LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

Cyberstalking, Deep Faking and Harassment of Women: Legal Frameworks and Enforcement Challenges

Author
Deeksha Saini

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

Cyberstalking, Deep Faking and Harassment of Women: Legal Frameworks and Enforcement Challenges

Deeksha Saini
Amity Law School Uttar Pradesh

Abstract
The advent of highly accessible generative Artificial Intelligence (AI) poses an unprecedented dual threat to the operational integrity and veracity of the criminal justice system (CJS). This report analyzes two principal manifestations of this threat: the proliferation of Deepfakes, hyper-realistic synthetic media and the rise of industrial-scale transnational Digital Arrest scams. Deepfakes fundamentally destabilize evidentiary foundations, introducing the "Liar's Dividend" where the mere possibility of AI fabrication compels courts to scrutinize genuine digital evidence. This technological crisis mandates a re-evaluation of judicial gatekeeping responsibilities, as current authentication standards are proven insufficient against sophisticated AI-generated falsifications.

Keywords: *Cyberstalking, Deep faking, Harassment.*

Digitalisation and Gendered Vulnerabilities in Cyberspace

The internet is one of the greatest sources of information and support one can have in the present era of modernization and technological advancement. The internet has made the world a global village and it's bound to do more in future. It has given so many avenues of growth to human beings from online businesses, jobs, websites, advocacy, political campaigning and even socialization. The internet and its community have offered many places for people to engage with their thoughts without any hesitation. It has led to many types of activism and debates. It has led to people coming out of their boxes and engaging in meaningful conversation. Social networking sites such as Twitter, Facebook, Instagram and other dating apps at present have given netizens a wide variety of activities to engage in. These social networking sites have provided a participatory and all-inclusive, open public environment with which many can have all-around inclusive development[1]. But the internet and these social networking sites have a dark side too. Online platforms often tend to be hostile places where people's voices are shunned if they speak anything against the crowd. Many are shut down from further participation with online abuses and different types of cybercrimes. Our social structures and legal environment have failed to handle the situation and lack the technological advancement to catch the perpetrators of crime which often leads to victimization of the person who has been abused. The anonymity

[1] https://nluassam.ac.in/docs/Journals/NLUALR/Volume-7/Article%207.pdf

of data is one of the important tools applied by many developed countries to hide the identity of the person and secure their data even at the time of data leaks[2], but the same anonymity becomes evil when it is used by the perpetrators of crime to hide their identity online once the crime has taken place. Digital Victimization is not a new phenomenon - wherever there have been cybercrimes, victimization has existed but for a long time. We have only been concerned with defining and understanding crimes and their types and what technology to employ to catch the perpetrators and not focused on digital victimization and its causes and how that can be tackled. Digital Victimization has taken men and women both into its hands but women often tend to be more vulnerable than men. Recent studies have shown an alarming increase in the number of women who have faced online abuses such as bullying, morphing images, deep fakes, stalking, voyeurism etc. Often social media and its open access provide a great opportunity for such crimes with abuses focusing towards sex/gender stereotyping.

Many incidents have taken place in the world including India which have led to digital victimization and often technological advancement of perpetrators of crime developing at much faster speed than any legal framework of a nation which provides benefits to them. Cyberbullying, cyberstalking, cyber hacking and phishing are the most common types of cybercrimes happening all over the world. With new social networking sites and public profiles, perpetrators or hackers can't get happier. There are other types of crime that have developed due to these social networking websites like trolling, making fake profiles, morphing images, cyber abuse, defamation and others.

Rise of Cyberstalking, Deepfakes, and Online Harassment Against Women

The rapid expansion of the digital realm has brought immense benefits, from connectivity to education and economic opportunities. However, it has also created a fertile ground for gender-based violence to evolve and proliferate. Studies across the world show that 16 to 58 per cent of women and girls have been targeted by violence online. Cyberviolence against women and girls is a pervasive issue, encompassing a wide range of harmful behaviours that exploit the anonymity and reach of digital platforms[3].

Gender-based violence is not a new phenomenon, but its migration to the digital world has magnified its scale and impact. As early as the advent of email and chat rooms, women became targets of cyberstalking and harassment. With the rise of social media, these threats expanded, providing perpetrators with tools to harass, exploit, and demean on a global scale.

