimidating them and inflicting harm upon them both mentally and physically. Furthermore, a research survey conducted by Statista revealed that in 2022 more than 3,400 cases of cybercrimes involving sexual harassment or exploitation were reported across India, marking a significant surge in such cybercrimes compared to the years 2016 and 2017.⁶ Technology affords stalkers the luxury of anonymity, as they can readily mask their identities in order to exploit their victims. One of the earliest instances of cyberstalking in India is the well-known case of Ritu Kohli, which came to light in 2001. Ritu Kohli, an Indian woman, was stalked by Manish Kathuria, who, with malicious intent, illegally engaged in chat conversations on the online platform www.mirc.com by impersonating her. He deliberately employed obscene and vulgar language, shared her telephone number and solicited others to chat with her. Consequently, Ritu Kohli began receiving telephone calls from both within India and abroad, in the course of which callers subjected her to obscene conversations. At the time, the existing legal framework classified the offence under Section 509 of the Indian Penal Code, 1860, which pertains to outraging the modesty of a woman, yet the statute did not explicitly recognise the outraging of a woman's modesty through digital media as a punishable offence. It was only in the wake of this case that amendments were introduced to the laws governing women's safety within the cyber domain.⁷

In Indian criminal jurisprudence, *mens rea*, that is, the criminal intent or state of mind of the offender, is regarded as one of the most critical elements required to establish the commission of any crime. As one delves deeper into the nuances of cyberstalking, it becomes imperative to understand the psychological patterns and intentions of cyberstalkers. Stalking is generally understood as a repetitive behaviour; it may also be viewed as a reward-oriented attitude towards victims, in which the perpetrator readily conceals their true identity and derives a sense

⁶ Cyber Crimes Related to Sexual Harassment and Exploitation in India 2016–2022, STATISTA (2023).

⁷ *Manish Kathuria v. Ritu Kohli* (2001) (unreported), discussed in Cyberstalking and the Indian Jurisprudence (2022); see The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860, § 509 (India).

of satisfaction or reward from psychologically tormenting their victims. A significant research initiative conducted by the Global Sociological Review undertook an in-depth exploration of the psychological and sociological factors underlying stalker behaviour. In that study, stalkers were categorised into three primary groups based on their psychological intentions, as follows.⁸

A. Obsessive cyberstalkers

This category concerns the obsessive nature of the stalker. Such stalkers are unwilling to accept that the relationship between the stalker and the victim has come to an end. In most cases, the stalker uses a defunct relationship as a pretext to intrude upon the victim's private life, finding it difficult to accept that the bond once shared with the victim no longer exists. Suppose that 'A' was engaged to 'S', but that, due to certain circumstances, the engagement was called off. Driven by a psychological obsession to maintain control over the life of 'S', 'A' cyberstalks 'S' and issues threats to prevent 'S' from moving on or becoming engaged to anyone else. In this scenario, 'A' would be classified as an obsessive cyberstalker.

B. Delusional cyberstalkers

The stalker in this category may be grappling with a form of mental impairment, such as schizophrenia. They harbour the belief that someone is in love with them, whereas, in reality, they have never even met that individual. In simple terms, this category may be understood as a situation in which the perpetrator, due to a state of cognitive dissonance, constructs a set of personal beliefs and subsequently conducts themselves in accordance with those beliefs.

C. Vindictive cyberstalkers

Cyberstalkers of this type harbour anger towards their targets stemming from some minor encounter, whether real or imagined. Stalkers who adopt this approach engage in vengeful and retaliatory acts in response to any perceived slight or wrongdoing that may have occurred. For instance, upon discovering that they have been betrayed by a partner, they may seek to exact revenge and take retaliatory measures, both to achieve personal gratification and to create a deterrent effect for the victim. Stalkers diagnosed with various mental disorders or cognitive impairments are often offenders who have lost their connection with physical reality, having retreated into their own internal, insular worlds. Numerous studies have indicated that the majority of cyberstalkers possess antisocial personalities; narcissism, in particular, is one personality trait frequently associated with cyberstalkers. Narcissism, or narcissistic behaviour,

⁸ Zainab Bibi & Ahmed Abbasi, *Cyber Stalking: Sociological and Psychological Perspective*, VII GLOBAL SOC. REV. 159 (2022).

is characterised by self-obsession and extreme self-centredness, often accompanied by a sense of entitlement. Such behaviours are underpinned by a lack of empathy towards others, which in turn leads to manipulative and controlling conduct. Social and digital platforms afford a degree of anonymity that enables individuals with antisocial personalities to masquerade as having a socially adjusted persona. Cyberstalking is a crime involving the misuse of technology to perpetrate harassment and violence against others within the personal sphere. The ease of global access, unfettered by physical boundaries, has made it possible to harass individuals located in any part of the world.

