Indian Journal of Modern Research and Reviews

This Journal is a member of the *'Committee on Publication Ethics'*

Online ISSN:2584-184X

Research Article

An Analytical Study on Deepfake Sexual Content in India: Criminal Liability and Constitutional Protection of Dignity and Privacy

Aditya [1], Dr. Poonam Verma [2*]

[1-2] LLM Scholar, School of Law, Justice and Governance, Gautam Buddha University
Greater Noida, Uttar Pradesh, India

Corresponding Author: * Dr. Poonam Verma

DOI: https://doi.org/10.5281/zenodo.20625836

Abstract

Deepfake sexual content has emerged as a serious manifestation of artificial intelligence misuse in the digital era, raising significant concerns regarding criminal liability, constitutional rights, and digital safety in India. These AI-generated synthetic media forms, often created without consent, pose severe threats to an individual's dignity, privacy, autonomy, and reputation. Although deepfake technology has legitimate applications in entertainment and communication, its misuse for producing non-consensual sexually explicit content has resulted in growing incidents of cyber harassment, gender-based violence, and psychological harm.

This study provides a doctrinal and analytical examination of deepfake sexual content in India, focusing on the adequacy of existing legal frameworks such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and constitutional protections under Article 21 of the Constitution of India. It explores criminal liability for creation, dissemination, and circulation of deepfake pornography, along with intermediary responsibility under Indian cyber law. The research further analyzes landmark judicial decisions on privacy, dignity, and freedom of expression to understand how constitutional jurisprudence addresses emerging digital harms.

The study finds that while existing laws offer indirect remedies, they are insufficient to address the unique challenges posed by AI-generated sexual content due to the absence of specific statutory provisions. It highlights enforcement difficulties such as anonymity of offenders, rapid content dissemination, cross-border jurisdiction issues, and lack of forensic capabilities. The paper concludes that India requires dedicated legislation, stronger regulatory mechanisms, improved cyber forensic infrastructure, and enhanced constitutional safeguards to effectively combat deepfake-related sexual exploitation while protecting human dignity and privacy in the digital age.

Manuscript Information

- **ISSN No:** 2584-184X
- **Received:** 04-04-2026
- **Accepted:** 02-06-2026
- **Published:** 10-06-2026
- **MRR:**4(6); 2026: 55-63

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Aditya, Verma P. An analytical study on deepfake sexual content in India: criminal liability and constitutional protection of dignity and privacy. Indian J Mod Res Rev. 2026;4(6):55-63.

Access this Article Online

www.mrrjournal.in

KEYWORDS: Deepfake, Artificial Intelligence, Cybercrime, Sexual Exploitation, Privacy, Dignity, Article 21, Criminal Liability, Intermediary Liability, Digital Harassment, Constitutional Law, India.

1. INTRODUCTION

AI and digitalization have revolutionised communication, entertainment and information sharing globally. One of the most recent and controversial and detrimental technological improvements is known as "deepfake" technology. Although deepfakes have legitimate uses such as in the film industry, in educational environments and in virtual communication services, there are serious legal, ethical and constitutional concerns about their misuse. [2] on the whole, deepfakes are fabricated pieces of audio, video, or image content, highly realistic, but non-true, produced using artificial intelligence techniques, especially deep learning algorithms.[1]

The rampant spread of such gender-bentcontent on social media platforms compounds the negative effect as it can be quickly piped into digital networks, inflicting emotional, reputational, psychological, and social trauma to the victim.

Current laws related to cybercrime, such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and those on obscenity, defamation, identity theft, voyeurism, and privacy offer partial protection but do not provide a holistic solution to address the unique issues posed by deepfake sexual content.[2] The lack of explicit laws leaves gray areas in criminal liability, evidentiary process, intermediary responsibility, and protecting the victim's interests.

In addition to the above, creation of deepfake with sexual images and content touches the gender-related aspects of equality and dignity, which are basic human rights, as these images most affect women and marginalised groups.

The problem of the study is that the technological advancement is exceeding the legal regulation in India. The study aimed to reflect upon the criminal liability with deepfake sexual content in India and analyse the constitutional safeguards for dignity & privacy in the digital age as well.[3]

2. REVIEW OF LITERATURE

As AI and deepfake technologies have come into existence, there has been significant academic debate on issues of privacy, cyber-criminal activity, digital ethics and misinformation. The threat of posting deep fake sexual content is already ample in the existing literature with regard to individual dignity,
autonomy and constitutional rights, particularly for women and vulnerable communities. [4]