[2] Kim Barker and Olga Jurasz, 'Online Misogyny' [2019] JoIA, 95, 114.
[3] https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/

In the 2010s, image-based abuse, or "revenge porn," began to draw significant attention. The non-consensual sharing of intimate images, often as an act of retaliation or control, became a devastating weapon against women. This form of abuse signalled a shift in the dynamics of violence: the internet's permanence and virality meant that victims' suffering could persist indefinitely.

The COVID-19 pandemic marked a turning point in the prevalence of cyberviolence. As lockdowns forced people to rely on digital spaces for work, education, and social interaction, the opportunities for abuse multiplied. UN Women's Rapid Gender Assessment on the impact of COVID-19 on violence against women highlighted significant increases in online harassment, image-based abuse, and cyberstalking during this period. Such was the case in the UK, where 38% of women reported increased online abuse.

The pandemic underscored the structural vulnerabilities in digital spaces, particularly for women and girls. The absence of robust regulatory frameworks allowed perpetrators to act with impunity. At the same time, the reliance on digital platforms meant that many victims could not escape the abuse.

Advancements in technology, especially artificial intelligence (AI), have added new layers of complexity to cyberviolence. Tools that generate deepfake pornography have made it easier for perpetrators to fabricate explicit content, blurring the lines between real and fake. Victims of such abuse often face immense difficulty disproving the authenticity of these materials, compounding their distress.

Social media platforms and messaging apps have also enabled the rapid dissemination of harmful content. Algorithms that prioritise engagement inadvertently amplify abusive behaviour, while encrypted messaging services provide perpetrators with anonymity and protection from law enforcement.

The future of cyberviolence against women is deeply concerning. The potential for abuse in up and coming immersive digital environments, such as the metaverse or virtual reality, is already raising alarms, with perpetrators finding increasingly sophisticated ways to exploit vulnerable individuals. Additionally, the global nature of the internet enables cyberviolence to transcend national borders, complicating efforts to hold perpetrators accountable. Weak or inconsistent legal frameworks further exacerbate the issue, leaving many victims without adequate recourse.

The rapid expansion of internet access, social media platforms, and digital technologies in India has significantly increased women's participation in online spaces. However, this digital inclusion has been accompanied by a sharp rise in cyberstalking, deepfake abuse, and online harassment targeting women. Social networking sites, messaging applications, and content-sharing platforms have

become common mediums through which women are subjected to persistent monitoring, unsolicited communication, threats, sexualised abuse, and intimidation. Cyberstalking in India has evolved beyond repeated messaging to include activities such as identity theft, impersonation, doxxing, and misuse of personal data. Women journalists, students, professionals, activists, and public figures are particularly vulnerable, though ordinary users are equally affected. The anonymity and borderless nature of the internet often embolden offenders and make detection and accountability difficult.

The emergence of deepfake technology has further aggravated the problem. Artificial intelligence is increasingly being misused to create non-consensual morphed images and sexually explicit videos of women, causing severe reputational, psychological, and social harm. Indian women have been frequent targets of such deepfake pornography, which spreads rapidly and is difficult to contain once uploaded online.

Online harassment, including trolling, hate speech, and sexual threats, has also intensified, reflecting deep-rooted gender biases and patriarchal attitudes. Despite the presence of legal provisions under the Information Technology Act and criminal laws, underreporting, lack of awareness, slow investigation, and technological challenges continue to hinder effective redressal. The rising incidence of these cyber offences highlights the urgent need for stronger legal frameworks, improved enforcement mechanisms, and gender-sensitive digital governance in India.

Understanding Cyberstalking

Engaging in harassing or threatening behaviour towards another individual through the use of electronic communication technologies such as the Internet, e-mail, or other electronic communication platforms is an example of cyberstalking. The majority of laws regarding stalking require the perpetrator to make a serious threat of violence against the victim. Other laws include threats against the victim's family, while still other laws require just that the alleged stalker's behaviour constitutes an implied threat. Due to the fact that it does not involve any physical contact, cyberstalking may give the impression that it is less harmful than traditional stalking[4]. This is because cyberstalking has essential traits with offline stalking. It has been established through anecdotal and informal statistics that cyberstalking is a significant and rapidly expanding problem. There are certain law enforcement agencies that have provided their officers with training on this matter; however, very few of these agencies have put their attention or resources especially on the issue of cyberstalking.

