# Artificial Intelligence and Privacy Breaches: A Socio-Legal Analysis of Digital Crimes against Women in India

Sunidhi Singh and Sufiya Ahmed*

*Department of Law, Babasaheb Bhimrao Ambedkar University, Lucknow, India*

**Abstract:** The issue of Digital Crimes Against Women in India is a growing concern within society today due to the rapid growth of Internet Access throughout the Country, as well as Digital Technologies. Within this discussion are some of the most common types of Digital Crime Against Women including Cyber-Bullying, Trolling and the abuse of Deep Fakes. Cyber-Bullying is defined as the intentional act of using Digital Platforms to abuse or threaten or degrade women through harassment. This has been shown to cause significant Psychological Distress for many women. Trolling is another common form of Digital Crime that occurs to women. This is the posting of inflammatory statements or comments meant to incite emotional responses and create further marginalization for women in Online Spaces. With the introduction of Deep Fake Technology, this has created an additional dimension of Digital Harassment. The objective of this paper is to explore the Multidimensional Nature of Digital Crime against Women in India. Digital Crimes will be examined through cyber-bullying, trolling and deep fakes.

This paper enhances the current body of Law in India by showing where India's Digital Laws are deficient regarding AI-based and Deepfake-generated Gendered Harms. In addition, it proposes to create additional Targeted Technology-Specific Regulations to protect Women's Digital Privacy and Dignity.

**Keywords:** Digital crime, cyberbullying, trolling, deepfakes, women's safety, India.

## INTRODUCTION

According to the WHO, "The United Nations defines violence against women as 'any act of gender-based violence that results in, or is likely to result in, physical, sexual, or mental harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life".[1]Crimes against women encompass offences that specifically target women due to their gender and involve acts of violence or exploitation directed exclusively at them. While women may fall victim to general crimes such as cheating, murder, or robbery, certain crimes are distinctively recognised as "crimes against women" because they affect women uniquely. These crimes are broadly categorised under two classifications, with one being crimes codified under the Indian Penal Code (IPC). The IPC identifies seven specific offences as crimes against women. These include rape under Section 376, kidnapping and abduction under Sections 363 to 373, dowry deaths under Section 304-B, and physical or mental torture under Section 498. Other offences in this category include molestation under Section 354, sexual harassment under Section 509, and the importation of girls under Section 366-B. The penal laws which are available to women as per the Indian penal code are as follows.

The offence of rape represents one of the gravest violations of a woman's bodily autonomy and dignity. Derived from the Latin term *rapio*, meaning "to seize," rape involves sexual intercourse with a woman without her consent, often through force, fear, or deception. Indian jurisprudence views this act as a heinous infringement of personal integrity, as stated in *Phul Singh v. State of Haryana*[2]. [3]Section 375 of the Indian Penal Code (IPC) defines rape and emphasises that "penetration is sufficient to constitute sexual intercourse necessary for the offence of rape." This provision underscores that the depth or completion of penetration is irrelevant. The courts have clarified that even the slightest penetration satisfies the legal threshold for establishing rape. This principle was firmly upheld in *G. Misra v. State of Orissa*[4]. Additionally, it is not necessary to prove the emission of semen to establish the completion of sexual intercourse, as the law regards proof of penetration sufficient to constitute the offence. In cases where penetration is not conclusively established, but the intent to commit rape is evident, the accused may be convicted of attempted rape. If the prosecution fails to prove the intent to

*Address correspondence to this author at the Department of Law, Babasaheb Bhimrao Ambedkar University, Lucknow, India; E-mail: sufi.bbau@gmail.com

[1]Violence against women available at https://www.who.int/news-room/fact-sheets/detail/violence-against-women

[2]AIR 1980 SC

[3]Indian Penal Code, Chapter XIV: Crimes Against Women (Manupatra, 2025) http://student.manupatra.com/Academic/Abk/Indian-Penal-Code/chapter14.htm

[4]AIR 1975

commit rape, the individual may still face conviction for the lesser charge of indecent assault[5].

Each of these crimes underscores the targeted nature of violence and exploitation faced by women, reflecting the need for stringent legal protections and societal awareness to address such issues effectively.[6] In the year 2023 Georgetown Institute released a women peace, and Security Index in which India ranks 128 out of 177 countries in terms of women's inclusion, justice, and security.

In view of the presence of such legislated safeguards under the Indian Penal Code, the current legal regime is still predominantly targeted towards physical and traditional forms of violence committed against women, and not adequately addressing associated contemporary forms of gender violence in the digital space. In particular, it must be observed that there is no dedicated provision in the Indian legal regime concerning artificial intelligence and deepfakes to explicitly deal with non-consensual digital content, synthetic media abuse, and technology-driven privacy violation committed through the use of artificial intelligence, which are currently being used to target women in a manner warranting significant legal intervention for providing a necessary remedy in the current gender violence regime in the context of artificial intelligence.