Robert Chesney and Danielle Keats Citron explore the threats of deep fake technology to democracy, privacy, and national security at great length. [2] the authors contend that deepfakes can "tool public perceptions and erode trust in reality by creating hyper-realistic but faux digital content. Their work in particular focuses on the threats of non-consensual pornographic deepfakes—whereby AI systems are used to create pornographic images of female faces—causing long-term reputational and psychological harm, especially to women.[5]

Danielle Keats Citron's work on technical harassment and cyber abuse is pivotal, as far as contextualizing this intersection of internet technology and sexual exploitation. [4] She gives reasons technologically-facilitated modes of abuse (revenge porn and manipulated sexual imagery) offend a sense of sexual privacy and dignity. Citron also contends that standard legal remedies frequently fail as online harms proliferate and are readily available and indelible.[6]

Mary Anne Frank's examines the gendered aspects of online harassment and sexual exploitation in cyberspace in a critical manner.[7]She documents how women are overrepresented in digital sexual violence, such as non-consensual explicit imagery and identity-based harassment. In his view, there is a lack of robust legal protections and that results in a "culture of impunity in online environments.Franks says there's a lack of strong legal protections and that creates a "culture of impunity in online environments".

Indian researchers who consider the question of the law of cybercrimes have also pointed out the lack in the legal framework to cope up with newer cybercrimes. Justice Yatindra Singh notes, for example, that the Information Technology Act, 2000 (IT Act), does not explicitly mention AI-generated harms like deep fakes but is limited to traditional cyber offences like hacking, obscenity, and identity theft etc. Aparna Viswanathan, on the other hand, reports that the laws governing cyber offences are concerned with traditional crimes of hacking, obscenity, identity theft, etc., and do not explicitly refer to AI generated crimes.[8]

Cybercrime regulation scholar N.S. Nappinai has pointed out that the pace of technological change far outstrips the development of the law in India.[9] She has also highlighted the difficulties for the law to keep up in many areas, such as identification of offenders, methods of gathering electronic evidence, and how criminal liability can be established in cybercrime offences where dissemination and anonymity remain major problems.

Since the Justice K.S. Puttaswamy v. Union of India decisions, the constitutional aspects of privacy have already been heavily debated. His research has shown that the digital privacy in the

[1] Aparna Viswanathan, Cyber Law: Indian and International Perspectives 214 (LexisNexis, New Delhi, 2021).

[2] The Information Technology Act, 2000 (Act 21 of 2000), ss. 66C, 66D, 66E, 67 and 67A; The Bharatiya Nyaya Sanhita, 2023.

[3] Gautam Bhatia, Privacy in the Modern Constitutional State 198 (Oxford University Press, New Delhi, 2019).

[4] Danielle Keats Citron, Hate Crimes in Cyberspace 102 (Harvard University Press, Cambridge, 2014).

[5] Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" 107 California Law Review 1753 (2019).

[6] Danielle Keats Citron, "Sexual Privacy" 128 Yale Law Journal 1870 (2019).

[7] Mary Anne Franks, "Sexual Harassment 2.0" 71 Maryland Law Review 655 (2012).

[8] Aparna Viswanathan, Cyber Law: Indian and International Perspectives 221 (LexisNexis, New Delhi, 2021).

[9] N.S. Nappinai, Cyber Crimes and the Law 149 (OakBridge Publishing, New Delhi, 2010).

digital age is not confined to physical privacy rather extends to the control of one's information, reputation and dignity that is all touched by the unauthorised circulations of private content.[10] Properly so, as the unauthorised manipulation and dissemination of intimate content is a violation of the constitutional right to privacy guaranteed by Article 21 of the Constitution.[13]

AI-generated deepfake pornography aimed at humiliating, intimidating, or silencing women is a modern form of gender-based violence. Feminist legal scholars and digital rights activists have also highlighted that creation of such deepfake content can have detrimental impacts on women's dignity.

Intermediary liability and platform governance is also discussed in the literature. To this end some scholars wish to see more responsibility coming from social media companies and other digital middlemen to detect and remove harmful deep-fakes content.[11] Yet there is the issue of freedom of speech and overcalling restrictions on freedom of expression, as well as technological feasibility of automated detection mechanisms.

While there are many publications covering cybercrime, privacy, and artificial intelligence, crucial research gaps are identified. Much research has either studied the technology of deepfakes or issues pertaining to cyber regulation. Moreover, limited studies have been given on the issue of so called deepfakes sexual content in context with criminal liability and constitutional protection of dignity and privacy in India. In addition, there is a lack of detailed analysis on how the notions of intermediary obligations, as well as legal remedies and protections for victims, will apply when dealing with AI-generated sexual exploitation.

