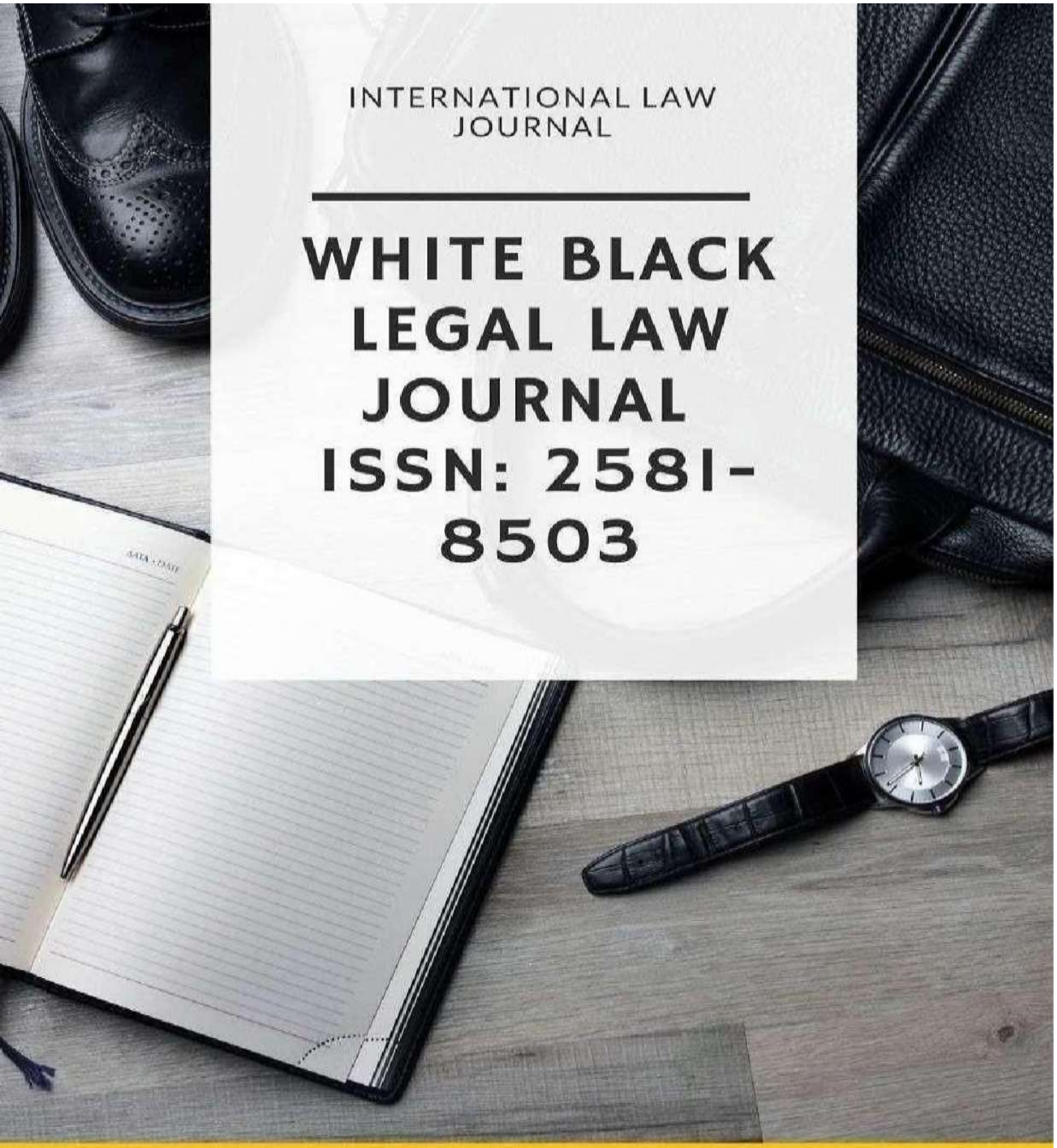

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

DEEPFAKE TECHNOLOGY AND ITS MISUSE AGAINST WOMEN: A CRITICAL ANALYSIS OF LEGAL FRAMEWORKS AND ETHICAL CHALLENGES IN INDIA

AUTHORED BY - MS. SAKSHI[1] & MS. GAYATRI[2]

