THE STANFORD JOURNAL
AN INTERNATIONAL JOURNAL
THE STANFORD JOURNAL ISSN: 3048-8923
(AN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH)
Volume–2, Issues– 3 July- September: 2025

DIGITAL VICTIMIZATION OF WOMEN IN THE ERA OF ARTIFICIAL INTELLIGENCE

Dr. Purnima Khanna
Assistant Professor,
Khalsa College of Law,
Amritsar.

Abstract

India's current laws on cybercrimes involving deep fakes are insufficient to adequately address the problem. It is challenging to adequately govern the use of artificial intelligence, machine learning, and deep fakes because the IT Act of 2000 contains no particular regulations pertaining to these technologies. The IT Act of 2000 may need to be updated to incorporate sections that expressly address the usage of deep fakes and the consequences for their misuse in order to better control offences caused by deep fakes. This would entail tougher legal safeguards for people whose photos or likenesses are exploited without their permission, as well as harsher punishments for those who produce or disseminate deep fakes for malevolent intent.

Key words: *Digital education, A.I., Women in the new era etc.*

Introduction

As technology has advanced in the present-day age of artificial intelligence, so too have crimes, and digitization of crimes has emerged as an enormous issue. Such crimes include financial fraud, harassment, and identity theft, cyber bullying, privacy violations and harassment among other illegal activities carried out through the use of digital technology. A vast array of malicious activities using computers and networks are included under cybercrime. Targeting individuals, organizations, or even governments may be part of it. The menace of cyber-crime has spread its tentacles throughout the world posing a major threat to nations, governments and general public. But women across the world are at risk of gender specific crimes in the sphere of cyber world. Cybercrimes prevalent against women mainly include online stalking, pornography, sending obscene messages, blackmailing, harassment, phishing, identity theft etc.

As more and more of us use the Internet in our daily lives, so criminals are taking advantage of our interconnectivity and reliance on the web to communicate. With an estimated 4.1 billion Internet users worldwide according to the International Telecommunication Union (ITU), the threats to Internet safety are growing exponentially. Criminals can remain anonymous and gain access to huge amounts of personal data

stored online, so the opportunities for crime in cyberspace are enormous: it is easier than ever to carry out and more difficult to detect.[1]

Cyber Crimes Against Women in the Era of Artificial Intelligence

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. It involves the development of computer systems capable of performing tasks that would typically require human intelligence, such as visual perception, speech recognition, decision-making, problem-solving, and language translation.[2]

AI has a complex impact on crime, providing both new opportunities for criminal action and chances to avoid crime. AI has the potential to improve law enforcement's capabilities, identify crime hotspots, and examine enormous volumes of data to find trends and potential suspects. But thieves are also using AI to create bogus content, automate attacks, and avoid detection. Though the Bhartiya Nyaya Sanhita and the Information Technology Act both attempt to some extent to prevent these offences, the effectiveness of these laws is still up for debate. Some major cyber crimes against women are as follows:

Various Types of Cyber-crimes Against Women

Cybercrimes prevalent against women mainly include online stalking, pornography, sending obscene messages, blackmailing, harassment, phishing, identity theft etc. Some of the chief cyber-crimes committed against women are discussed as follows:

a.Synthetic Media Crimes

Deepfake is an artificial intelligence tool that uses machine learning algorithms, particularly generative adversarial networks (GANs), to generate synthetic material, including photos, videos, and audio recordings etc. The primary objective of deepfake technology is to create highly realistic synthetic media that imitate actual individuals,

[1] 14th United Nations Congress on Crime Prevention and Criminal Justice, available at: https://unis.unvienna.org/unis/en/events/2021/crime_congress_digital-crime.html (Visited on July 27th, 2025)

[2] Hifajatali Sayyed, "Artificial Interlligence and Criminal Liability in India, Exploring Legal Implications and Challenges", available at: https://www.tandfonline.com/doi/full/10.1080/23311886.2024.2343195#d1e126 (Visited on July 27th, 2025)

albeit with certain elements of the content altered.[3] Criminals utilise deepfake technology to impersonate executives or famous personalities, employing AI-generated visuals and sounds that complicate detection of scams, thereby facilitating high-value fraud, including corporate email compromise (BEC), extortion, and social manipulation. Consequently, synthetic media is often employed by criminals to perpetrate offences such as identity theft, virtual forgery, hate speech, online defamation, and obscenity.