## INDIAN CONSTITUTIONAL PROVISIONS RELATED TO PRIVACY

The Constitution of India guarantees equal rights to women, ensuring their protection and empowerment under various provisions. Article 21 of the Indian Constitution safeguards the right to life and personal liberty for all citizens, as well as women. Additionally, several sections of the Constitution, such as the Directive Principles of State Policy, the Preamble, and the Fundamental Rights, emphasize the protection and promotion of women's rights. To further enhance the safety and well-being of women, the National Commission for Women at the central level and at the state level have been established. These bodies aim to address women's issues and provide institutional support for their welfare[7].

The Indian Penal Code also contains provisions to protect women and deter gender-based violence. Over the years, Parliament has enacted several laws to safeguard women's rights and promote gender equality. Legislative efforts, coupled with initiatives by state and central governments, have been supported by non-governmental organisations to advance women's empowerment and address issues affecting their safety and dignity. Despite these measures, crimes against women continue to persist, highlighting the need for more effective implementation of laws and sustained efforts to create a safer and more equitable society. However, the advancement in technology has also led to an increase in the commission of cybercrime against women. Cybercrime refers to any unlawful activity in which a computer serves as the principal instrument for perpetrating the offense. This concept has broadened to encompass various illicit acts conducted via digital platforms, including offenses committed on the web, violations of Internet-related laws, and unauthorized activities facilitated through online networks. It also includes crimes such as computer-related fraud, cyberstalking, identity theft, and the distribution of contraband through digital means. Additionally, cybercrime extends to offenses that compromise digital infrastructure, such as deploying malicious software to disrupt operations[8].

## CYBERCRIME AGAINST WOMEN

Cybercrime has emerged as a persistent worldwide issue, intensifying with the speedy development of technology. Among the most concerning aspects of this phenomenon is the increasing victimization of women in the digital space, which poses a significant threat to personal security and privacy. While India was among the pioneering nations to introduce the Information Technology Act, 2000, to address cyber-related offences, the legislation remains insufficient in adequately safeguarding women against online threats such as cyberstalking, harassment, and image-based abuse. The absence of specific provisions addressing gender-based cyber violence highlights a critical gap in the legal framework, necessitating urgent reforms to ensure comprehensive protection for women in cyberspace.

[5]Indian Penal Code, supra note 1.

[6]Mangoli R.N. and Tarase Ganapati M., "Crime Against Women in India: A Statistical Review," *International Journal of Criminology and Sociological Theory*, Vol. 2, No. 2,December 2009, pp. 292-302.

[7]Kharwar Shiv and Kumar Vivek, "Crimes Against Women in the 21st Century," *SSRN Electronic Journal* (2021), DOI: 10.2139/ssrn.3762049

[8]Dr. Monika Jain, "Victimization of Women Beneath Cyberspace in Indian Upbringing" *Bharati Law Review* 1 (Apr.–June 2017).

Cybercrimes are typically categorized into three main groups: offences against individuals, property, and government institutions. Crimes targeting individuals include online harassment, cyberstalking, and identity theft, while offences against property involve hacking, data breaches, and financial fraud. Cybercrimes against governments may encompass cyberterrorism, hacking into state systems, and disrupting essential services. Given the widespread reliance on digital technology, cybercrime has emerged as a significant global concern, necessitating stringent legal frameworks and cybersecurity measures to mitigate its impact.

## DEEP FAKE

Over the past two decades, gender-based violence has risen significantly, with an estimated one out of three women experiencing some form of violence at least once in their lifetime, as per the World Health Organisation. Violence against women encompasses a wide range of gender-specific acts, primarily targeting women and girls, that may inflict immediate or long-term harm. These acts can manifest in various forms, including physical, sexual, and psychological abuse, often leading to profound personal and societal consequences[9].

The World Health Organisation defines "violence against women as any act of gender-based violence that causes or is probable to cause bodily, sexual, or mental harm or suffering. This includes intimidations, coercion, or the arbitrary deprivation of liberty, whether happening in public or private spheres. Such violence remains a pervasive global issue, necessitating comprehensive legal, social, and policy interventions to protect and empower women while addressing the root causes of gender-based violence[10]. Deepfakes are created with the help of GANs, which stand for Generative Adversarial Networks; a deep learning technology developed by Ian Goodfellow back in 2014. GANs are made up of two competing neural networks: a generator that produces synthetic content and a discriminator that assesses whether the content is real or fake. After constant adversarial training, the generator keeps improving to create realistic output while the discriminator continuously improves its skills in identifying falsified material, thereby yielding very convincing media deepfakes.

Further technical repetition with respect to GAN working has been intentionally avoided to prevent redundancy.

This can be used for perfect good things in entertainment, education, research areas, among others. However, its misuse has, in turn, developed into a big concern under the aspect of digital crime. Through malicious execution, deepfakes have facilitated the spread of misinformation, character assassination, identity fabrication, and breaches of privacy against women and other highly vulnerable targets. These events highlight a pressing necessity for a legal approach to deal with these incidents, ethical digitization practice, and increasing awareness among the general public[11].