Abstract

Deepfake technology, enabled by advances in Artificial Intelligence and Generative Adversarial Networks, has transformed digital content creation by producing highly realistic synthetic media. While it offers legitimate applications in entertainment, education, and communication, its misuse has raised serious legal and ethical concerns, particularly in relation to women. In India, the rapid proliferation of deepfakes through social media platforms has led to a surge in non-consensual explicit content, identity manipulation, impersonation, and cyber harassment disproportionately targeting women. Such misuse results in severe psychological trauma, reputational damage, and social stigma, while also discouraging women's participation in online spaces. The existing legal framework in India, primarily governed by the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and constitutional protections under Article 21 of the Constitution of India, provides partial remedies but remains inadequate to address the complexities of AI-generated content. The absence of a clear statutory definition of deepfakes and the lack of dedicated legislation create challenges in enforcement and accountability. Judicial interventions have attempted to bridge these gaps by recognizing personality rights and granting relief against unauthorized digital use of identity. However, the evolving nature of deepfake technology necessitates a more comprehensive and specialized regulatory approach. The issue also raises broader ethical concerns relating to consent, autonomy, and the misuse of emerging technologies. Addressing these challenges requires a balanced framework that strengthens legal protections, enhances platform accountability, and promotes digital awareness to safeguard individual rights in the rapidly evolving digital landscape.

Keywords: Deepfake Technology, Artificial Intelligence, Cyber Harassment, Gender-Based Violence, Privacy and Personality Rights, Indian Legal Framework

[1] Student of LLM, University School of Law, Rayat Bahra University, Mohali, Punjab 140104, India
[2] Assistant Professor, University School of Law, Rayat Bahra University, Mohali, Punjab 140104, India

1. Introduction

Deepfake technology has emerged as a result of the rapid advancement of artificial intelligence, which has drastically changed the production and distribution of digital material. Deepfakes, which are based on sophisticated methods like generative adversarial networks, allow for the modification of photos, movies, and audio to create incredibly lifelike yet fake representations of people. Even though the technology has creative uses in culture and entertainment, its abuse has become a major problem, especially for women. Deepfake information has spread more quickly in India due to the country's extensive use of digital channels like Telegram and Instagram. Non-consensual explicit material, identity deception, and reputational damage disproportionately affect women. In addition to violating privacy and dignity, this kind of misuse causes psychological pain and societal stigmatization. Deepfakes are difficult to identify due to their lifelike appearance, which increases their detrimental effects. Although current laws under the Indian Penal Code and the Information Technology Act, 2000 make an effort to combat cybercrimes, they are unable to adequately handle the particular difficulties presented by content created by artificial intelligence. This disparity demonstrates the increasing conflict between the growth of technology and the defense of individual liberties.[3]

2. Research Methodology

This study adopts a qualitative and doctrinal research methodology to examine the misuse of deepfake technology against women and the adequacy of existing legal frameworks in India. The research is primarily based on secondary sources, including statutes, judicial decisions, academic literature, and credible online materials. Key legislations such as the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 are analyzed to understand their applicability to deepfake-related offences. Constitutional provisions, particularly Article 21 of the Constitution of India, are also examined to assess the protection of privacy, dignity, and reputation. The study further relies on case law analysis to evaluate judicial responses to emerging issues of personality rights, impersonation, and digital misuse. Relevant judgments are critically examined to identify trends and gaps in legal interpretation. Additionally, scholarly articles, journals, and reports on Artificial Intelligence and deepfake technology are reviewed to understand the technical and ethical dimensions of the issue. An analytical and descriptive approach is employed to assess the effectiveness of existing laws and highlight

[3] Meenakshi Meenakshi, "Deepfake Technology and Legal Challenges in India: An Analysis," 3 *International Journal of Teaching, Learning and Education* 18–24 (2024).

regulatory shortcomings. The methodology also incorporates a critical perspective to explore ethical concerns such as consent, autonomy, and gender-based harm. This approach enables a comprehensive evaluation of both legal and societal implications of deepfake misuse in India.