Hence, the current study attempts to fill this lacuna and analyze the criminal and constitutional dimensions of deep fake sexual content in India and also assess the sufficiency of the current legal frameworks and suggest appropriate changes.

3. OBJECTIVES OF THE STUDY

To explore the idea and the technological character of deepfake sexual material.

To investigate the laws pertaining to the offences of Deepfake in India.

To learn about criminal liability for the development, dissemination and circulation of deepfake sexual images.

To examine dignity, privacy and reputation protection in the context of constitution.

To examine judicial perspectives on issues of privacy, cybercrime and digital sexual exploitation.

Identifying gaps and problems related to the existing laws

To recommend law and policy interventions to address issue of Deep fake pornography in India.

Research Questions

What is the definition of a deepfake "sex" clip and how tech does it work?

What is the current situation with regards to the penality available under Indian law for committing a criminal deep fake sexual offence?

In what ways is deepfake pornography a violation of constitutional rights to dignity and right to privacy?

What about existing cyber legislation and criminal legislation; is it sufficient to combat AI generated sexual exploitation?

How can the protection of Indian law against sexual abuse using deepfakes technology be enhanced through changes in the law?

4. RESEARCH METHODOLOGY

The present study entails a doctrinal research and analytical methodology approach to analyze the rising problem of Deepfakes accompanied sexual materials in the Indian social set up and its impact on criminal liability and privacy and constitutional right. Qualitative analysis is the main method of research and secondary data sources have been used frequently.

Existing legal provisions, constitutional principles, judicial decisions, and statutory frameworks related to cybercrime, privacy, obscenity, digital harassment and artificial intelligence have been analysed by using the doctrinal method. The research aims to explore how the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023 and certain constitutional provisions, especially Article 21 of the Constitution of India, can be applied to these situations.

The present study also examines the decisions given by the Supreme Court of India and other High Courts pertaining to Privacy, Dignity and Freedom of Speech, Intermediary Liability, Cyber Offences and Digital Rights. The judicial interpretation has been analyzed critically in order to find out the protections afforded in the constitution when it comes to sexual exploitation through technological facility.

The study relies on secondary data which has been gathered from books, journal articles, law reviews, legal commentaries, government reports, committee reports, online databases, newspapers and authentic electronic resources. Electronic sources of academic writing on artificial intelligence, cyber law, confidentiality in the digital age, online harassment and feminist legal theory have also been reviewed in order to develop interdisciplinary insight into this topic.

The methodology that has been used is Analytical which is aimed at analyzing the existing legal framework is adequate or not for deepfake sexual content. The study uncovers lacuna in Indian cyber laws, implementation issues, a lack of evidence and even regulatory vacuum. International legal developments and regulatory approaches have also been compared to see how people across the world are responding to deepfake technology and to digital sexual abuse.

The research is limited to the legal and constitutional aspects of sexual content by Deepfakes in India. The study is not empirical research of fieldwork and does not depend upon interviews or any quantitative survey work. Instead, it provides

[10] Gautam Bhatia, Privacy in the Modern Constitutional State 204 (Oxford University Press, New Delhi, 2019).

[11] Karan Lahiri, "Deepfakes, Free Speech and Platform Liability in India" 14 Indian Journal of Law and Technology 92 (2022).

in-depth legal analysis of laws, judicial decisions, and policies on deepfake technology and digital privacy.

The methodology aims to offer a holistic account of the criminal and constitutional ramifications of deepFake sexual content, while recommending ways to enhance legal protection, ensure human dignity, and to regulate artificial intelligence in the digital age effectively.

5. DISCUSSION / ANALYSIS

Concept and Nature of Deepfake Sexual Content

Advanced algorithms, especially Generative Adversarial Networks (GANs), enable deepfake systems to manipulate and synthesize digital content, such as audio, video, and images, with a remarkable degree of realism.Deepfake technology: Refers to the use of artificial intelligence and machine learning techniques to generate manipulated digital content that appears authentic and realistic.[12]

At first, deepfake technology has been utilized in entertainment and film creation, virtual reality, education, and digital communication, where it provides authentic dubbing, movie visual effects, recreation of historical materials and interactive virtual experiences.[4] But, with the advent of easily accessible artificial intelligence software and editing applications, deepfake content has come to be produced widely today, even without much technical expertise.[5] However, today everyone can create deepfake content with minimal technical expertise via easily accessible online tools and mobile applications.