III. LEGAL RESPONSES AND CHALLENGES

The objective of every law is to ensure safety and to regulate those forms of human behaviour that have an adverse impact on society as a whole. Laws are an integral part of life; they require individuals to realign their ethics, values and conduct to suit the needs of society. It is through law that justice is served, implying that every individual is entitled to equal opportunities and to the right to lead a dignified life. The Constitution of India stands as one of the most voluminous constitutional documents in the world; it embodies the values of equality, justice, liberty and freedom for all human beings. The principles of equality and liberty enshrined in Articles 14, 15 and 21 of the Constitution also reflect the spirit of the fundamental right to live a secure life.⁹ In India, crimes such as cyberstalking disproportionately target women; indeed, women continue to be the primary targets even within the digital realm. Cyberstalking constitutes a form of harassment perpetrated on cyber platforms; as society increasingly comes to terms with the nuances of technological advancement, cybercrime is emerging as a formidable threat to the present generation. To combat cybercrimes effectively and safeguard the cyber security of the populace, necessary reforms must be instituted within the legal framework.

In India, the laws governing cyberspace are of relatively recent origin when compared with the statutes enforced in other nations across the globe. Prior to 2013, India possessed no specific legislation directly addressing or regulating cyberstalking; it was only in the aftermath of the Delhi gang-rape incident of 2012 that the imperative to amend the criminal law was seriously contemplated. The Justice Verma Committee was constituted with the specific mandate of formulating robust recommendations to ensure swift justice and stringent punitive action against perpetrators of sexual assault and crimes against women. The Committee, chaired by the Honourable Justice J.S. Verma, comprised two other distinguished members: the

⁹ INDIA CONST. arts. 14, 15, 21.

Honourable Justice Leila Seth and India's former Solicitor General, Gopal Subramaniam. Under the amendments made to the criminal law, several provisions were enacted to ensure the safety of women in both the physical world and the digital sphere. Chapter Seven of the Committee's report, titled 'Sexual Abuse of Children', notes that, amidst the categories of offences such as molestation, stalking and sexual harassment, there exists another offence known as 'sexual ragging'.¹⁰ Ragging constitutes an abuse of power; it frequently reinforces pre-existing, archaic and harmful gender-based stereotypes prevalent within society. Sexual ragging may be characterised as a specific form of ragging in which an individual is targeted on the basis of their sexual orientation or gender identity. This form of ragging manifests as voyeurism, the dissemination of obscene material for purposes of revenge, that is, revenge pornography, and other related cybercrimes, offences that were subsequently recognised and codified under the Criminal Law (Amendment) Act, 2013. The 2013 Amendment Act introduced the following principal provision.

Section 354D of the Indian Penal Code, 1860, defined the act of stalking and provided for the punishment thereof. This provision has now been replaced by Section 78 of the Bharatiya Nyaya Sanhita, 2023; however, the regulatory framework and structure of the law remain substantially unchanged. Under Section 78, any man who follows a woman and, despite her clear indication of disinterest, repeatedly contacts or attempts to contact her with the intention of establishing personal interaction, or who monitors a woman's use of the internet, email or any other form of electronic communication, commits the offence of stalking. Such conduct is not deemed to constitute stalking where the man proves that it was pursued for the purpose of preventing or detecting crime and that he had been entrusted by the State with the responsibility of preventing and detecting crime; that it was done in compliance with any law, or with any condition or requirement imposed by any person under any law; or that, in the particular circumstances, the conduct was reasonable and justified. A person who commits the offence of stalking is liable, on first conviction, to imprisonment of either description for a term which may extend to three years, together with a fine, and, on a second or subsequent conviction, to imprisonment of either description for a term which may extend to five years, together with a fine.¹¹

Section 77 of the Bharatiya Nyaya Sanhita, 2023, addresses voyeurism. It provides that whoever watches, or captures the image of, a woman engaging in a private act in circumstances where she would usually have the expectation that neither the offender nor any other person at the

¹⁰ *Report of the Committee on Amendments to Criminal Law* ch. 7 (2013) (Justice J.S. Verma Committee).