[4] https://www.ojp.gov/ncjrs/virtual-library/abstracts/cyberstalking-new-challenge-law-enforcement-and-industry-report

Cyberstalking is a form of cybercrime in which a cybercriminal utilizes the internet to repeatedly threaten another person. Email, social media, and other internet platforms are frequently used as vehicles for the commission of this crime. It is even possible for cyberstalking to occur in conjunction with the more traditional form of stalking, which is when the perpetrator harasses the victim in a physical setting. Despite the fact that there is no unified legal approach to cyberstalking, a number of states have taken steps toward making these acts illegal and penalized by law. Cyberstalkers have access to a wealth of information that enables them to organize their harassment, which can be found on social media platforms, blogs, image-sharing websites, and a variety of other commonly utilized online sharing activities.

False charges, fraud, the destruction of information, threats to life, and manipulation through threats of exposure are all examples of the kind of behaviors that fall under this category. The use of e-mails and other kinds of messaging apps, messages declared to an online page or a discussion cluster, and frequently even social media are all methods that stalkers employ in order to send unwelcome messages and harass a particular individual by drawing unwanted attention to them. The term "cyberstalking" is frequently used interchangeably with "internet stalking," "e-stalking," and "online stalking."

Individuals who engage in cyberstalking may pose as their victims, post fraudulent information, or make comments that are dangerous. In order to escape detection, they frequently create many accounts.[5] Further, they are able to follow the position of the victim or their personal activities by utilizing GPS or malware. In addition to being a dangerous scenario that might result in offline threats, cyberstalking is also a serious problem that destroys privacy and frequently requires legal action to put an end to. Stalking someone online is both destructive and unlawful.

Cyberstalking is a severe problem that can have a profound impact on the victims since it invades their privacy and can have a profound emotional impact. Ongoing harassment, threats, and monitoring carried out online are all components of this phenomenon, which can occasionally result in actual physical harm. In order for individuals to defend themselves and their rights when using the internet, it is necessary for them to be aware of cyberstalking, to remain vigilant all the time, and to take legal action if it is necessary. It is possible to prevent events like this and make the online world a safer place for everyone if we educate people about the hazards of cyberstalking and encourage them to adopt safer techniques when using the internet.

[5] https://www.geeksforgeeks.org/computer-networks/what-is-cyberstalking/

Online Harassment of Women

The use of information and communication technology by an individual or a group with the intention of repeatedly inflicting harm onto another person is what is meant by the term "online harassment." In the context of a virtual world, this may include engaging in activities such as issuing threats, causing embarrassment, or generating shame.

This type of behavior extends to the display of discriminatory ideas and views, including but not limited to sexism, racism, xenophobia, homophobia, transphobia, and ableist prejudices. It is also possible for information technology to encompass incidents of sexual harassment and cyberstalking that take place online, as well as the perpetration of image-based sexual abuse or other forms of sexually inappropriate behavior that takes place online[6]. There are a few other names that can be used to describe online harassment, including cyberaggression, cyberbullying, cyber-harassment, cyberhate, cybervictimization, and illegal online behavior.

This phenomena happens across a variety of online platforms, including but not limited to social media platforms (such as Facebook, Instagram, Snapchat, TikTok, and Twitter), text messaging (SMS), instant messaging (via devices, email provider services, applications, and social media messaging capabilities), and email. Persecuting someone online or even just having to deal with nasty stuff on the internet can be quite upsetting. It poses a risk to the health of our community, our right to freedom of expression, and our capacity to take part in conversations and communal activities to the fullest extent possible[7].

Cybercrimes committed against women in India are becoming an increasing source of concern. These crimes have a substantial impact not only on the mental and physical health of women, but also on their economic well-being. Online harassment, cyber stalking, cyberbullying, revenge porn, and financial fraud are some of the numerous sorts of cyber crimes that are committed against women as a result of the internet. One of the most prevalent types of cybercrime committed against women in India is the act of having them harassed online. It is the practice of sending threatening, abusive, or disrespectful messages or comments to women through the use of internet platforms. 54.8% of women have reported having experienced some form of online harassment, according to a research conducted by the National Commission for Women. Women who are subjected to online harassment may experience severe mental discomfort, worry, and fear, which can leave them feeling that they are in danger and defenceless. An additional form of cybercrime that women in India are subjected to is known as

[6] https://reportandsupport.ox.ac.uk/support/what-is-online-harassment
[7] https://www.eap-india.com/online-harassment-meaning-types-impact/

cyberstalking. This term refers to a pattern of persistent harassment that occurs online and involves following, monitoring, or tracking the activities of another person while they are online. It is possible for cyberstalkers to harass and stalk their victims through the use of a variety of digital channels, including social media, emails, and messaging applications. According to a report that was compiled by the Cyber Crime Cell of the Mumbai Police, the number of instances of cyber stalking that have occurred in India over the course of the past year has increased by 91%3.