Deepfake sexual content can be particularly harmful when generated by inserting a person's face or likeness into sexually explicit imagery or video without their knowledge, and can be hard to detect, raising the likelihood of deception and exploitation. The victim is usually a woman, celebrity, journalist, blogger or private individuals, and psychological, reputational and emotional damage inflicted by Deepfake pornography is severe.[13]

Deepfake sexual content is fundamentally invasive, as it infringes upon the bodily autonomy, sexual privacy, and personal dignity of the individual(s) shown in the portrayed explicit material, in a way that cannot be achieved with conventional sources of sexually explicit content or even defamatory material. Although the material is completely fabricated, it has potentially serious, real and devastating social consequences that affect victims.[14] Victims can suffer humiliation, anxiety, depression, isolation, professional damage, and online harassment.

Deepfake sexual content is also a contemporary cyber gender violence. It is highly likely that the vast majority of deepfake pornography found online targets women to be used for revenge, misogyny, blackmail, intimidation or silence women in public and professional settings. Thus, there is a link between the phenomenon and gender discrimination, digital abuse and online exploitation.

The problem is exacerbated by the speedy dissemination of both manipulated content, via social media platforms. Once explicit material goes viral, it is hard to remove it and digital platforms enable offenders to replicate and share it instantaneously across jurisdictions. [12] There is also the anonymity of digital platforms, which makes it difficult to identify offenders and implement legal measures.

The "traditional" legal regimes were not built to handle AI-powered synthetic media and the ability to misleadingly create extremely realistic fabricated media. With this in mind, there are risks that current cyber-legislation and/or policy frameworks could be lacking in classification or regulation of the harms associated with deepfakes.

Deepfake sexual content directly violates Article 21 of the Constitution of India, which provide constitutional protection to the right to privacy, dignity and reputation that every individual is entitled to.[15] The perpetration of fraudulent sexual content to defame or tarnish a person's identity is an example of an attack on informational autonomy and mental integrity at the constitutional level. It is thus not a mere cybercrime problem, but a problem of human rights and constitutional protection in the digital age.

The use of AI in creating deepfake sexual material, therefore, exemplifies the darker aspects of AI technology, where innovation for good purpose is used for harassment and exploitation, and ultimately abuse. But as it surges in popularity, it is clear the need to urgently regulate it using the law, technology, and constitutional measures to combat digitally created sexual violence.

Criminal liability in Indian law.

In fact, all legally binding layers governing cybercrime and criminality have been written and conceived prior to the advent of technologically advanced AI tools and algorithms for creating fabricated intimate content, which causes humiliation, social harassment and psychological trauma. Therefore, Deepfake sexual porn videos represent a new form of cybercrime and gender-based violence, rendering the traditional legal framework insufficient.

The introduction of Section 66C, which criminalizes identity theft, and Section 66D, which criminalizes cheating through personation, in the Information Technology Act, 2000, shows that although the Act predates the surge in AI driven technologies, its general narrative provides a limited scope of regulation for offences surrounding deepfake pornography.[16]

Similarly, Sections 67 and 67A punish dissemination of obscene and sexually explicit materials in electronic form and

[12] Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" 107 California Law Review 1753 (2019).

[13] Mary Anne Franks, "Sexual Harassment 2.0" 71 Maryland Law Review 655 (2012).

[14] Danielle Keats Citron and Mary Anne Franks, "Criminalizing Revenge Porn" 49 Wake Forest Law Review 345 (2014).

[15] Justice Yatindra Singh, Cyber Laws 322 (Universal Law Publishing, New Delhi, 2019).

[16] The Information Technology Act, 2000 (Act 21 of 2000).

since deepfake pornographic videos could be shared on social media or apps, or websites, they could also fall within the purview of criminality under the provisions of these Section.[17]

In addition to cyber laws, Bharatiya Nyaya Sanhita, 2023 provides for criminal liability related to defamation in many cases of deepfake sexual content. Deepfake sexual content will, in many cases, also amount to offences under voyeurism, insult to modesty, stalking and sexual harassment, which are enumerated under the criminal law provisions. In many instances, the usage of such content is for blackmail, intimidation, revenge or coercion, and thus causes the victim significant emotional distress and fear. This will further amount to criminal intimidation and criminal harassment under provisions of criminal laws.