The victims of deepfake criminal acts may endure significant psychological effects, including emotional pain and trauma. At the societal level, deepfakes can erode public confidence in media and institutions, potentially jeopardising social and political stability. In 2023 in the small town of Almendralejo in Spain, AI-generated naked images of more than 20 girls, aged between 11 and 17, were being circulated on social media without their knowledge. The pictures were created using photos of the targeted girls fully clothed, many of them taken from their own social media accounts. These were then processed by an application that generates an imagined image of the person without clothes on. To everyone's shock, the suspects in the case were also boys, aged between 11 and 14. The crucial questions before the law enforcement agencies were regarding privacy breach and child pornography. However, Spain lacked adequate laws to tackle the situation. This case is a significant example of how, in spite of a humongous development in AI, domestic and international laws are inadequate to face the adverse consequences of misuse of AI.

b. Cyber Stalking

It may be defined as "invading someone's privacy with the goal to terrify, torment, torture, or intimidate the victim is known as stalking. The offender contacts and tries to build a relationship without the victim's knowledge or consent."[4]It includes "contacting or attempting to engage with the victim via social networking sites or phone conversations despite her evident indifference, writing messages (often threatening) on

[3] See Available at: https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/ (Visited on July 15th, 2025)

[4]Aashank Dwivedi, Crime against women through social media, available at

https://timesofindia.indiatimes.com/readersblog/aashank-dwivedi/crime-against-women-through-social-media-48132/https://timesofindia.indiatimes.com/readersblog/aashank-dwivedi/crime-against-women-through-social-media-48132/ (Visited on September 5th, 2025)

the victim's page, and persistently pestering the victims with e-mails messages/phone calls, among other things."[5]

It is "an extension of the physical form of stalking, where the internet is used to pursue, harass or contact another in unsolicited fashion."[6] It involves "following a person's movements across the internet by posting messages (threatening) on the bulletin boards frequented by the victim, entering the chat rooms frequented by the victim, constantly bombarding the victim with emails etc."[7] Abused women are followed in the cyber world by their assailants who can secretly watch them without their knowledge. This allows the stalker to threaten, impersonate and discredit the victim on the internet. Victims of cyber-stalking, are as scared as those being stalked in the real world.[8] A cyber stalker does not have to leave his home to harass his target and has no fear of physical avenge since he knows that he cannot be physically touched in cyberspace.[9]

c. Data Privacy Violation

The widespread utilisation of AI in criminal activity poses significant hazard to information security and privacy in India. Criminals are utilizing AI algorithms to gather and exploit personal information, harming individuals' safety and privacy. The legal community is rapidly concerned over data breaches and illegal access to sensitive information due to the escalating dependence on AI across several sectors. Legal frameworks must evolve to protect citizens' data and guarantee that data privacy laws are current and enforced as AI-enabled crimes become increasingly intricate and pervasive.

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's foundational comprehensive legislation governing the processing of digital personal data. It seeks to reconcile the necessity for approved data processing with the individual's right to safeguard their personal information. As per the Act, personal information may only be handled for legitimate reasons with the agreement of the data principal.

d. Revenge-porn

[5] A. Thiruthi, "Everything about cybercrimes against women", https://blog.ipleaders.in/everything-about-cybercrimes-against-women/ (Visited on September 5th, 2025)

[6] Wayne Petherick "Cyber Stalking, obsession, obsessional pursuit and the Digital Criminal", available at www.criminology/stalking(Visited on September 5th, 2025)

[7] AmitaVerma 60

[8] *id*158

[9] Vishwanath, p. 35

THE STANFORD JOURNAL ISSN: 3048-8923
(AN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH)
Volume–2, Issues– 3 July- September: 2025

According to a report by United Nations "women have also been the predominant target of image-based sexual abuse (IBSA) (colloquially referred to as 'revenge porn'), a form of cyber harassment which involves the "non-consensual creation, distribution and threat to distribute nude or sexual images" to cause "the victim distress, humiliation, and/or harm them in some way."[10] According to Powell and Henry, "the term 'revenge porn' is inherently problematic as it fails to capture the range of perpetrator motivations which extend beyond revenge, for instance, perpetrators who distribute images in order to obtain monetary benefits or boost social status, or perpetrators who use images as a means to exert further control over their partners or ex-partners."[11]

e. Cyber Defamation

Cyber tort including libel and defamation is another common crime against women in the net. Although this can happen to both genders, but women are more vulnerable.[12]Cybercrime against women includes "actions like disseminating a woman's private photos or displaying her photos and contact information on websites with pornographic content. Given that it interferes with the women's right to privacy, which is a basic right, this also amounts to defamation.[13]" It is possible "to send offensive, unpleasant messages via WhatsApp, mail, or any other social media site."[14]

f. Cyber Bullying

Cyber harassment includes "blackmailing, threatening, bullying and even cheating via e-mail. Though e-harassments are similar to the letter harassment but creates problem when posted from a fake mail identity."[15] According to Jaishankar and Halder talk about secondary victimization of women which is caused by gender stereotype cyber harassment. The authors describe the process which begins "after the victim begins interacting with reporting agencies, her family and friends and society as a whole".[16]

---

[10] Gender-based interpersonal cybercrime, available athttps://www.unodc.org/e4j/zh/cybercrime/module-12/key-issues/gender-based-interpersonal-cybercrime.html(Visited on July 27th, 2025)

[11] *ibid*

[12]https://www.ijrar.org/papers/IJRAR1944342.pdf(Visited on September 5th, 2025)

[13]*ibid*

[14]*ibid*

[15]Nuzhat Parveen 295

[16]D. Halder & K. Jaishankar, 'Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of US, UK and India' [2011a] 6(4) Victims and Offenders 386.