When someone is harassed, humiliated, or intimidated through the use of technology, this is known as cyberbullying. One of the most prevalent types of cybercrime committed against women, particularly among young girls and women, is cyber sexual assault. There are many different manifestations of cyberbullying, such as the dissemination of rumours, the posting of abusive remarks, and the publishing of embarrassing images or videos. According to the findings of a survey conducted by the Cyber and Media Cell of the Delhi Police, forty percent of the victims of cyberbullying in India were female. One of the most terrible types of cybercrime committed against women in India is the utilisation of revenge porn. Distributing sexually explicit photographs or videos without the agreement of the victim is a form of cyberbullying, which is typically carried out as an act of retaliation or blackmail. A research that was published by the Cyber Peace Foundation indicates that there has been a 148% increase in the number of cases of revenge porn in India over the course of the previous year. [8]Pornography that is intended to exact revenge can cause severe mental and emotional pain, in addition to causing damage to a woman's reputation. Women in India are also becoming increasingly concerned about the issue of cyber financial fraud. Cybercriminals have discovered new techniques to swindle victims who are unaware of their identity as a result of the proliferation of online transactions. Phishing, credit card fraud, and other forms of online financial frauds are all examples of activities that fall under the category of cyber financial fraud. There has been a notable rise in the amount of fraudulent activity involving internet banking in India over the course of the past year, as stated in a study published by the Reserve Bank of India.

[8] Anand, E., & Kaushik, T. K. (2026). From Privacy Breach to ‘Virtual Rape’: Analyzing Revenge Porn as an Emerging Contour of Cybercrime against Women under the Indian Legal Framework. *National Journal of Criminal Law*, *9*(1). Retrieved from https://lawjournals.celnet.in/index.php/njcl/article/view/1988

Case Laws on Cyber Crimes Against Women

The vast majority of cybercrimes are carried out without being reported by women because they are not aware of where they may report such crimes and they are reluctant to do so.[9] The infamous Ritu Kohli case, which occurred in the year 2000, was said to be the first instance of cybercrime directed only at women.

1. **The Ritu Kohli Case:** This was the first sexual offense committed over the internet in India. Delhi was the location where the first report of it was made on June 18, 2000. Manish Kathuria, a software engineer who is thirty years old, was taken into custody by authorities from the Crime Branch of the Delhi police department for harassing a woman through the use of an internet messaging service. According to reports, Manish used to use the name Mrs. Ritu Kohli when he went online to speak on the website www.micr.com. During the course of their conversation, he used foul language and provided her with his home phone number in order to prolong the conversation. As a consequence of this, Mrs. Kohli started getting calls at her house that were improper. As a result of the disruptions, Mrs. Kohli submitted a complaint, and after conducting an investigation, the Delhi police identified the person responsible for the disturbances and initiated criminal proceedings against him for insulting Ritu Kohli's modesty[10]. The charges were brought under section 67 of the Information Technology Act[11] and section 509 of the Indian Penal Code. The police registered her case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of Ritu Kohli. But Section 509 refers only to a word, a gesture or an act intended to insult modesty of a woman. But when same things are done on Internet, then there is no mention about it in the said section. This case caused alarm to the Indian government, for the need to amend laws regarding the aforesaid crime and regarding protection of victims under the same. So, in 2008, Indian legislature had amended the IT Act 2000 and made provisions for cyber stalking. The IT Act, 2008 does not directly address stalking. But the problem is dealt more as an "intrusion on to the privacy of individual" than as regular cyber offences which are discussed in the IT Act, 2008.[12]

2. **State of Tamil Nadu v. Suhas Katti[13]:** This is a case that involves the publishing of remarks that are obscene, libellous, and aggravating in a Yahoo chat group that pertains to a woman who has recently divorced. Through the use of a fictitious email account that he had created in the victim's name, the accused sent emails to the victim. Following the posting of the texts, the woman was subjected to online harassment, and she started receiving