Thus, criminalization of deep fake in sexually explicit content is in harmony with the constitutional framework of India where the right to life and personal liberty also encompasses the right to informational privacy, mental integrity and autonomy. [23] The Government has a constitutional duty to provide for effective legal remedies against sexual exploitation and online abuse using technology.[18]

Intermediaries and digital platforms are also important in deepfake, with regards to criminal liability. However, the anonymous and borderless nature of online communication makes its detection and prosecution difficult, while Section 79 of the Information Technology Act can result in the loss of safe harbour protection for social media companies and other internet platforms that fail to take appropriate "due diligence" to remove unlawful content after being informed of it. Efficient detection systems are absent and content moderation is slow, which further compounds the harm upon victims.[19]

All this said, the Indian law framework still has several challenges on the ground in terms of effectively dealing with crimes involving deepfakes in practice and a complete lack of any specific statutory definitions of AI sexual exploitation, impersonation and non-consensual synthetic media raise the pressing need for more comprehensive legislation in India specifically addressing deepfakes.[20]

Challenges in Enforcement

Manipulated media content can often be created and circulated by perpetrators using fake profiles or anonymous communication, which makes it easy for them to evade identification and difficult for law enforcement agencies to investigate and prosecute the crimes.[21]

Digital content also tends to become permanent – once up online, copies can be made, downloaded and re-shared within a few moments by the countless users – and can travel across platforms, making effective containment almost impossible.

An issue is also the procedural difficulties in securing cooperation from foreign authorities and spreading platforms for investigation since deepfake content may be hosted on servers within other countries or spread via digital platforms.

The low level of technical know-how among investigators and law enforcement agencies is another major hurdle. Deepfake technology also requires specialized technical expertise, which is required to detect and authenticate the manipulated content and take necessary action. Many police officials and law enforcement agencies also lack adequate information regarding digital forensics and investigation, which make up an important part of the effectiveness of any legal remedy for victims of manipulation.Delay, as a result of lack of expertise or essential resources for digitized evidentiary analysis, also often hamper the effectiveness of the legal remedial actions.[22]

The lack of AI-specific tools and the ability to construct an AI deepfake that closely mimics human body movements, speech patterns and facial expressions further compound the difficulty of detecting AI-generated content.

Further, the delays in takedown of such content by intermediaries under Indian cyber law and social media platforms means that harmful deepfake sexual content is often not removed immediately and the victims have to continuously email various platforms and authorities to have the content removed. Even though intermediaries are required to ensure due diligence under Indian cyber law, this is never consistent because of the procedures to be followed, absence of moderation systems and inadequate reporting mechanisms within the platform.

The collective nature of these challenges highlights both the need for more robust legal and institutional tools to protect against deepfakes and AI-powered cybercrimes, as well as the need for more advanced technological capabilities, expertise and international cooperation among law enforcement agencies to effectively combat and regulate AI crime in the digital age.[23]

Case Laws / Case Analysis

Indian judiciary has also contributed in a major way in giving more protections related to privacy, dignity, reputation and digital rights which are directly concerned in dealing with harm arising from deepfake porn content. While there is no significant case law yet established in India on the topic of deepfake pornography, several precedent setting cases

[17] The Information Technology Act, 2000 (Act 21 of 2000), ss. 67 and 67A.

[18] The Information Technology Act, 2000 (Act 21 of 2000), s. 79.

[19] Deepa Das Acevedo, "Digital Harassment and Privacy Rights in India" Indian Journal of Law and Technology 89 (2021).

[20] Aparna Viswanathan, Cyber Law: Indian and International Perspectives 231 (LexisNexis, New Delhi, 2021).

[21] N.S. Nappinai, Cyber Crimes and the Law 156 (OakBridge Publishing, New Delhi, 2010).

[22] Aparna Viswanathan, Cyber Law: Indian and International Perspectives 233 (LexisNexis, New Delhi, 2021).

[23] Gautam Bhatia, Privacy in the Modern Constitutional State 216 (Oxford University Press, New Delhi, 2019).

regarding privacy, cybercrime, freedom of speech and online harassment are relevant with regards to the concepts of law concerning the exploitation of AI in sexual content.

In Justice K.S. Puttaswamy v. Union of India, the Supreme Court of India recognized the right to privacy as a fundamental right protected under Article 21 of the Constitution. The Court held that privacy includes personal autonomy, bodily integrity, informational control, dignity, and protection of individual identity.This judgment is highly significant in the context of deepfake sexual content because unauthorized manipulation and circulation of intimate fabricated material directly violates informational privacy and personal dignity.The decision established that individuals possess constitutional protection against unlawful intrusion into their private lives, including misuse of personal data and digital identity.[24]

In R. Rajagopal v. State of Tamil Nadu, the Supreme Court found that every person has a right to protect the privacy of his/her personal life, family life, marriage, and his/her reputation against any publication without his/her consent, except in certain limited situations envisioned in the article, which are related to certain types of public records. This rule has become relevant in recent deepfake sexual instances where fabricated explicit content is being distributed without the victim's consent, tampering with their reputation and dignity along the way.[25]

The Supreme Court's ruling in Shreya Singhal v. Union of India is also pertinent in the case of deepfake sexual content, where it highlighted that freedom of speech cannot be invoked to allow harmful use of online platforms when it is contrary to dignity and privacy. The Court also noted that there is a need for responsibility of digital platforms with regard to addressing illegal content online and referred to intermediary liability.[26]

It was the first case in India – considered one of the early Indian cybercrime convictions with reference to the harassment of a woman through obscene and defamatory e-mail messages Although this was not a deep fake case, the principals involved in this case are relevant to issues of sexual exploitation and cyber harassment in the current context.