¹¹ The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023, § 78 (India); see The Criminal Law (Amendment) Act, 2013, No. 13, Acts of Parliament, 2013 (India).

behest of the offender would be watching her, or who disseminates such an image, is liable, on first conviction, to imprisonment of either description for a term of not less than one year, which may extend to three years, together with a fine, and, on a second or subsequent conviction, to imprisonment of either description for a term of not less than three years, which may extend to seven years, together with a fine.¹² For the purposes of this section, a 'private act' includes an act performed in a place where, in the circumstances, a reasonable expectation of privacy exists and where the victim's genitals, posterior or breasts are exposed or are covered only by underwear; or where the victim is using a lavatory; or where the victim is engaging in a sexual act that is not ordinarily performed in public. Where the victim consents to the capture of images or to the recording of the act, but does not consent to their dissemination to third parties, any such dissemination is deemed to be an offence under this section.

Section 77 thus safeguards the privacy and dignity of women, voyeurism being a gender-specific crime committed against women. Both Section 77 and Section 78 serve as a response to the misuse of the internet in violation of women's right to a safe existence. Voyeurism is an offence against the right to privacy; in common parlance, it implies recording or watching a woman in a situation in which she expects complete privacy. The term 'disseminates', as used in Section 77, refers to the act of circulating recorded images. Examples of acts constituting voyeurism include the unauthorised or non-consensual use of hidden cameras in private settings, peeping, the use of binoculars and spying. Furthermore, where an offender captures an image of a woman and shares it online or through other channels, such an act also falls within the purview of the offence of voyeurism. There may also be instances in which voyeuristic material is used for the purposes of blackmail, extortion or online harassment. Revenge pornography may be regarded as a grave misuse of voyeuristic material.

Another significant piece of legislation governing the virtual landscape in India is the Information Technology (Amendment) Act, 2008. This Act enacts provisions designed to ensure cyber security, privacy on digital platforms and data protection. While it does not specifically regulate cyberstalking, it prohibits the unauthorised use or violation of privacy and confidentiality, and it prescribes penalties for the transmission of offensive messages through communication services. Section 72 of the Information Technology (Amendment) Act, 2008, specifically addresses the breach of privacy or confidentiality.¹³ Privacy may be defined as the act of concealing or keeping separate any information or data that an individual wishes to restrict to themselves. A breach of privacy or confidentiality refers to a situation in which an offender

¹² The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023, § 77 (India).

¹³ The Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009, § 72 (India).

gains access to a victim's personal information without their consent and makes it public, thereby causing or threatening to cause harm to the victim. Such confidential or private information may include images, conversations, electronic records and registers, and similar items.

Enforcing and implementing laws designed to curb cybercrime presents numerous challenges. The internet serves as a medium of global reach and connectivity that transcends physical barriers; this gives rise to cross-border jurisdictional issues, complicates the task of locating digital evidence and traces, and makes it difficult to keep pace with the rapidly evolving complexities of technological platforms. Cyber laws in India face similar challenges. First, the rapid advancement of technology necessitates the swift adoption of corresponding technical solutions, an area in which India currently lags behind. Secondly, incidents of cyberstalking in India are under-reported, largely on account of prevailing societal attitudes towards such crimes. Following consultations with experts, the Justice J.S. Verma Committee report highlighted that heinous acts such as stalking, voyeurism and harassment are often dismissed as trivial offences. There is an urgent need to transform the prevailing attitudes and perceptions surrounding this crime. The low rate of reported cyberstalking incidents in the country stems from a lack of awareness regarding the offence and a tendency to overlook its gravity. Furthermore, the availability of adequate resources to facilitate prompt action against cybercrimes must be given due consideration. A dearth of resources or a lack of awareness among law enforcement officials would only serve to embolden perpetrators. Triveni Singh, a former Indian Police Service officer specialising in the resolution of cybercrimes, has stated that India requires a national-level cybercrime investigation bureau, capacity-building and skill-development initiatives for law enforcement personnel, and a dedicated cyber forensic laboratory in every police station.

Moreover, preserving digital evidence often proves to be a challenging endeavour, as such data is susceptible to ready manipulation or deletion. Digital evidence encompasses social media activity; location data obtained through GPS; threatening or malicious electronic communications such as emails, text messages and chat logs; IP addresses; the perpetrator's browsing history and online habits; and digital files and online profiles. Given their sensitive nature, these evidentiary elements may be readily altered or erased. Evidence is the primary source that influences and supports the determination of a situation; it is therefore crucial in concluding whether or not a crime has occurred.

Meeting these challenges requires careful deliberation. In short, there are four principal challenges in tackling cyberstalking, as set out below.