---

[9] https://www.cnlu.ac.in/wp-content/uploads/2025/04/Cyber-Crimes-Against-Women-And-Prevention-by-Samridhi-Goyal.pdf

[10] https://www.worldpulse.org/story/cyber-stalking-a-virtual-crime-with-real-consequences-43984

[11] The Information Technology Act, section 67

[12] https://www.iosrjournals.org/iosr-jhss/papers/Vol.29-Issue11/Ser-11/H2911115560.pdf

[13] CC No. 4680 of 2004.a

unwanted phone calls on the assumption that she was participating in solicitation. It was as a consequence of this that she submitted a case to the Egmore Court in February of 2004. Based on the report, the cyber department of the Chennai police department was able to locate and detain the person responsible for the crime. Furthermore, the accused was found to be responsible for the violations of sections 469/509 of the Indian Penal Code as well as section 67 of the Information Technology Act, which was passed in the year 2000.

Deepfake Technology: An Overview

The term "deepfakes" refers to artificial intelligence-generated synthetic media (video, audio, etc.) that are designed to convincingly simulate a human saying or doing something that they have never done. In order to imitate the manner in which people communicate, many contemporary deepfakes employ techniques such as voice cloning, synthetic video calls, and material generated by artificial intelligence. Since generative artificial intelligence technologies have made these tools more accessible, there has been a significant growth in the number of incidents in which they have been utilized to counterfeit identities and take advantage of trust on an enterprise level.

Throughout the course of history, the production of deepfakes needed a significant amount of technical expertise as well as computer capacity. The technical barrier to entry, on the other hand, has been dropped, and attackers may now generate a convincing video call with little to no prior training in programming by creating a near-exact reproduction of an executive's voice by using a brief audio clip. According to Cybersecurity Drive, the number of deepfake files discovered on the internet has increased from around 500,000 in 2023 to an anticipated 8 million in 2025. This growth occurred within the same time period. "It's a perfect storm that leads us to really sense that 2026 will be the year of impersonation attacks," said Aaron Painter, CEO of Nametag. "It's a perfect storm."[14]

The danger is not merely a theoretical concern for businesses. The verification mechanisms that are relied on by corporations are explicitly targeted by deepfakes. These verification processes include a voice on a phone call, a face in a video meeting, or an email that reads just like one written by the chief financial officer. Deepfake fraud losses in the United States reached over $1.1 billion in 2025, which is more than three times the amount of $360 million that was lost the previous year. Deep fakes take use of human trust, which is significantly more difficult to "patch" than technological obstacles. As a result, the attack surface

---

14 https://www.researchgate.net/publication/395549166_Deepfake_Understanding_the_Technology_Background_Content_Differences_from_Traditional_Forgery_and_Impact_on_Public_Trust

continues to expand. Deepfakes, on the other hand, are also becoming increasingly used in ways that are detrimental to society. phony news and films are being produced by malicious actors with the use of this wonderful technology in order to manipulate public opinion, increase instances of cyberbullying, and also stimulate the production of phony pornographic videos.

To the extent that it is difficult to differentiate between what is false and what is real, the content that is produced with the assistance of deepfake technology can be extraordinarily lifelike. This, in turn, is contributing to the gradual loss of faith in the information sources. Nevertheless, technological improvements are assisting in the development of some powerful deepfake artificial intelligence detection tools. These programs are able to determine if films are real or edited. Some examples of these technologies include Deepware Scanner, Sentinel, Fake Catcher by Intel, Microsoft's Video Authenticator, and others[15].

When it comes to the effects that deepfake has on society, there are both positive and negative outcomes. Additionally, deepfake technology will further blur the barrier between reality and illusion, which will result in a crisis of confidence throughout the entire civilized world. A significant amount of a fraudulent Value-Added Tax Invoice was brought to justice by the Hongkou District People's Procuratorate of Shanghai Municipality in China in the month of March 2021. In order to circumvent the facial recognition system and fraudulently issue regular VAT invoices, the criminal suspect fabricated action videos that included nodding, shaking the head, blinking, and opening the mouth[16]. These videos were created through the technical processing of high-definition profile images and information from identification cards belonging to other individuals.