2. Meaning and Evolution of Deepfake Technology

2.1 Definition of Deepfake Technology

Deepfake technology refers to the use of artificial intelligence to create or manipulate digital content in a way that convincingly alters reality. The term "deepfake" is derived from "deep learning" and "fake," indicating the role of advanced AI systems in generating fabricated yet highly realistic images, audio, or videos. These manipulated outputs often involve swapping faces, altering speech, or synthesizing entirely new visual content that appears authentic to the human eye. At its core, deepfake technology relies on sophisticated computational models capable of learning patterns from vast datasets. One of the most significant technological foundations of deepfakes is Generative Adversarial Networks (GANs). GANs function through a dual-model system: a generator that creates synthetic content and a discriminator that evaluates its authenticity. Through continuous interaction, these models refine the output until it becomes nearly indistinguishable from real data. This process enables the creation of hyper-realistic media that challenges conventional methods of verification. In addition to GANs, deepfakes also utilize machine learning techniques such as neural networks, facial recognition, and voice cloning. These technologies collectively contribute to the seamless blending of artificial elements with real-world data, making deepfakes increasingly accessible and difficult to detect.[4]

2.2 Technological Basis: AI and Machine Learning

The development of deepfake technology is deeply rooted in the broader fields of Artificial Intelligence and Machine Learning. Artificial intelligence provides the overarching framework that enables machines to simulate human intelligence, while machine learning allows systems to improve their performance through data-driven training. Within this framework, deep learning—a subset of machine learning—plays a critical role. Deep learning models, particularly convolutional neural networks (CNNs), are designed to process and analyze visual and auditory data with high precision. These models can identify facial features, expressions,

[4] Mika Westerlund, "The Emergence of Deepfake Technology: A Review," 9 *Technology Innovation Management Review* (2019).

and speech patterns, which are then replicated or altered in deepfake content. The accessibility of open-source tools and software has further accelerated the spread of deepfake technology. Applications and platforms now allow users with minimal technical expertise to generate manipulated content, democratizing the technology but also increasing its potential for misuse.[5]

2.3 Evolution and Rise of Synthetic Media in the Digital Age

The evolution of deepfake technology can be traced back to early experiments in image editing and computer-generated imagery (CGI). However, the term "deepfake" gained prominence around 2017, when AI-driven face-swapping tools began circulating on online forums. Since then, rapid advancements in computational power and data availability have significantly enhanced the quality and realism of synthetic media. In the digital age, synthetic media has expanded beyond entertainment and visual effects to include applications in education, marketing, and virtual communication. For instance, deepfake technology can be used to recreate historical figures, enable multilingual dubbing, or enhance accessibility through voice synthesis. These positive applications highlight the transformative potential of the technology. However, the same features that make deepfakes innovative also make them susceptible to misuse. The ability to create realistic yet false representations has contributed to the rise of misinformation, identity manipulation, and digital exploitation. The viral nature of online platforms further amplifies the reach and impact of such content, making synthetic media a powerful yet double-edged phenomenon. As deepfake technology continues to evolve, it blurs the line between reality and fabrication, raising critical concerns about trust, authenticity, and accountability in the digital ecosystem.[6]

3. Understanding Deepfake Technology

3.1 Technical Framework

1. Role of AI, Deep Learning, and Neural Networks

Deepfake technology is built upon the foundations of Artificial Intelligence, which enables machines to simulate human cognitive functions such as recognition, prediction, and decision-making. Within this broader framework, Deep Learning plays a central role by using layered neural architectures to process vast amounts of data. These systems are trained on extensive

[5] Konstantin A. Pantserev, "The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability" *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity* (Springer International Publishing, 2020)(last visited April 25, 2026).
[6] Yifei Wang, "Synthetic Realities in the Digital Age: Navigating the Opportunities and Challenges of AI-Generated Content" *TechRxiv* (2023).

datasets of images, videos, and audio recordings to learn patterns such as facial expressions, speech rhythms, and body movements. A key component in this process is the use of Neural Networks, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs). CNNs are primarily responsible for analyzing visual data, such as identifying facial features and mapping them onto another face, while RNNs are used for sequential data like speech and audio patterns. Another critical technique is Generative Adversarial Networks, where two neural networks—the generator and the discriminator—compete to produce increasingly realistic outputs. This adversarial training allows the system to refine synthetic content to a level that is often indistinguishable from genuine media. The integration of these technologies enables automated learning and continuous improvement, making deepfake tools more accurate, efficient, and accessible. As computational power increases and datasets expand, the realism and sophistication of deepfakes continue to advance.[7]

2. Types of Deepfake Technologies

a) Face-Swapping

Face-swapping is the most widely recognized form of deepfake technology. It involves replacing one person's face with another in images or videos while maintaining realistic expressions, lighting, and movements. This technique uses facial mapping and alignment algorithms to ensure that the swapped face blends seamlessly with the target body. While it has legitimate uses in filmmaking and digital entertainment, it is frequently misused to create misleading or harmful content.