In Kharak Singh v. State of Uttar Pradesh, the Supreme Court noted that personal liberty and protection from arbitrary interference in anyone's life are crucial elements of the Article 21 of the Constitution. The Supreme Court observed that any sort of interference in the personal liberty of anyone constitutes violation of constitutional guarantees under Article 21. This judgment established early constitutional principles to guide the protection of privacy rights in India and remains relevant in the context of digital surveillance and misuse of identity and information of an individual.[27]

In Subramanian Swamy v. Union of India, the Supreme Court reiterated the constitutionality of criminal defamation and that reputation is an integral part of the right to life under Article 21.[28]Reputational harm and public humiliation caused by deepfake explicit content is often extremely harmful, rendering the concepts of this judgment particularly relevant to the question of criminal liability for fabricated explicit content.

As deepfake sexual exploitation becomes increasingly prevalent, deeper judicial understanding and legislative change are needed to shield dignity, privacy, autonomy and reputation in an AI world.While courts have yet to establish a specific legal doctrine for tackling deepfakes sexualization, the available constitutional principles and jurisprudence on cybercrime offers adequate legal scaffolding for the regulation of deepfake-induced harms in India.

Findings

According to the study, DF sexual content has become a grave category of cyber violence, targeting vulnerable people and women in particular, through technology. The exploitation of AI-driven deep fake pornography poses a more sophisticated and harmful version of online exploitation. The psychological harm, defamation, abuse and violation of autonomy, dignity and privacy of individuals in a digital landscape wrought by deepfakes pornography is not concern enough.

The study also indicates the future remedies and solutions are presented within the existing legal framework in India, which are fragmented and indirect in the context of deep fake sexual offence. Provisions in the Information Technology Act, 2000; The Bharatiya Nyaya Sanhita, 2023; and constitutional protections under Articles 19 and 31 on privacy and dignity of the individual may be brought in, but there is no specific provision dedicated to AI agent sexual manipulation and synthetic media offences. Lack of clear terminology in the statute and lack of specific legal parameters leave unclear the issue of criminal responsibility, evidentiary requirements, and victim safeguarding.

Another important finding of the study is that the fundamental rights of India enshrined in the Constitution of India, specifically the right to dignity and privacy guaranteed by Article 21 of Indian Constitution, can serve as a good legal and theoretical underpinning in safeguarding individuals from deepfake abuse. For example, the recognition of the right to informational privacy, bodily integrity, reputation and mental integrity provided by a judge gives weight to the notion that the creation of non-consensual sexual deep fake videos is a severe violation of fundamental rights.

Yet another key discovery is the technological and procedural challenges that the enforcement agencies encounter when investigating offences committed by deepfakes. Limited powers of legal remediation due to challenges, including anonymous perpetrators, quick dissemination on the Internet, lack of forensic skills, cross-border issues involving jurisdiction, and lack of advanced detection capabilities. Existing investigation

[24] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

[25] R. Rajagopal v. State of Tamil Nadu (1994) 6 SCC 632

[26] Shreya Singhal v. Union of India (2015) 5 SCC 1.

[27] · Kharak Singh v. State of Uttar Pradesh AIR 1963 SC 1295.

[28] Subramanian Swamy v. Union of India (2016) 7 SCC 221.

mechanisms include tools that lack sophistication in addressing AI-generated content.

The study also notes that women are disproportionately targeted in the production of non-consensual deepfake pornography, as well as journalists, celebrities, influencers and the marginalized. This is the symptom of online harassment and abuse of technology, misogyny and violence against women in general. Emotional, social and professional consequences are common for a victim of having explicit content manipulated and circulated.

The research also highlights the shortcomings in intermediary regulation and content moderation mechanisms. While the growth of manipulative content can spread very quickly over digital platforms, social media and digital/native intermediaries do not necessarily remove harmful content quickly enough. Victimization and online abuse is ongoing owing to delayed takedown and less effective monitoring mechanisms.

Last but not least, the study highlights that there is a need for holistic and specific legislation for deepfake technology and AI-generated harms in India. The current depth of laws is inadequate to control synthetic media offences and the rather high-tech forms of cyber-exploitation of victims. Robust legal protections, cyber forensic tools, intermediate liability, and public awareness are crucial for ensuring that dignity, privacy, and digital rights are protected in the era of digital innovation and artificial intelligence.