It is possible that deepfake technology might be used to disseminate false information, cause social unrest, and divide people. In the year 2018, for example, more than twenty individuals were slain viciously across the entirety of India as a direct result of rumors that circulated on WhatsApp regarding the kidnapping of young children or other illicit activities. The court system and the practice of law are likewise vulnerable to the dangers posed by deepfake technology. Artificial intelligence technology is increasingly being utilized in the judicial system. If the detection technology is unable to keep up with the pace of deepfake technology, it has the potential to result in the incorrect judgment of cases, which would have a significant impact on both the interests of victims and the institution of justice.

[15] https://www.usaii.org/ai-insights/resources/deepfake-technology-an-overview-of-its-impact-on-society

[16] https://www.unit21.ai/fraud-aml-dictionary/deepfake

Regulatory Framework and Ai

While India does not have any legislation on data protection, personal information is safeguarded by Sections 43A and 72A of The Information Technology Act[17]. Similar to GDPR, it grants individuals the entitlement to receive compensation for the unauthorised revealed of their personal data. The right to privacy is enshrined as a basic right in the Indian Constitution, as affirmed by the Supreme Court in 2017. AI is projected to contribute 957 billion US dollars, equivalent to around 15% of India's current gross value, by 2035. Artificial intelligence will inevitably influence the lives of individuals in the future. In 2018, the Policy Commission of NITI Aayog initiated a number of artificial intelligence (AI) application programmes. Four committees were established by the Ministry of Electronics. The purpose of Information Technology is to emphasise and analyse different ethical issues associated with AI. The Joint Parliamentary Committee is now deliberating on the Personal Data Protection Bill 2019 (PDP Bill), which is derived from a preliminary data protection statute. The transformation of a bill into law occurs upon its approval by both chambers of Parliament. The proliferation of AI in India is outpacing the development of regulatory frameworks to oversee its implementation. Enterprises are currently employing AI technology to enhance the skills of their employees. [18]

The recently implemented New Education Policy focuses significant importance on the instruction of coding skills to students, commencing from the sixth grade. India is poised to become a hub for cutting-edge AI technologies in the coming years. Cyril Amar Chand Mangaldas is the pioneering law practice in India to utilise artificial intelligence (AI) primarily for the examination and enhancement of legal documents, particularly contracts. During a function organised by the Supreme Court Bar Association (SCBA), CJI SA Bobde addressed the subject of heightened use of artificial intelligence (AI) within the legal system, with a specific focus on docket management and decision-making. Nevertheless, the absence of a desire to adapt to this emerging phenomenon could impede the widespread adoption of artificial intelligence (AI) in developing countries such as India. Moreover, there is apprehension regarding the potential adverse impact of AI on an economy characterised by a surplus of labour, such as India, where a significant portion of the population is underprivileged and lacks literacy skills.

[17] Section 43A and 72A of IT Act, 2000

[18] ANTARA ROY- Artificial Intelligence With Law In India, Volume 12, Issue 1 January 2024, file:///D:/Your%20Data%20Don't%20Delete/Downloads/IJCRT2401013.pdf, Last visited 30th March 2024.

Conclusion

The safeguarding of women's privacy must remain a paramount priority as we traverse the swiftly evolving technology landscape. If deepfake technology remains unregulated, it might devastate the lives of several women. It is our collective responsibility to advocate for legislation, denounce injustice, and strive to create a digital environment that safeguards individuals' rights to privacy and dignity, particularly those of women. We can solely anticipate safeguarding the integrity of privacy against this substantial technical threat through collaborative efforts. It is feasible to address the adverse impacts of disruptive technologies, such as malicious deepfakes, in a reactive manner rather than a proactive one. Consequently, it is imperative that industry stakeholders, particularly small and medium-sized enterprises and developers of deep learning technologies, participate in the regulatory process.

These organisations are most equipped to provide an accurate understanding of the pertinent technologies at the designated time. Consequently, it will be simpler to identify, report, and assess the level of scepticism warranted when encountering deepfaked information. It will also facilitate measures against abusive and illegal deepfaked content. The digital realm resembles a perpetual arms race between security measures and innovation, with malicious actors, unfortunately, often prevailing.