## MISINFORMATION AND FAKE NEWS

Deepfake technology is increasingly being utilized to generate highly realistic yet deceptive digital content, including videos, audio recordings, and images. These artificially manipulated media can be employed to disseminate misinformation, often blurring the distinction between authentic and fabricated content. The capacity of deepfakes to convincingly alter visual and auditory representations raises significant concerns, as such content may be used to mislead audiences, tarnish reputations, and facilitate various forms of fraudulent or unethical activities. Given the sophistication of deepfake algorithms, distinguishing manipulated content from genuine material poses a considerable challenge, thereby exacerbating the potential risks associated with its misuse. Deepfake technology has emerged as a significant tool for digital manipulation, posing serious risks to individuals, institutions, and democratic systems. The ability to fabricate highly realistic yet deceptive content enables malicious actors to compromise reputations, distort public perception, and erode trust in legitimate sources of verified information. Such technology can be strategically deployed to spread false narratives, influence political outcomes, and weaken democratic institutions by misleading the public and creating confusion.

In 2024, the World Economic Forum published The Global Risks Report, which highlights the increasing

[9]Jennifer Laffier & Aalyia Rehman, *Deepfakes and Harm to Women*, 3 J. Digit. Life & Learning 1 (2023), available at https://doi.org/10.51357/jdll.v3i1.218

[10]Jennifer Laffier & Aalyia Rehman, *supra note 1*

[11]Daniel L. Byman, Chongyang Gao, Chris Meserole & V.S. Subrahmanian, *Deepfakes and International Conflict*, Foreign Policy at Brookings (Jan. 2023), available at https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf

danger of misinformation and disinformation, identifying them as the most critical threats facing the global community in the coming years. The rapid proliferation of manipulated content, particularly through digital and social media platforms, makes it increasingly difficult to distinguish between authentic and falsified information. This growing challenge underscores the necessity for robust regulatory frameworks, the development of advanced detection technologies, and heightened public awareness to counter the potential harms posed by deepfake-driven misinformation.[12] The ramifications of deepfakes on public confidence hold substantial importance. When applied to distort the image of politicians, public servants, and business leaders, they have the capacity to diminish individuals' trust in governmental bodies, media platforms, legal frameworks, and private establishments.

In contrast to conventional disinformation, deepfake information is imbued with heightened realism, persuasiveness, plausibility, and dissemination intent.[13] As a result, viewers may develop erroneous beliefs due to the prevalence of deepfake news. Deepfake videos have the potential to distort collective recollections of public events.[14] This can have serious consequences for public perception, trust, and decision-making. Deepfakes possess the potential to be utilized in a malicious manner for the purpose of spreading misinformation or defaming individuals. As a result, the identification and detection of Deepfakes show a serious part in enhancing the credibility of social media platforms and other media-sharing websites. The easy accessibility of audio-visual content through social media, coupled with the accessibility to modern tools such as TensorFlow or Kera's, AI software, and cost-effective computing resources, along with the swift advancement of deep-learning (DL) methods, specifically Generative Adversarial Networks (GAN), has facilitated the creation of deepfakes with the intention of disseminating disinformation, monetary frauds, hoaxes, and disrupting government operations. Deepfake content can spread rapidly on social media and other online platforms, making it challenging for victims to control the dissemination of false information or to clear their name.

India's unfortunate reputation as the disseminator of misinformation is linked to its high rate of Internet usage and the growing trend of social media engagement. The country boasts a staggering 323 million internet users, with 67% residing in urban areas and the remaining 33% in rural regions. The lack of media literacy stands out as a pivotal element contributing to the proliferation of misinformation during the pandemic[15]. Throughout the COVID-19 pandemic, false information regarding remedies and therapies spread rapidly through various social media channels in India. One notable case revolved around a widely circulated video promoting the consumption of cow urine as a preventive or curative measure against COVID-19. Despite being discredited by health authorities, the video amassed millions of views and played a role in the dissemination of misinformation, thereby posing potential health hazards as certain individuals embraced and acted upon the inaccurate content.

## POLITICAL MANIPULATION

Political deepfake information may have an influence on the attitudes of recipients toward politicians. Deepfake news with high source vibrancy amplifies the reliability and engagement intention of fraudulent broadcasts[16]. There have been numerous occurrences worldwide where deepfakes have been employed to advance political interests by exploiting the likeness and image of renowned political figures. These individuals may be portrayed as using a racial epithet, accepting a bribe, and admitting to complicity in a crime, among other things.