b) Voice Cloning

Voice cloning utilizes deep learning models to replicate an individual's voice by analyzing tone, pitch, and speech patterns. By training on short audio samples, these systems can generate speech that closely mimics the original speaker. This technology is increasingly used in virtual assistants and dubbing but also raises concerns when used for impersonation, fraud, or harassment.

c) "Nudify" Applications

[7] Meghana Lokhande and Prajot Raut, "Artificial Intelligence for Detecting Cyber Attacks in Deepfake & Identity Theft" *2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA)*.

"Nudify" applications represent one of the most controversial and harmful uses of deepfake technology. These tools use AI algorithms to generate non-consensual explicit images by digitally altering photographs, often targeting women. By simulating the removal of clothing or generating synthetic nude images, such applications violate privacy, dignity, and consent. Their existence highlights the darker side of deepfake innovation and underscores the urgent need for legal and ethical safeguards.

Together, these forms demonstrate the versatility of deepfake technology while also exposing its potential for misuse. The same technical framework that enables creative and beneficial applications can also be exploited, making it essential to understand both its capabilities and its risks.[8]

3.2 Accessibility and Proliferation

1. Ease of Creation and Distribution via Social Media

The rapid proliferation of deepfake technology is closely linked to the ease with which such content can be created and disseminated in the digital age. Social media platforms such as Instagram, Facebook, and Telegram provide instantaneous channels for sharing multimedia content with vast audiences. Once a deepfake is uploaded, it can spread rapidly through shares, reposts, and algorithm-driven recommendations, often reaching thousands or even millions of users within a short period. The viral nature of these platforms amplifies the impact of manipulated content, making it difficult to control or contain once released. Unlike traditional media, where editorial oversight acts as a filter, social media allows user-generated content to circulate with minimal verification. This creates an environment where deepfakes can thrive, particularly when they are sensational or emotionally provocative. Moreover, encrypted messaging services and private groups further complicate detection and regulation, as harmful content can be circulated beyond public scrutiny.[9]

2. Democratization of Deepfake Tools

Another key factor contributing to the widespread use of deepfake technology is its increasing accessibility. What was once limited to highly skilled programmers and researchers has now

[8] Ramamurthy Dhanyalakshmi and Gabriel Stoian, "A Survey on Face-Swapping Methods for Identity Manipulation in Deepfake Applications," 19 *IET Image Processing* (2025).
[9] M. S. Yessimova and T. V. Shevyakova, "Deep Fakes in the Digital Media Age: Opportunities and Threats.," 73 *Herald of Journalism / Habaršy Žurnalistika Seriâsy* (2024).

become available to ordinary users through user-friendly applications and open-source software. Advances in Machine Learning and cloud computing have simplified the technical requirements, enabling individuals with minimal expertise to create convincing deepfakes. Numerous applications and online platforms now offer pre-trained models, automated editing tools, and step-by-step interfaces, significantly lowering the barrier to entry. Users can generate manipulated content using basic devices such as smartphones or personal computers, often within minutes. This democratization of technology has both positive and negative implications. On one hand, it fosters creativity and innovation in digital media; on the other, it increases the risk of misuse, as individuals can exploit these tools for harassment, misinformation, or exploitation without requiring advanced technical knowledge. The combination of easy creation and rapid distribution has transformed deepfakes from a niche technological experiment into a widespread digital phenomenon. This accessibility underscores the urgent need for stronger regulatory frameworks and digital literacy to mitigate potential harms.[10]

4. Gendered Misuse of Deepfakes

4.1 Deepfake Pornography and Non-consensual Content

One of the most alarming aspects of deepfake technology is its overwhelming association with sexually explicit material. A significant proportion of deepfake content available online is pornographic in nature, created by digitally superimposing a person's face onto explicit videos or images without their consent. This form of manipulation is made possible through advanced techniques such as Generative Adversarial Networks, which enable the production of highly realistic and deceptive visuals. The scale of this problem has expanded rapidly with the availability of user-friendly tools and online platforms that host or distribute such content. Unlike traditional forms of image manipulation, deepfake pornography is particularly harmful because of its realism, which makes it difficult for viewers to distinguish between genuine and fabricated material. As a result, victims often face severe reputational damage, emotional distress, and long-term psychological harm.[11]

4.2 Targeting of Women: Celebrities and Private Individuals

[10] Dr. Arif Khan, "Deepfake Governance: Ai-generated Misinformation and the Future of Electoral Trust," 3 *Advance Social Science Archive Journal* 2208–2220 (2025).
[11] Thuy Dung Le and Nicola Döring, "Perspectives on Non-consensual Deepfake Pornography: A Content Analysis of Reddit Discussions Initiated by Perpetrators, Victims, and Bystanders" *Sexuality & Culture* 1–25 (2026).