In today's digitally networked society, cyberstalking and internet harassment are serious concerns that are growing in number. These threats affect people of all ages and backgrounds, and they are becoming more prevalent. As a result of these offences, victims not only experience a violation of their privacy and dignity, but they also experience severe negative effects on their mental health and overall well-being. Furthermore, the widespread nature of these offences undermines public faith in the security of online communities, resulting in an atmosphere that is characterised by dread and mistrust throughout the community. Given the psychological pain, harm to professional and personal reputations, disturbance with daily routines, and intrusive nature of these offences, it is clear that there is a need for more suitable legal protections and responsive mechanisms that are able to properly address them. Important laws has been introduced in India to combat internet abuse, most notably the Information Technology Act of 2000 and the Bharatiya Nyaya Sanhita, 2023.

Both of these pieces of legislation were introduced in the year 2000. Despite the fact that these acts represent significant strides in the right direction, there are a number of obstacles that hinder them from being implemented in the appropriate manner. There are lingering concerns that contribute to the difficulties that victims have when attempting to seek remedy. These problems include uncertain jurisdiction, gaps in enforcement, and widespread public ignorance regarding the

legal options that is available. Also, the legal system is generally behind the pace of fast growing technology and the rising complexity of cyber harassment, and victims are left without recourse or help. This is a problem because cyber harassment is becoming increasingly complicated.

Suggestions

In order to facilitate law enforcement, it is important to make investments in the enhancement of the operational effectiveness of police forces and investigating agencies. This can be accomplished through the supply of cutting-edge digital technology, expertise, and professional training that support the effective detection, tracing, and conviction of cybercriminals. To accomplish this, you will need to have access to the most recent forensic tools, analytics capabilities, and cybersecurity frameworks. In addition, in order to effectively address cybercrime that occurs across international borders, it is necessary to develop mutual legal assistance treaties (MLATs) and cross-agency collaboration at the global level. This will make it easier to share information and best practices in a timely manner.

Implementing solid support mechanisms that provide victims of cyber abuse with assistance in a variety of different areas is an important step in victim support systems. This may involve the establishment of specialised help desks and helplines that are available around the clock and are staffed by experienced professionals who are able to provide immediate psychological support and advice. Working together with non-governmental organisations (NGOs) will result in an increase in the provision of legal assistance and services to victims who are coping with the consequences of cyberattacks. Furthermore, recovery and rehabilitation can be considerably improved by employing a victim-centered strategy that takes into consideration the particular needs and experiences of each victim. This approach can assist victims in gaining confidence and establishing their life.

It is the responsibility of the platform to ensure that social media and other online platforms have content moderation methods that are both effective and appropriate, with the goal of preventing the dissemination of content that is offensive. It is imperative that the platforms incorporate rapid reporting tools, which allow users to either report abusive content or perform rapid identification of abusive behaviour or content. They are required to speed up the process of erasing the content in order to effectively protect users. Additionally, in order to protect user rights, platforms need to have clearly defined protocols for sharing relevant user data with law enforcement authorities in a manner that is in accordance with the legislation and regulations that are currently in place regarding privacy.

Fostering international cooperation: In order to develop a unified response to cybercrime, it is important to encourage a collaborative approach among cyber law enforcement organisations around the world. It is necessary to achieve convergence of the cybercrime laws of various jurisdictions in order to close gaps that are used by cybercriminals operating on a global scale across the world. Through the sharing of intelligence, best practices, and resources, the authorities may be able to improve their ability to investigate and prosecute cybercriminals who operate across international borders. Globally, there will be an increase in cybersecurity.

Bibliography

Primary Sources- Statutes and Books

Statutes

- UNCITRAL Model Law on Electronic Commerce (1996) with Additional Article 5 as adopted in 1998, United Nations on International Trade Law.
- Information and Technology Act 2000
- The Information and Technology (Amendment) Act 2008.
- Data Protection and Privacy Act 2023
- The General Data Protection Regulation
- Bharatiya Nayaya Sahita Act 2023

Books

- Prof. R.K.Chaubey, An Introduction to Cyber Crime and Cyber law, Kamal Law House, 2012.
- Abraham D. Sofaer, Seymour E, .The Transnational Dimension of Cyber Crime Terrorism, Hoover Institution Press, 2001.