A. Cross-border jurisdiction

Cross-border jurisdiction is an international challenge that must be addressed. It requires international cooperation to meet such global challenges. Mutual legal assistance treaties or agreements may prove an effective strategy for combating this global problem. Such treaties allow countries to reach beyond their own borders to interrogate suspects; they provide for cooperation between countries to ensure the exchange of information and law enforcement across regional boundaries. As an example, the Convention on Cybercrime, also known as the Budapest Convention, was the first international treaty relating to computer crimes. It was opened for signature by the Council of Europe at Budapest in November 2001 and entered into force on 1 July 2004. The aim of the treaty was to ensure international cooperation in reducing cybercrimes against humanity. Such conventions and treaties help to establish global provisions and rules that prevent the misuse of the internet to harm others, and enable member countries to resolve cross-border jurisdictional issues more readily.¹⁴

B. Adopting technological advancements

Technological advancements are changing the digital sector every day, and the world is witnessing the development of artificial intelligence and updated technologies that increasingly surpass human capabilities. Parallel to these evolutionary reforms, cyber law faces many obstacles. To tackle this problem, the Online Safety Act 2023, passed by the United Kingdom, represents a remarkable legislative shift. The Act seeks to ensure the online protection and safety of children and adults by imposing a reasonable liability on social media companies and various online search engines.¹⁵ This approach helps to implement solutions from the grassroots level, so that technology itself assists in coping with the new challenges arising from its development.

C. Under-reporting

Under-reporting refers to the failure to report a specific situation or incident. A lack of support for victims, a complacent attitude towards crime and indifferent societal behaviour are all factors that contribute to the under-reporting of specific offences. To combat the mindset that leads to under-reporting, attitudes must undergo a transformation. The gravity of a crime, whether committed online or offline, must be formally acknowledged and addressed. Furthermore, it is essential to raise awareness regarding the formal remedies available to victims, as well as the inherent dangers associated with cybercrimes. For instance, India currently facilitates the reporting of cybercrimes by women through its National Cyber Crime

¹⁴ Convention on Cybercrime, opened for signature Nov. 23, 2001, E.T.S. No. 185 (entered into force July 1, 2004).

¹⁵ Online Safety Act 2023, c. 50 (U.K.).

Reporting Portal. Notably, this platform allows for anonymous reporting and enables victims to track the progress of the investigation into their cases. However, owing to a lack of awareness regarding such initiatives, India continues to face the challenge of under-reporting in the realm of cybercrime.

D. Preservation of digital evidence

The preservation and collection of digital evidence constitute a major challenge in the investigative process. Fundamentally, this concern may be addressed through rigorous research and technological advancement that keeps pace with digital evolution. Secondly, it is crucial to foster awareness among individuals regarding the importance of safeguarding their data and information, which often contain evidentiary fragments vital for identifying and implicating perpetrators. Consequently, the availability of a substantial pool of digital forensics experts is an absolute necessity. Most effectively, forensic imaging techniques should be employed to create exact duplicates of collected data; this ensures data integrity and prevents the tampering or alteration of original evidence. Additionally, to ensure proper reporting and prompt action against cybercrimes, dedicated cyber security cells should be established within every police station.

IV. IMPACT ON VICTIMS: SOCIAL AND PSYCHOLOGICAL

As described by the World Health Organization, mental health denotes a state of well-being that enables people to cope with the stresses of life, realise their potential, learn well, work well and contribute to their community. The World Health Organization has further observed that, in 2019, 970 million people globally were living with a mental disorder, with anxiety and depression being the most common.¹⁶ Mental health is an important part of a person's life; its well-being determines the well-being of other components of life, such as healthy relationships, physical health and fitness, and personal development. Cyberstalking has harmful consequences for mental health and well-being, producing effects such as depression, anxiety, fear, insomnia and post-traumatic stress disorder. Depression, as described by the American Psychiatric Association, is a common and serious mental disorder that negatively affects how a person feels, thinks, acts and understands the world.¹⁷ Cyberstalking may cause depression by negatively affecting a person's ability to feel, act and understand, such that the victim is conditioned to a persistent feeling of uncertainty. The victim may come to perceive the world as a dangerous place and may feel as though they are constantly being pursued. In addition, cyberstalking may

¹⁶ World Health Org., *World Mental Health Report: Transforming Mental Health for All* (2022).