THE STANFORD JOURNAL ISSN: 3048-8923
(AN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH)
Volume–2, Issues– 3 July- September: 2025

g. Cyber Pornography

It is a practice "to produce, distribute, and communicate pornographic content online.[17] Apart from still pictures and images, full motion video clips and complete movies are also available."[18] In the present times "information technology has made it very easy to create and distribute pornographic materials through the internet, and this material can be transmitted to the entire world network within seconds."[19]

h. Cybersex Trafficking

In contrast to sex trafficking, "the victim, in case of cybersex trafficking, has no direct interaction with the abuser. Cybersex trafficking occurs when a dealer broadcasts, records, or photographs the victim doing sexual/intimate actions from a central place and then sells the material on the internet to sexual abusers and purchasers."[20] The offenders "have sexually abused women by coercing, manipulating, and blackmailing them into becoming involved in cybersex trafficking."[21]

i. Morphing

Influencers and bloggers often post their daily life routine in pictures and stories and make videos that are shared via public profile on such social media platforms that can be viewed by the world at large. Such pictures are easily available and can be used for morphing images and can be shared on media platforms and victims can be harassed for such crimes and even extortion can take place.[22] Morphing includes "altering or altering the real picture by a fake or unauthorised user by creating a fake profile, downloading the victim's photo from the internet, editing it in a way that compromises the victim's original identity, and posting it on social networking sites, or by any other method that can damage the victim's reputation.[23]" Unfortunately, "it is now such a prevalent practice

[17] Supra note 9

[18] Nuzhat Parveen 296

[19] K. Mani 219

[20] Supra note 10

[21] *ibid*

[22] Mary Banach, 'Victimization Online: The down Side of Seeking Human Services for Women on the Internet' [2000] Cyber psychology & behavior: The Impact of the Internet, multimedia and virtual reality on behavior and society

[23] Supra note 9

THE STANFORD JOURNAL ISSN: 3048-8923
(AN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH)
Volume–2, Issues– 3 July- September: 2025

that anyone can use it for amusement or to exact retribution, endangering the modesty of the woman."[24]

Legal Framework

In India, the Information Technology Law, 2000 is the main legislation regulating cyber-crimes. The relevant sections are discussed as follows:

i. ***Section 66B- Punishment for dishonestly receiving stolen computer resource or communication device***

It provides that if a person retains stolen computer source or any communication device like a mobile phone etc., with knowledge that it is a stolen property, he is liable to be punishment of imprisonment up to three years or fine up to one lakh or both.

i. ***Section 66C- Punishment for identity theft***

It provides for punishment of a term up to three years and fine up to one lakh rupees, for the offence of "fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person."[25]

ii. ***Section 66D- Punishment for cheating by personation by using computer resource***

It provides that if a person commits offence of cheating by personation with the help of any computer device or computer resource, he shall be punished with imprisonment up to three years and also to fine of maximum one lakh rupees.

iii. ***Section 66E- Punishment for violation of privacy***

According to this section, if a person captures, publishes or transmits an image of private part of a person, without the consent of other person, thereby violating the privacy of such person, he shall be punished with imprisonment which may extend up to three years or with fine which may extend up to two lakh rupees or with both.

It is important to note that according to the explanation to this section:

- "a. transmit means to electronically send a visual image with the intent that it be viewed by a person or persons;

[24] *ibid*

[25] See Sec 66 C, *Information Technology Act*, 2000

- b. capture, with respect to an image, means to videotape, photograph, film or record by any means;
- c. private area means the naked or undergarment clad genitals, public area, buttocks or female breast;
- d. publishes means reproduction in the printed or electronic form and making it available for public;
- e. under circumstances violating privacy‖ means circumstances in which a person can have a reasonable expectation that he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place."[26]

v. Section 67- Punishment for publishing or transmitting obscene material in electronic form

If any person publishes or transmits obscene material in electronic form, which can corrupt the mind of the person reading or seeing it, he may be punished, on first conviction, with an imprisonment of maximum three years and with fine of maximum five lakh rupees. In case of subsequent conviction, the imprisonment may extend up to five years with a fine of maximum ten lakh rupees.

vi. Section 67A- Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form

As per the provisions of this section if a person publishes or transmits any sexually explicit material in electronic form, he shall be liable, in case of first conviction, to an imprisonment which may extend up to five years along with a fine of maximum ten lakh rupees.