Secondary Sources- Websites, Articles and Journals

Websites

- Artificial Intelligence: Key Business and Legal Issues to Consider, 19th Sept 2023, https://www.sidley.com/en/insights/newsupdates/2023/09/artificial-intelligence-key-business-and-legal-issues-to-consider.
- UNRIC – Cyber Violence against Women: https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/
- UNODC Cybercrime Module: https://www.unodc.org
- OJP Cyberstalking Report: https://www.ojp.gov
- GeeksforGeeks – Cyberstalking: https://www.geeksforgeeks.org
- Cyberbullying.org: https://cyberbullying.org
- iPredator – Cyberstalking Facts: https://ipredator.co

- Oxford University – Online Harassment: https://reportandsupport.ox.ac.uk
- EAP India – Online Harassment: https://www.eap-india.com
- WorldPulse – Cyberstalking: https://www.worldpulse.org
- ResearchGate – Deepfake Study.
- USAII – Deepfake Technology Overview.
- Unit21 – Deepfake Definition.
- Proofpoint – Deepfake Threat Reference.
- Fortinet – Deepfake Cyber Glossary.
- MIT Media Lab – Deepfake Detection Project.
- WIPO Magazine – Deepfakes in Entertainment.
- Stimson Center – AI and Violence Against Women.
- Vikaspedia – Digital Abuse of Women.

Journal Articles

- Kim Barker & Olga Jurasz, *Online Misogyny* (2019) Journal of International Affairs 95, 114.
- Mika Westerlund, "The Emergence of Deepfake Technology: A Review" (2019) 9(11) *Technology Innovation Management Review* 39–52.
- S. Nivedha & Samanvitha Murali, "Deepfakes in India: Unraveling India's Legislative Uncertainty and Jurisdictional Dilemma" (2024) 11(11) *TIJER* 604–622.
- Avadhesh Pratap Singh, Madhav Goswami & Mugdha Garg, "The Ethics of Deepfakes: A Digital Age Crisis" (2024) 6(5) *International Journal of Legal Science and Innovation* 393–406.
- Shraddha Pandit & Jia Singh, "The East & West of Deepfakes: A Comparative Study of Laws in India & UK" (2024) 6(3) *International Journal of Legal Science and Innovation* 1324–1336.
- Tasnimul Md Hassan, "The Perils and Promises of Artificial Intelligence in Criminal Sentencing" (2024) 19(2) *Indian Journal of Law and Technology*.
- Shailendra Rajput, "Critical Analysis in Cyber Crime Related to Artificial Intelligence with Indian Perspective" (2025) 10(33s) *Journal of Information Systems Engineering and Management*.
- Anand, E. & Kaushik, T.K., "From Privacy Breach to 'Virtual Rape': Analysing Revenge Porn as Cybercrime against Women" (2026) 9(1) *National Journal of Criminal Law*.
- ANTARA ROY, "Artificial Intelligence With Law in India" (2024) 12(1) *IJCRT*.

Research Papers / Reports / Working Papers

- Jiyanshi Yadav & Ashish Parihar, "Deepfakes: The Nexus of Technology and Crime" (2025) SSRN Electronic Journal.
- Francesca Palmiotto, "Detecting Deep Fake Evidence with AI: A Criminal Law Perspective" (2023) SSRN Electronic Journal.
- NLU Assam Law Review, Vol. 7, Article 7.
- National Law University Assam PDF (Cyber law journal).
- Samridhi Goyal, "Cyber Crimes Against Women and Prevention" (CNLU, 2025).
- Kerala Fire & Rescue Journal, Vol. 10.
- IJELS Article on Impact of Cybercrime.
- IOSR Journal of Humanities and Social Science, Vol. 29 Issue 11.
- IJCRT Research Paper (Deepfake-related).

Blogs / Online Articles

- Tsaaro, "Impact of DPDP Act on AI" (2024).
- Trilegal, "DPDP Decode: AI & Data Protection" (2023).
- IJLT Blog, "Deepfake Conundrum & DPDP Act" (2024).
- MIT-WPU Blog, "Ethical Implications of Deepfake Technology".
- Woxsen Law Review Blog Papers.
- Aspiring for Intelligence (Substack article).

Newspaper Articles / Media Reports

- Aaratrika Bhaumik, "Regulating Deepfakes in India" *The Hindu* (2023).
- Dia Rekhi & Suraksha P., "Experts Flag Data Bill's Silence on AI" *Economic Times* (2023).
- "Digital Personal Data Protection: Update This Law" *Mint* (2023).
- India Today Web Desk, "Rana Ayyub Deepfake Case" (2018).
- Nilesh Christopher, "Deepfakes in Indian Election Campaign" *Vice* (2020).
- Odisha TV News Report on Cyber Pornography Conviction.
- Times of India, Cyber Pornography Case Report.

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618