In 2020, India witnessed its first-ever use of AI-generated deepfake technology in political campaigning when several deepfake videos of politician Manoj Tiwari was circulated on WhatsApp groups. These videos depicted Tiwari making accusations towards his political rival Arvind Kejriwal in both English and Haryanvi languages, preceding the elections in Delhi, the Indian capital state. In a diverse and politically sensitive country like India, deepfakes can exacerbate existing communal tensions, incite violence, and erode trust in democratic institutions, leading to social unrest and instability. India,

[12]World Economic Forum, *Global Risk Report 2024*, available at: https://www.weforum.org/publications/global-risks-report-2024/

[13]Yoori Hwang, Ji Youn Ryu, and Se-Hoon Jeong, "Effects of Disinformation Using Deepfake: The Protective Effect of Media Literacy Education," *Cyberpsychology, Behaviour, and Social Networking* 24, no. 3 (2021): 188-193

[14]Gillian Murphy and Emma Flynn, "Deepfake False Memories," *Memory* 30, no. 4 (2022): 480-492

[15]Ashish Sharma, "India's Floating Disinformation During the COVID-19 Pandemic," *Journal of Media Ethics* 37, no. 2 (2022): 145-147.

[16]Jiyoung Lee and Soo Yun Shin, "Something That They Never Said: Multimodal Disinformation and Source Vividness in Understanding the Power of AI-enabled Deepfake News," *Media Psychology* 25, no. 4 (2022): 531-546.

particularly during elections, by exploiting deepfake technology. Countries with strained diplomatic relations or territorial disputes with India may seek to undermine its stability and influence public opinion through the dissemination of deepfake content. This could include neighbouring countries like Pakistan or China, which have geopolitical interests in the region. Non-state actors such as terrorist organisations operating in the region may seek to exploit deepfake technology to spread propaganda, incite violence, undermine the democratic process in India, or breach the national security of the country. By exploiting vulnerabilities in the information ecosystem, these actors can amplify existing social and political divisions, erode trust in democratic institutions, and destabilise the electoral process in India[17].

The issue of political deepfakes also has the potential to significantly impact the field of journalism as well as the overall quality of democracy. These manipulated videos can lead viewers to question the authenticity of the content, resulting in decreased levels of trust in social media news. Additionally, politicians may use real videos as a defence against accusations by claiming they are deepfakes, a tactic known as the 'liar's dividend'[18]. If left unaddressed, political deepfakes could prove to be perilous not only for those directly involved but also for the general public who may find themselves unsure of which news sources to believe, leading to a lack of trust in online information. Therefore, safeguarding against the malicious use of deepfake technology is essential for protecting the integrity of Indian elections and preserving democratic norms and principles.

## RASHMIKA MANDANA CASE

On November 5, 2023, a deepfake video featuring Indian actress Rashmika Mandanna began circulating across various social media platforms. The video was made by an individual who imposed Mandana's likeness in place of some other woman, Zara Patel, a social media influencer. The creator's motive was to increase viewership on his fan page dedicated to Rashmika Mandana, which had previously failed to attract significant attention. This incident highlights the growing misuse of deepfake technology, particularly targeting women, and underscores the ethical and legal challenges associated with such nonconsensual use of personal images. Nearly a month later, law enforcement authorities apprehended the individual responsible for creating the deepfake. Despite criminal proceedings being initiated against him, the video continued to be reachable on platforms like X (formerly Twitter), and links to it continued to circulate across various news platforms. This persistence underscores the inadequacies in content moderation systems on social media platforms and the difficulties in effectively removing harmful or misleading material.

The Rashmika Mandana case is exemplary of a broader pattern of nonconsensual image-based victimisation of women in India, reflecting their increasing vulnerability in the digital age. Such incidents not only violate privacy but also perpetuate harm and distress for the individuals involved. Furthermore, a cursory examination of platforms like YouTube reveals a troubling trend in content creation. Searches for terms such as "funny videos" or "funny falls" yield content that often exploits personal images of men, women, and children, frequently harvested without consent from social media profiles or professional photographers' pages. These images, originally intended for private use or to commemorate special occasions, are repurposed into so-called humorous content. When manipulated and shared without consent, such content can cause significant emotional distress, embarrassment, and reputational harm to the individuals depicted.

These cases collectively highlight the urgent need for stronger regulatory frameworks and improved enforcement mechanisms to address the misuse of digital technologies. They also emphasise the importance of raising public awareness about the ethical implications of sharing and manipulating personal images without consent. As digital platforms continue to evolve, safeguarding individuals' privacy and dignity must remain a priority to mitigate the risks posed by nonconsensual image-based exploitation.