¹⁷ What Is Depression?, AM. PSYCHIATRIC ASS'N.

cause serious feelings of anxiety and fear. Anxiety is a serious disorder in which a person experiences fear regarding situations that would ordinarily be unremarkable; it generates negative expectations regarding the consequences of life. In the context of cyberstalking, the victim may feel anxious and anticipate dire consequences from the ordinary actions they take, perceiving themselves to be continually followed and under surveillance. The feeling of fear and the loss of confidence in the normal routine of life make for a miserable existence for victims of cyberstalking. They may experience flashbacks and become fixated on the situation in which the cyberstalking first occurred, which impedes the normal course of their lives and their ability to foster relationships with those around them. Insomnia is a condition in which a person is unable to sleep; the victim may experience insomnia owing to frightening thoughts and flashbacks. In addition, cyberstalking has an impact on social well-being. Social prestige is accorded the utmost importance in India, often being preferred above personal boundaries and individual happiness. It is challenging to acknowledge that, in many cases, reports of crimes against women are suppressed simply because they bear upon the social standing of a family. Gender-specific crimes, and crimes committed against women, frequently attract a victim-blaming approach within the nation. For instance, in the context of cyberstalking, a woman may be blamed for maintaining social media accounts, for engaging in conversation with a stranger, or for sharing pictures of herself on social media platforms. As a result of such an approach, the victim's family often refrains from reporting or complaining of the crime, and the victim is demeaned by society. This prevailing socio-cultural approach to cybercrime results in harm to the social prestige and reputation of the family, and it calls for a change in the mindset and prevailing attitude towards crimes related to women.

V. CONCLUSION AND THE WAY FORWARD

Technology is bringing about revolutions in various forms. While it has historically served as a double-edged sword for humanity, the emergence of artificial intelligence in daily routines necessitates a formal and deliberate examination of its implications. In this era of digitisation, personal safety and privacy remain areas of vulnerability. Online security measures must evolve in tandem with the increasing complexities of technological advancement. For a long time, women in India have faced criminal adversities in both the physical and the digital realms. The safety of women must now be advocated in practical terms, and it must be ensured that the development of new technologies does not result in an escalation of crimes against women. Rather than leading to violations of human safety and privacy, the advancement of artificial intelligence and technology should serve to enhance human security and protection. Navigating the landscape of artificial intelligence will present a demanding challenge for privacy and cyber

security. Cyberstalking may be understood as a form of online harassment and misuse of the internet. To curb its proliferation, initiatives promoting internet ethics and awareness campaigns should be launched. Victim empowerment is another matter of critical importance; victims must be afforded appropriate representation and opportunities to share their experiences and to educate others about the consequences of cyberstalking. Social media platforms can provide the necessary impetus in the right direction, and may be used to raise public awareness regarding available remedies and personal coping strategies. Social media campaigns are often recognised as effective tools for fostering awareness and knowledge concerning such crimes. As previously noted, cyberstalking can have detrimental effects on both physical safety and mental well-being. With the advent of artificial intelligence, a time may eventually arrive when cybercrimes evolve into a major existential threat to humanity. Artificial intelligence facilitates the creation of self-evolving systems, a development that could potentially cast a dark shadow over the future of human safety. As a rapidly developing nation, India must prioritise investment in technological research and development. It must keep pace with global technological advancements and prioritise cyber security, as this is likely to become an increasingly pressing concern for humanity.

VI. BIBLIOGRAPHY

1. Parveen Sadotra & Jasbir Kour, *The Technical and Legal Perspective of Cyber Stalking*, Int'l J. Res. Pedagogy & Tech. Educ. & Movement Sci.
2. Ameema Miftha, *The Social, Legal and Technical Perspectives of Cyber Stalking in India*
3. Sapna Sukrut Deo, *Cyber Stalking and Online Harassment: A New Challenge for Law Enforcement*.
4. Kagan Kircaburun, Peter K. Jonason & Mark D. Griffiths, *The Dark Tetrad Traits and Problematic Social Media Use: The Mediating Role of Cyberbullying and Cyberstalking*, 135 *Personality & Individual Differences* 264 (2018).
5. Zainab Bibi & Ahmed Abbasi, *Cyber Stalking: Sociological and Psychological Perspective*, VII *Global Soc. Rev.* 159 (2022).
6. *Report of the Committee on Amendments to Criminal Law* (2013) (Justice J.S. Verma Committee).
7. K.V. Ravi Kumar, *Cyber Stalking and Online Harassment in India: A Socio-Legal Analysis*.

8. Udit Agnihotri, *The Cyber Stalking Situation in India: A Social, Legal and Technological Viewpoint*.
9. *Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and Therapeutic Jurisprudential Perspectives*.