Deepfake pornography disproportionately targets women, reflecting broader patterns of gender-based exploitation in digital spaces. Initially, high-profile figures such as actresses, influencers, and public personalities were the primary targets, as their images and videos were readily available online. However, the scope has expanded to include private individuals, whose photos are often taken from social media platforms like Instagram and Facebook without their knowledge or consent. This shift from public figures to ordinary women has intensified the severity of the issue, as private individuals typically lack the resources, visibility, or legal support to effectively respond. The misuse of personal images in explicit deepfakes constitutes a serious violation of privacy, dignity, and bodily autonomy. It also reinforces harmful stereotypes and perpetuates a culture of online harassment and misogyny. Furthermore, victims often encounter significant barriers when seeking legal remedies. Social stigma, fear of public exposure, and the slow pace of legal processes discourage reporting and accountability. The gendered nature of deepfake misuse thus highlights not only technological vulnerabilities but also deep-rooted societal inequalities that exacerbate the impact on women.[12]

4.3 Cyber Harassment and Online Abuse

1. Morphing and Image Manipulation

Morphing involves digitally altering images or videos to place a person's face onto another body or context, often without consent. With the advancement of Artificial Intelligence, such manipulation has become more realistic and easier to execute. In many cases, women's images are taken from social media and altered into objectionable or misleading content. This form of abuse not only invades privacy but also subjects victims to humiliation and unwanted public scrutiny.[13]

2. Revenge Porn and Non-consensual Dissemination

Revenge porn refers to the sharing of intimate images or videos without the consent of the individual, often with the intent to harass, intimidate, or seek retaliation. Deepfake technology has intensified this issue by enabling the creation of explicit content even where no original material exists. By using tools based on Generative Adversarial Networks, perpetrators can fabricate realistic intimate visuals, making it more difficult for victims to prove falsification

[12] Pragya Sharma and Payodhi Daschaudhuri, "Synthetic Faces, Real Disrepute: Deepfake and the Quest to Safeguard Celebrity Rights and Reputation," 2 *Journal of Legal Research and Polity* (2025).
[13] Akshay Agarwal and Nalini Ratha, "Chapter 8 - Manipulating faces for identity theft via morphing and deepfake: Digital privacy," in V. Govindaraju, A. S. R. S. Rao, *et al.* (eds.), *Deep Learning* 223–41 (Elsevier, 2023).

and defend their dignity.[14]

3. Impersonation and Identity Misuse

Deepfake technology facilitates impersonation by allowing individuals to mimic another person's appearance or voice convincingly. This can be used to create fake videos, audio clips, or messages that appear authentic. Such impersonation can damage personal and professional relationships, spread misinformation, or even lead to financial fraud. Women are particularly vulnerable, as impersonation is often used as a tool for harassment or character assassination.[15]

4. Psychological Harm

Victims of deepfake-based abuse often experience severe psychological distress, including anxiety, depression, fear, and a loss of sense of security. The inability to control or remove manipulated content from digital platforms can lead to a feeling of helplessness. The realistic nature of deepfakes intensifies emotional trauma, as victims struggle with the perception that others may believe the fabricated content to be real.[16]

5. Reputational Damage

Deepfake misuse can cause long-lasting harm to an individual's reputation. Once such content is circulated online, it can be difficult to completely erase, leading to continued judgment and social backlash. Victims may face consequences in their personal lives, careers, and social interactions, even when the content is proven to be fake.