Collectively, these illustrations highlight a grave and evolving challenge within India's cyber legal landscape. They reveal the complexity of online harassment, which extends outside conventional forms of cyberstalking and impersonation to more nuanced exploitations such as character defamation and privacy invasion. These cases highlight the urgent need for a robust and receptive legal framework, as well as a decent re-evaluation of content-making and sharing practices in

[17]Shinu Vig, "Regulating Deepfakes: An Indian Perspective," *Journal of Strategic Security* 17, no. 3.
[18]Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen, "The State of Deepfakes: Landscape, Threats and Impact," *Deep trace*, available at: https://regmedia.co.uk/2019/10/08/deepfake_report.pdf

the digital sphere. Such measures are essential to safeguard individuals from invasive and damaging forms of exploitation. The amendments of 2008 in the IT Act 2000 represented an advanced step by broadening the scope of cybercrimes to include impersonation, privacy violations, and cyberterrorism. However, it also exposed systemic lacks in addressing the intricate difficulties of digital harassment. The outline of the concept of 'body corporate' in Section 43A was an admirable effort to enhance liability for data protection. Yet, when examined through the lens of critical legal theory, this legislative move discloses a partial approach to addressing the multifaceted extent of cybercrimes.

This discourse sheds light on the pervasive issue of nonconsensual image-based victimisation, mainly affecting females in the digital domain. Within this context, privacy infringement, heightened threats of harassment, and the potential for significant damage to social esteem are increasingly prevalent. India's patriarchal societal structure exacerbates the harm witnessed by women who are shown maliciously online, adversely affecting their prospects in marital and service markets. Women represented as sexual commodities not only endure profound personal suffering but also cause their families to social disgrace and seclusion[19]. Furthermore, law enforcement agencies often trivialise the severity of women's witnesses with online harassment, creating additional barriers to seeking and obtaining justice. This minimisation of their experiences emboldens offenders, intensifying the victimisation of women both digitally and bodily. Such dynamics reflect the wider social context in India, where gender-based discrimination and inequality persist, further complicating efforts to address online harassment effectively.

## CASES ON DEEPFAKE

In conclusion, addressing these challenges requires a comprehensive approach that combines stringent legal measures, ethical content practices, and societal change. Strengthening the legal framework to address the nuances of digital harassment, raising awareness about the ethical implications of online behaviour, and fostering a culture of accountability are essential steps toward protecting individuals, particularly women, from the harms of nonconsensual image-based exploitation[20].

## NON-CONSENSUAL INTIMATE IMAGE ABUSE

The issue of unconsented pictures -based victimization of females in Internet has garnered significant attention, particularly in the context of defining " non-consensual intimate image abuse ."The United Nations Economic and Social Commission for West Asia (UNESCWA) conceptualize non-consensual intimate image abuse as a form of nonconsensual pornography, wherein intimate images or videos are shared without the person's consent, often with the intent to harm, shame, or exert control over the victim. This phenomenon reflects a broader gender-based digital violence that disproportionately affects women, undermining their privacy, dignity, and psychological well-being. According to UNESCWA, the term non-consensual intimate image abusedenotes "Nonconsensual pornography (the most common form of which is known as 'involves the online distribution of sexually graphic photographs or videos without the consent of the individual in the images. The perpetrator is often an ex-partner who obtains images or videos in the course of a prior relationship and aims to publicly shame and humiliate the victim, in retaliation for ending a relationship. However, perpetrators are not necessarily partners or ex-partners, and the motive is not always revenge[21].

non-consensual intimate image abuse is fundamentally characterised by the non-consensual sharing of images or audiovisual content of a victim by a perpetrator. This content may encompass various forms, including photographs or videos depicting the victim in compromising situations, which may or may not have been captured with their consent. Such material can range from intimate images shared by a partner to voyeuristic content captured by individuals such as colleagues, relatives, or acquaintances. In certain instances, even if the images were initially captured with the victim's consent, they may be shared without permission, either in their original form or as doctored versions. These images are often

[19]T. Saha and A. Srivastava, "Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization," *International Journal of Cyber Criminology* 8 (2014): 57.

[20]Debarati Halder and Subhajit Basu, "Digital Dichotomies: Navigating Non-Consensual Image-Based Harassment and Legal Challenges in India," *Information & Communications Technology Law*,

[21]Halder, D., & Basu, S., "Digital Dichotomies: Navigating Non-Consensual Image-Based Harassment and Legal Challenges in India", *Information & Communications Technology Law*, (2024) 1–24, available at https://doi.org/10.1080/13600834.2024.2408914