Major Challenges in Curbing Digital Crimes

Artificial Intelligence allows for the creation of highly realistic fake videos or images, has opened up access to a new and alarming form of crime. In case of cyber-crimes committed with the help of AI it is difficult to fix Criminal Liability. Sukhodolov et al.

[26] See Section 66 E, *Information Technology Act*, 2000

THE STANFORD JOURNAL ISSN: 3048-8923
(AN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH)
Volume–2, Issues– 3 July- September: 2025

believes that the existing laws may not adequately address AIC's aspects like criminal intent, which is customarily applied to human beings.[27]

Furthermore, India does not have a specific law to regulate AI. Although they provide some protection, the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023 are inadequate to deal with the specific challenges of artificial intelligence, such as algorithmic explainability and autonomous decision-making. The inadequate legal regime fails to address the growing cyber-crimes against women.

There are challenges related to the speed with which deepfakes can be created and disseminated, which often exceeds the ability of researchers and law enforcement to detect and respond. In addition, currently available detection techniques still have limitations, often resulting in false positives or being unable to detect more sophisticated deepfakes. Furthermore, society is also faced with ethical and legal challenges relating to the intervention of deep-fake content. [28]

Generally, the criminals are attracted to the cyber-crimes due to the absence of direct contact with the victim, the comparatively lenient punishments in some nations, and, of course, the challenge of identifying, obtaining, and seizing forensically significant information in the virtual world. The multinational and enormous character of cybercrimes presents another difficulty because they can be planned and carried out virtually anywhere.

Conclusion and Suggesting Remarks

To address the threat posed by AI-enabled crimes, there is an urgent need to develop effective strategies and tools to detect and combat fake content. This includes improving digital literacy among the general public as well as developing new technologies capable of accurately detecting digital manipulation. In addition, there is a need to build a robust legal framework that can address the unique challenges brought about by deepfakes. This includes the creation of new laws that can address cases of deepfake crime, as well as the provision of adequate support and protection for victims of this type of crime. By recognizing and responding to this real threat of crime presented by deepfakes, society can move towards a future where AI technology is used in an ethical and responsible

[27] A. Sukhodolov et al, "Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects", *Journal of Siberian Federal University*, 13(1), 2020, 116-122. Available at: https://doi.org/10.17516/1997-1370-0542 (Visited on July 29th, 2025)

[28]Mahrus Ali et al, "Substantive Justice International Journal of Law", Vol. 8 No. 1, 2025, available at: /https://www.substantivejustice.id/index.php/sucila/article/view/306#:~:text=Historically%2C%20victimology%20has%20focused%20on,individuals%20in%20the%20digital%20age. (Visited on July 29th, 2025)

THE STANFORD JOURNAL ISSN: 3048-8923
(AN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH)
Volume–2, Issues– 3 July- September: 2025

manner while minimizing the potential for abuse and exploitation.[29] It is hereby suggested that:

- The definition of crime shall be expanded so as to encompass within its purview intentional and unintentional AI-induced crime. This will assist law enforcement in determining the accused's criminal culpability and holding him accountable.
- The obligation of ensuring sufficient safety standards to stop the usage of AI in criminal activity shall be placed on the AI developers.
- To regulate the nation's AI development and application, the government shall set up a nodal agency.
- In order to prevent cross-border crimes caused by artificial intelligence, international conventions and treaties shall be established to guarantee cooperation between different countries.
- Future research on explainable AI and the development of safety standards for AI would provide a more comprehensive understanding of the required AI regulations.[30]
- The AI regulating framework shall be based on 'PEEC' doctrine, i.e. on considerations of 'public interest' and 'principles of environmental sustainability', 'economic development' and 'criminal law'.[31]

[29] Mahrus Ali

[30] N. Bhatt, "Crimes in the Age of Artificial Intelligence: a Hybrid Approach to Liability and Security in the Digital Era", *Journal of Digital Technologies and Law*, 2025;3(1):65–88. Available at: https://doi.org/10.21202/jdtl.2025 (Visited on July 29th, 2025)

[31] N. Bhatt & J. Bhatt, "Towards a Novel Eclectic Framework for Administering Artificial Intelligence Technologies: A Proposed 'PEEC' Doctrine", *EPRA International Journal of Research and Development (IJRD)*, 8(9), 2023, 27-36. Available at: https://doi.org/10.13140/RG.2.2.11434.18888 (Visited on July 29th, 2025)