6. Social Stigma and Isolation

In many cases, victims—especially women—face societal stigma and victim-blaming. Cultural attitudes may lead to the individual being judged rather than supported, resulting in social isolation. Fear of public exposure often discourages victims from reporting such incidents, thereby allowing perpetrators to evade accountability and perpetuating the cycle of online abuse.[17]

[14] Mattia Falduti and Sergio Tessaris, "Mapping the Interdisciplinary Research on Non-consensual Pornography: Technical and Quantitative Perspectives," 4 *Digital Threats: Research and Practice* (2023).
[15] Alisha Gilbert and Zhigang Gong, "Digital Identity Theft Using Deepfakes" *Information Technology Security and Risk Management* (CRC Press, 2024).
[16] Md. Zafar Sadique Gaurav Yadav, "Psychological Trauma and Legal Challenges of Deep fake Technology," 37 *Sciences of Conservation and Archaeology* 143–50 (2025).
[17] Mohammed, Fatima and Salam, A. F., "Towards a Theory of Digital Stigma and Deep Fake Video Technology Stigmatization in a Digitally Mediated Environment" (2022). *AMCIS 2022*

4.4 Societal Impact

1. Chilling Effect on Women's Online Participation

The growing misuse of deepfake technology has created a significant deterrent for women's active participation in digital spaces. The fear of being targeted through manipulated images, videos, or impersonation discourages many women from expressing themselves freely online. Platforms such as Instagram and Facebook, which are otherwise intended for communication and self-expression, can become spaces of vulnerability. This chilling effect manifests in various ways, including reduced engagement, self-censorship, and withdrawal from public discourse. Women may avoid sharing personal photos, opinions, or professional achievements due to the risk of misuse. As a result, their digital presence becomes limited, restricting opportunities for networking, career growth, and participation in social or political discussions. The threat of deepfake abuse thus undermines the inclusivity and openness that digital platforms are meant to promote.[18]

2. Reinforcement of Gender Inequality

Deepfake misuse not only reflects existing gender inequalities but also reinforces them in the digital environment. The disproportionate targeting of women, especially through sexually explicit or defamatory content, perpetuates harmful stereotypes and objectification. Technologies rooted in Artificial Intelligence, when misused, can amplify societal biases rather than eliminate them. Such practices contribute to a broader culture of online misogyny, where women are more likely to face harassment, scrutiny, and reputational harm. The normalization of such abuse further marginalizes women and discourages equal participation in digital and public life. Additionally, systemic barriers, such as lack of awareness, limited access to legal remedies, and social stigma make it harder for women to seek justice. Consequently, the societal impact of deepfake technology extends beyond individual harm, affecting gender equality, digital rights, and the overall integrity of online communities.[19]

5. Legal Framework in India

The rapid emergence of deepfake technology has posed significant challenges to India's

[18] Jeffrey T. Hancock and Jeremy N. Bailenson, "The Social Impact of Deepfakes," 24 *Cyberpsychology, Behavior, and Social Networking* (2021).
[19] Emily Chapman, "Unveiling the Threat- AI and Deepfakes' Impact on Women" *Departmental Honors & Graduate Capstone Projects* (2024).

existing legal system, particularly in addressing cybercrimes and protecting individual rights in the digital space. While there is no specific legislation exclusively dealing with deepfakes, various provisions under the Information Technology Act, 2000 and the Indian Penal Code are invoked to regulate related offences such as identity theft, obscenity, defamation, and online harassment. These laws provide a foundational framework for addressing misuse, yet they were enacted before the rise of advanced artificial intelligence technologies and therefore struggle to adequately capture the complexities of AI-generated content. The absence of a dedicated legal regime creates ambiguity in enforcement and often leads to fragmented remedies. Issues such as consent, authenticity, and accountability become difficult to resolve when dealing with highly realistic synthetic media. As a result, the Indian legal framework is increasingly being tested in its ability to respond effectively to the evolving threats posed by deepfake technology.

5.1 Constitutional Protections

1. Article 21: Right to Privacy, Dignity, and Reputation

The Constitution of India guarantees fundamental rights that form the backbone of individual protection against emerging digital harms, including those caused by deepfakes. Article 21 of the Constitution of India[20] ensures the right to life and personal liberty, which has been expansively interpreted by the judiciary to include the rights to privacy, dignity, and reputation. A landmark development in this context is the judgment in Justice K.S. Puttaswamy v. Union of India[21], where the Supreme Court explicitly recognized the right to privacy as a fundamental right. This includes informational privacy and the protection of one's personal identity in the digital sphere. Deepfake misuse, particularly in the form of non-consensual content, directly violates these constitutional guarantees by infringing upon an individual's autonomy, dignity, and control over personal data. Additionally, the right to reputation has been recognized as an integral part of Article 21, acknowledging that harm to one's public image can have serious personal and social consequences. Deepfakes, due to their realistic nature, can significantly damage an individual's reputation, thereby falling within the scope of constitutional protection.[22]

2. Judicial Expansion of Personality Rights

[20] The Constitution of India, art. 21
[21] (2017) 10 SCC 1
[22] Akanksha Singh Journal, "Deepfake Technology and Personality Rights: A Cyberlaw Analysis of Identity, Consent, And Constitutional Protection," 8 *IJLLR Journal* (2026).