accompanied by sexually explicit or defamatory text, intended to harm the victim's reputation or inflict emotional distress. The act is typically motivated by a desire for revenge, often stemming from emotional turmoil caused by events such as the dissolution of a romantic relationship, jealousy, or interpersonal conflicts in professional or familial settings. non-consensual intimate image abuse is widely regarded as a reprehensible act due to its potential to cause significant psychological and emotional harm to the victim.[22] It is often a manifestation of personal grievances, such as those arising from breakups in heterosexual or homosexual relationships, workplace rivalries, or familial disputes. The dissemination of such content not only violates the victim's privacy but also serves as a tool for public humiliation and reputational damage. The act is intrinsically linked to the perpetrator's desire for retribution or personal gratification, making it a deeply unethical and harmful behaviour. Consequently, non-consensual intimate image abuse is recognised as a serious violation of individual rights and a source of profound distress for those affected. Indian legislation currently lacks specific recognition of non-consensual intimate image abuse as a distinct criminal offence. Consequently, the criminal justice system in India addresses instances of non-consensual photo-based harassment, including non-consensual intimate image abuse, through a combination of existing lawful provisions. These include Section 354C of the Indian Penal Code (IPC), which criminalises voyeurism, and Section 509 IPC, which punishes the use of words, gestures, or acts intended to insult the modesty of a woman. Additionally, provisions under the Information Technology Act, 2000, such as Section 67, which prohibits the creation and distribution of sexually explicit material, and Section 67A, which targets the dissemination of obscene content in electronic form, are often invoked to address such offences. While these provisions provide a legal framework to combat certain aspects of non-consensual intimate image abuse, the absence of a specific statute addressing this issue highlights a significant gap in the legal system. This fragmented approach underscores the need for comprehensive legislation tailored to address the unique nature and consequences of non-consensual intimate image abuse ensuring more effective protection for victims and accountability for perpetrators[23]. It is argued that the current legal treatment of non-consensual intimate image abuse in India may fall short of delivering comprehensive justice, as courts often fail to fully recognise the perpetrator's underlying motive—revenge. This oversight can result in the absence of critical judicial measures, such as restraining orders to prevent the culprit from further disseminating the victim's photos or contacting them in the future. A pertinent example is the 2018 case from West Bengal, India, where a state public prosecutor successfully represented a woman subjected to non-consensual intimate image abuse by a man with whom she had an emotional relationship. While the accused was sentenced to five years of imprisonment and the court awarded compensation to the victim, there is no evidence to suggest that the court took additional steps to prohibit the perpetrator from further exploiting the victim's images. This case highlights a significant gap in the judicial response, underscoring the need for more robust legal mechanisms to address the specific harms associated with non-consensual intimate image abuse and to ensure long-term protection for victims[24].

Although these provisions of the IPC and the Information and Technology Act are available, these are largely inadequate in dealing with the rising problems of non-consensual content generated by AI, digitally altered, and deepfake content, as these laws were not drafted having in mind the element of automation, massive distribution, and attribution of the misuse of artificial intelligence itself.

## CYBERBULLYING AND HARASSMENT

Individuals can be targeted through deepfake technology, with malicious actors creating fake content to harass or defame them online. Deepfakes can be used to manipulate and cheat people by making it appear as if someone is saying or doing something that they never did. This might include creating fake videos of persons engaged in illegal or immoral activities, making false statements, or engaging in inappropriate conduct. The majority of deepfakes encountered on the internet are of a pornographic nature. The inception of deepfake pornography began to spread several years ago when a Reddit user shared doctored videos of actresses with their faces swapped onto the bodies of

[22]Ministry of Justice, UK Government, *Revenge Porn: Fact Sheet* (2015) https://assets.publishing.service.gov.uk/media/5a80be45ed915d74e33fc281/revenge-porn-factsheet.pdf

[23]Ministry of Justice, UK Government, supra note 1

[24]S Brinda, supra note 1.

porn actors[25]. Since then, numerous unauthorized videos have been uploaded to various websites by deepfake creators, with many famous individuals such as actors, journalists, and public figures being targeted, resulting in harm to their image and brand. In fact, certain websites are commercially misusing this technology by offering users the ability to create their own deepfakes and facilitating the creation of unauthorised sexual videos of other people without their consent or knowledge

## HARASSMENT VIA E-MAIL

It also includes blackmailing, threatening, sending of love letters in anonymous names or sending of embarrassing emails. There is the Criminal Procedure Code, the Indian Penal Code and the Information Technology Act under which such offences and their punishment are described. Under The IT Act, 2000, Section 66 A talks about Punishment for sending offensive messages through communication service, etc and Section 67A and 67B is defined as Punishment for transmitting of material which contains sexually explicit material and Punishment for transmitting of material depicting children in sexually explicit act via electronic form, respectively. Section 67 C of the IT Act deals with an obligation of an intermediary to preserve and retain such information in the prescribed manner by the central government and under section 509 0f Indian Penal Code (IPC) for uttering any word or making any gesture intended to insult the modesty of a woman.[26]

## ONLINE TROLLING

Historically, the term “trolling” emerged in the early 1990s, initially describing the act of deceiving, pranking, or misleading users under false pretences for the purpose of amusement or ridicule. During this period, trolling was primarily associated with playful or mischievous behaviour within online communities. However, while contentious or adversarial communication has long been a feature of internet discourse, the phenomenon of trolling has changed significantly in recent years. On platforms such as Twitter, trolling—often referred to as “e-bile”—has become increasingly pervasive, characterised by its heightened rhetorical aggression and often gendered dimensions. This shift reflects a broader transformation in online interactions, where trolling now frequently serves as a vehicle for hostility, harassment, and the perpetuation of discriminatory attitudes, marking a departure from its earlier, more benign connotations.