Recommendations / Suggestions

The study faithfully suggests that India should have dedicated and comprehensive laws pertaining specifically to the deepfake technology and the harms they can cause, through artificial intelligence. Today's cyber legislation and criminal laws have not yet been designed to be effective in controlling the creation, publication, and dissemination of non-consensual deep fake sexual content. General provisions in a separate statutory framework should clearly define the making of fake, sexually explicit material of an individual using AI as criminalised behavior.

The law should introduce clearly defined legal terms with regard to deepfakes, synthetic media, digital impersonation, and genital imagery created with AI tools to reduce the ambiguity of enforcement and prosecution. Moreover, there must also be clear consent-based standards, and any use of someone's image, voice, or identity for explicit use without their consent must also be deemed to be an offence, even if the image/video are technically made-up or manipulated.

The study also recommends the establishment of specialized cyber forensic laboratories and the foundation of technological infrastructure to detect deep fidelity and assurance of electronic evidence. AI-Generated content is becoming more advanced and harder to detect with traditional investigations. For that reason, public coaching should have the option to use state-of-the-art forensics tools, machine learning detection, and technical experts who can see manipulated digital material and work out where it originated.

More extensive due diligence should be imposed on social media, online intermediaries and digital communication services in checking, filtering and removing harmful content in deepfake posts. To enforce quicker takedown processes and strict liability requirements to make sure that explicit, manipulated content is removed from the platform promptly after it's reported by victims or found by the authorities. To not do so should result in legal penalization and consequences.

Recommendations also involve creating institutional structures to support victims of deepfake sexual abuse, such as compensation mechanisms, psychological counselling, online rehabilitation and legal support. The mental and emotional distress, loss of reputation, anxiety, depression and humiliation faced by the victims is often profound. Hence, the reaction that should be made through the law should not be just on punishment but also should be on protection and rehabilitation of the affected persons.

National and institutional-level public awareness needs to be undertaken around consent, online privacy, the misuse of AI, and cyber safety. Schools, the media and online platforms must push back against the dangers of deep fake technologies and educate users on how to report online abuse.

The study also calls for the training of police officers and investigators, prosecutors and judges in handling AI-related offenses through specially designed technical training programs. Enforcement goes hand in hand with digital forensic and synthetic media technologies, collection of electronic evidence, and governances of online platforms. However, enforcement agencies will likely continue to struggle to investigate and prosecute deepfake offences in absence of the necessary technological skills.

The judiciary should continue expanding constitutional jurisprudence relating to informational privacy, digital dignity, mental integrity, and online autonomy under Article 21 of the Constitution of India. Courts must recognize that non-consensual deepfake sexual content constitutes a serious violation of fundamental rights and human dignity in the digital era.

Finally, stronger safeguards should be introduced for protecting women, children, and vulnerable groups from online sexual exploitation through artificial intelligence technologies. Gender-sensitive cyber laws, stricter punishment for AI-generated sexual abuse, and proactive digital monitoring mechanisms are essential to prevent misuse of technology and ensure a safer digital environment for all individuals.

CONCLUSION

Deepfake sexual content has emerged as one of the most dangerous manifestations of artificial intelligence misuse in contemporary society. By enabling the creation of realistic but fabricated sexual material without consent, deepfake technology threatens individual dignity, privacy, autonomy, and reputation on an unprecedented scale. The psychological, social, and professional consequences faced by victims demonstrate that such acts are not merely technological misuse but serious violations of human rights and constitutional values.

In India, the absence of comprehensive legislation specifically targeting deepfake offences creates substantial legal

uncertainty. Although provisions under the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023, offer partial remedies, they remain insufficient to address the unique challenges posed by AI-generated sexual exploitation. The rapidly evolving nature of artificial intelligence requires a modern and technologically responsive legal framework.

Constitutionally, the right to dignity and privacy under Article 21 provides a strong foundation for protecting individuals against digital abuse. Judicial recognition of informational privacy and personal autonomy reinforces the need for robust legal safeguards against non-consensual deepfake sexual content.

The study concludes that India urgently requires dedicated legislation, improved cyber forensic capabilities, stronger intermediary accountability, and greater constitutional sensitivity toward digital sexual violence. A balanced legal approach that protects both technological innovation and human dignity is essential for ensuring justice in the digital age.