Cyber-trolling has been identified as the online manifestation of everyday sadism, reflecting a tendency among certain individuals to derive pleasure from causing distress or disruption in digital environments. This behaviour often contributes to the rapid escalation of conflicts in online discussions, which can quickly spiral out of control. Such interactions frequently devolve into hostile exchanges of personal attacks and insults, a phenomenon commonly referred to as "flame wars.

Gender-based trolling, or gender trolling, represents a distinct and particularly malicious form of online harassment that targets individuals based on their gender identity. This phenomenon is widely recognised as one of the most pervasive and harmful manifestations of digital violence, disproportionately affecting women and girls.[27] Gender trolling encompasses a range of deliberate actions, including the posting of derogatory comments or messages, the dissemination of offensive images or videos, and the creation of memes or hashtags designed to provoke, harass, or incite violence against women. Such behaviours not only perpetuate gender-based discrimination but also contribute to a hostile online environment that undermines the safety and well-being of women and girls in digital spaces. The widespread proliferation of the Internet into even the most remote areas has unlocked unprecedented opportunities for content creators globally.[28] With an active social media user base of 3.81 billion individuals in the year 2020, there has been a significant surge in the demand for diverse forms of content, whether for entertainment, consumption, or intellectual discourse. This growing demand underscores the necessity for content creators to maintain a robust online presence, as their professional success increasingly depends on their ability to engage with and expand their digital audience. The evolving dynamics of digital content creation emphasize the importance of consistent and strategic

[25]H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke, “Information Privacy: Measuring Individuals' Concerns About Organizational Practices,” *MIS Quarterly* (1996): 167-196.
[26]Shobhna Jeet, “Cyber Crime Against Women in India: Information Technology Act, 2000,” *Elixir Criminal Law* 47 (2012): 8891

[27]Mantilla, K. (2013). *Gendertrolling: Misogyny Adapts to New Media*. Feminist Studies, 39(2), 563–570. Available online: https://muse.jhu.edu/article/831729/summary
[28]Gardiner, Becky, *et al*. "The Dark Side of Guardian Comments." *The Guardian* (Print and Online), 2016.

efforts to cultivate and sustain an influential online footprint. Instagram has emerged as one of the most significant social networking platforms worldwide, boasting a monthly active user base of one billion individuals. As of 2019, the platform was home to approximately 3.7 million influencers and content creators, reflecting its growing influence in the digital landscape in 2020. This widespread adoption highlights Instagram's pivotal role in shaping online communication, content dissemination, and user engagement, making it a critical space for both personal expression and professional content creation[29].

## NCRB DATA ON CRIME AGAINST WOMEN

The latest data from the National Crime Records Bureau shows that the rate of crimes against women in India- calculated as crimes per 100,000 of the women population - increased 12.9% between 2018 and 2022. In India, the reported crimes against women per 100,000 women population is 66.4 in 2022, in comparison with 58.8 in 2018. This may be due to various factors: an increase in actual crimes, an improvement in the reporting mechanism, and an increased willingness of women to speak out about their experiences of violence. Statistics in “Crime in India 2022, the annual report by NCRB, show a total of 13 States and Union Territories that have recorded crime rates higher than the national average of 66.4. Delhi tops the list at 144.4, followed by Haryana (118.7), Telangana (117), Rajasthan (115.1), Odisha (103.3), Andhra Pradesh (96.2), Andaman and Nicobar Islands (93.7), Kerala (82), Assam (81.2), Madhya Pradesh (78.8), Uttarakhand (77), Maharashtra (75.1), and West Bengal (71.8). The rate of crime in Uttar Pradesh — which contributed nearly 15 per cent of the cases in India — stood at 58.6.[30]

## CONCLUSION

The sharp increase in digital crimes against women, such as online trolling, non-consensual intimate image abuse cyberstalking, and other forms of online harassment, highlights the critical need for robust legal and societal measures. According to the latest data from the National Crime Records Bureau (NCRB), crimes against women in India rose by 12.9% between 2018 and 2022, with the crime rate climbing from 58.8 to 66.4 per 100,000 women. This upward trend not only indicates the growing incidence of such crimes but also reflects improved reporting mechanisms and a greater willingness among women to speak out against harassment and violence.

The NCRB’s 2022 report, "Crime in India," shows that crime rates are quite higher in 13 states and Union Territories than the national average, with Delhi reporting the highest rate at 144.4 crimes per 100,000 women. This data underscores the widespread nature of gender-based violence, both offline and online, across India. Digital crimes, in particular, have become a significant concern, as perpetrators exploit the anonymity and vast reach of the internet to target women. Acts like online trolling, non-consensual intimate image abuse and cyberstalking not only cause deep psychological harm but also foster a culture of fear and silence, deterring women from engaging freely in digital spaces.

Addressing this escalating crisis requires a multifaceted approach. Strengthening legal frameworks, enhancing enforcement mechanisms, and launching widespread awareness campaigns are essential steps to educate women and law enforcement agencies about digital safety and rights. Social media platforms and technology companies must also take proactive measures to combat online harassment and create safer online environments. Empowering women through digital literacy programs and support systems, while ensuring accountability for perpetrators, is vital to reversing this troubling trend. Only through collective action can we build a society where women can navigate both physical and digital spaces without fear of violence or exploitation.

## REFERENCES

Abdul-Rahman Kabbara, “Bots & Deepfakes,” NSI Intern Integration Project, August 2021, available at: https://nsiteam.com/social/wp-content/uploads/2021/08/IIJO_eIntern-IP_Bots-and-Deepfakes_Kabbara_FINAL.pdf

Angouri, J., & Tseliga, T. (2010). “You Have No Idea What You Are Talking About!” From E-Disagreement to E-Impoliteness in Two Online Fora. Journal of Politeness Research: Language, Behaviour, and Culture, 6(1). https://doi.org/10.1515/jplr.2010.004

Ansari Bushra and Rajaram Sowmya, "It’s Women’s Day, but on the ground, little has changed," ISDM Blog, Published on 15 April, 2024, available at https://www.isdm.org.in/blog/its-womens-day-but-on-ground-little-has-changed

[29]Tewari, P., & Gore Mehendale, Sneha. (2022). *Persisting misogyny: A gendered analysis of online harassment of Indian content creators on Instagram and its impact on mental health*. *Cardiometry*, (25), 493–501. https://doi.org/10.18137/cardiometry.2022.25.493501

[30]Ansari Bushra and Rajaram Sowmya, "It’s Women’s Day, but on the ground, little has changed," *ISDM Blog*, Published on 15 April, 2024, available at https://www.isdm.org.in/blog/its-womens-day-but-on-ground-little-has-changed

Chandell Gosse and Jacquelyn Burkell, "Politics and Porn: How News Media Characterizes Problems Presented by Deepfakes," Critical Studies in Media Communication 37, no. 5 (2020): 497-511.

Danielle Keats Citron and Mary Anne Franks, "Criminalizing Revenge Porn," Wake Forest Law Review 49 (2014): 345, University of Maryland Legal Studies Research Paper No. 2014-1, available at https://ssrn.com/abstract=2368946

Gruber, James E. "A Typology of Personal and Environmental Sexual Harassment: Research and Policy Implications for the 1990s." Sex Roles, vol. 26, no. 11, 1992, pp. 447-464.

Jane, Emma A. "Flaming? What Flaming? The Pitfalls and Potentials of Researching Online Hostility." Ethics and Information Technology 17, no. 1 (2015): 65–87.

Mangoli R.N. and Tarase Ganapati M., "Crime Against Women in India: A Statistical Review," International Journal of Criminology and Sociological Theory, Vol. 2, No. 2, December 2009, pp. 292-302.

Ministry of Justice, UK Government, Revenge Porn: Fact Sheet (2015) https://assets.publishing.service.gov.uk/media/5a80be45ed915d74e33fc281/revenge-porn-factsheet.pdf

Momina Masood, Marriam Nawaz, Ali Javed, Tahira Nazir, Awais Mehmood, and Rabbia Mahum, "Classification of Deepfake Videos Using Pre-Trained Convolutional Neural Networks," in 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2) (IEEE, 2021), 1-6.

Online Gender-based Violence Judicial Resource Guide, Module 2 – Typologies of Online Gender-Based Offenses in Law, 2.5 Gender Trolling, IT for Change, https://projects.itforchange.net/online-violence-gender-and-law-guide/module-2-typologies-of-online-gender-based-offenses-in (last visited 6 February 2025]).

Paarth Neekhara, Brian Dolhansky, Joanna Bitton, and Cristian Canton Ferrer, "Adversarial Threats to Deepfake Detection: A Practical Perspective," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2021): 923-932.

Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics," Foreign Affairs 98 (2019): 147

S Brinda, 'Local Lawyer Wins Revenge Porn Case' The Telegraph (9 March 2018) https://www.telegraphindia.com/west-bengal/local-lawyer-wins-revenge-porn-case/cid/1412240

Sophie Maddocks, "A Deepfake Porn Plot Intended to Silence Me: Exploring Continuities Between Pornographic and 'Political' Deep Fakes," Porn Studies 7, no. 4 (2020): 415-423.

Tom Dobber, Nadia Metoui, Damian Trilling, Natali Helberger, and Claes de Vreese, "Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?" The International Journal of Press/Politics 26, no. 1 (2021): 69-91.

Vasileia Karasavva and Aalia Noorbhai, "The Real Threat of Deepfake Pornography: A Review of Canadian Policy," Cyberpsychology, Behavior, and Social Networking 24, no. 3 (2021): 203-209.

Received on 06-02-2026 Accepted on 03-03-2026 Published on 13-04-2026

https://doi.org/10.6000/2817-2302.2026.05.02