REFERENCES

1. Viswanathan A. *Cyber Law: Indian and International Perspectives*. New Delhi: LexisNexis, 2021.
2. Citron DK. *Hate Crimes in Cyberspace*. Cambridge: Harvard University Press; 2014.
3. Bhatia G. *Privacy in the Modern Constitutional State*. New Delhi: Oxford University Press; 2019.
4. Singh Y. *Cyber Laws*. New Delhi: Universal Law Publishing; 2019.
5. Nappinai NS. *Cyber Crimes and the Law*. New Delhi: OakBridge Publishing; 2010.
6. Zarsky T. *Privacy and Data Protection in the Digital Era*. Oxford: Oxford University Press; 2019.
7. Hoofnagle CJ. *Federal Trade Commission Privacy Law and Policy*. Cambridge: Cambridge University Press; 2016.
8. Murray A. *Information Technology Law: The Law and Society*. Oxford: Oxford University Press; 2019.
9. Herring J. *Medical Law and Ethics*. Oxford: Oxford University Press; 2020.
10. Bainbridge D. *Introduction to Computer Law*. London: Pearson Education; 2015.
11. Chesney R, Citron DK. Deep fakes: a looming challenge for privacy, democracy, and national security. *Calif Law Rev*. 2019;107:1753-1819.
12. Citron DK, Franks MA. Criminalizing revenge porn. *Wake Forest Law Rev*. 2014;49:345-391.
13. Franks MA. Sexual harassment 2.0. *Md Law Rev*. 2012;71:655-688.
14. Acevedo DD. Digital harassment and privacy rights in India. *Indian J Law Technol*. 2021;89-104.
15. Lahiri K. Deepfakes, free speech and platform liability in India. *Indian J Law Technol*. 2022;14:92-118.
16. Groh M. Deepfake detection and the role of artificial intelligence. *J Cyber Policy*. 2021;12:44-59.
17. Citron DK. Sexual privacy. *Yale Law J*. 2019;128:1870-1960.
18. Baxi U. Human dignity in constitutional governance. *J Indian Law Inst*. 2002;44:321-340.
19. Duggal P. Cybercrime and digital evidence in India. *Supreme Court J*. 2018;3:45-58.
20. Ajder H. The state of deepfakes: landscape, threats and impact. *Deeptrace Rep*. 2019;7:12-35.
21. Constitution of India. New Delhi: Government of India; 1950.
22. Information Technology Act, 2000 (Act No. 21 of 2000). New Delhi: Government of India; 2000.
23. Bharatiya Nyaya Sanhita, 2023. New Delhi: Government of India; 2023.
24. Bharatiya Nagarik Suraksha Sanhita, 2023. New Delhi: Government of India; 2023.
25. Bharatiya Sakshya Adhiniyam, 2023. New Delhi: Government of India; 2023.
26. Digital Personal Data Protection Act, 2023. New Delhi: Government of India; 2023.
27. Indecent Representation of Women (Prohibition) Act, 1986 (Act No. 60 of 1986). New Delhi: Government of India; 1986.
28. Protection of Children from Sexual Offences Act, 2012 (Act No. 32 of 2012). New Delhi: Government of India; 2012.
29. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. New Delhi: Government of India; 2021.
30. Indian Evidence Act, 1872 (Act No. 1 of 1872). New Delhi: Government of India; 1872.
31. Law Commission of India. *Report No. 267: Hate Speech*. New Delhi: Law Commission of India; 2017.
32. Government of India, Ministry of Home Affairs. *Report of the Committee on Reforms of Criminal Justice System*. New Delhi: Ministry of Home Affairs; 2003.
33. NITI Aayog. *National Strategy for Artificial Intelligence*. New Delhi: Government of India; 2018.
34. UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO; 2021.
35. European Commission. *Proposal for an Artificial Intelligence Act*. Brussels: European Commission; 2021.
36. Ajder H. *The State of Deepfakes: Landscape, Threats and Impact*. London: Deeptrace Labs; 2019.
37. Ministry of Electronics and Information Technology. Available from: https://www.meity.gov.in.

38. National Crime Records Bureau. Available from: https://www.ncrb.gov.in.
39. UNESCO. Available from: https://www.unesco.org.
40. World Economic Forum. Available from: https://www.weforum.org.
41. Internet Freedom Foundation. Available from: https://internetfreedom.in.
42. Electronic Frontier Foundation. Available from: https://www.eff.org.
43. Deeptrace Labs. Available from: https://www.deeptracelabs.com.
44. United Nations Office on Drugs and Crime. Available from: https://www.unodc.org.

About the Corresponding Author

Dr. Poonam Verma is an LLM scholar at the School of Law, Justice and Governance, Gautam Buddha University, Greater Noida, Uttar Pradesh, India. Her academic interests include legal studies, constitutional law, and governance. She is engaged in advanced research and scholarly activities contributing to the field of law and justice.