Indian courts have also contributed to the development of personality rights, which protect an individual's identity, image, and likeness from unauthorized commercial or malicious use. Although not explicitly codified in statutes, these rights have evolved through judicial interpretation, drawing from constitutional principles and intellectual property doctrines. In cases such as R. Rajagopal v. State of Tamil Nadu[23], the Supreme Court emphasized the "right to be let alone," reinforcing the importance of privacy and control over personal information. Similarly, in ICC Development (International) Ltd. v. Arvee Enterprises[24], the court recognized the commercial aspect of personality rights, particularly in relation to publicity and endorsement. These judicial developments are highly relevant in the context of deepfakes, where an individual's face, voice, or identity may be used without consent. The unauthorized digital replication of a person's likeness can be seen as a violation of personality rights, especially when it results in exploitation, defamation, or financial gain. Thus, constitutional protections, combined with evolving judicial interpretations, provide an important—though still developing framework for addressing the challenges posed by deepfake technology.

5.2 Information Technology Act, 2000

1. Section 66E – Violation of Privacy

The Information Technology Act, 2000 provides important statutory safeguards against digital offences, including those arising from the misuse of deepfake technology. Section 66E of the Information Technology Act, 2000[25] specifically addresses the offence of capturing, publishing, or transmitting images of a person's private area without their consent. This provision is particularly relevant in cases involving deepfake pornography or manipulated intimate content, where an individual's image is used without authorization. Although Section 66E was not enacted with AI-generated content in mind, its scope can extend to deepfake misuse where privacy is clearly violated. The provision emphasizes consent as a central element, and any non-consensual creation or circulation of such content may attract liability. However, challenges remain in proving the origin of the content and identifying perpetrators, especially when deepfakes are created and shared anonymously.[26]

[23] 1994 SCC (6) 632
[24] 2003(26)PTC245(DEL)
[25] The Information Technology Act, 2000, Sec. 66E
[26] Rahul Kailas Bharati, "Violation of Privacy in Cyberspace (Section 66E of the IT Act, 2000)" *Handbook on the Information Technology Act, 2000: Offences, Penalties, and the Impact of New Criminal Laws.* (Deep Science Publishing, 2025).

2. Sections 67 and 67A – Obscene and Sexually Explicit Content

Section 67 and Section 67A of the Information Technology Act, 2000[27] deal with the publication or transmission of obscene and sexually explicit material in electronic form. Section 67 penalizes the dissemination of content that is lascivious or appeals to prurient interests, while Section 67A imposes stricter penalties for material that contains explicit sexual acts. These provisions are frequently invoked in cases involving deepfake pornography, as such content falls within the ambit of obscenity and sexually explicit material. Even if the content is artificially generated, its circulation can still cause real harm to individuals, particularly women, by damaging their dignity and reputation. However, the application of these sections to deepfakes is not without limitations. The law does not explicitly address synthetic or AI-generated media, which creates interpretational gaps. Additionally, enforcement is complicated by the speed of online dissemination and jurisdictional issues, especially when content is hosted on foreign platforms. Despite these challenges, Sections 67 and 67A remain key legal tools in addressing the circulation of harmful deepfake content in India.[28]

5.3 Bharatiya Nyaya Sanhita, 2023

1. Section 356 – Defamation

The BNS provides key provisions that can be applied to address harms caused by deepfake technology. Section 356 of the BNS[29] defines defamation as any false statement made with the intention to harm a person's reputation. Deepfake content, by creating fabricated yet realistic representations, can falsely portray individuals in compromising or misleading situations. Such portrayals can significantly damage personal and professional reputation, making this provision directly relevant in cases of deepfake misuse. Even though the content is artificially generated, the harm caused to reputation is real and actionable under this section.[30]

2. Section 79 – Word, Gesture or Act Intended to Insult the Modesty of a Woman

Section 79 of the BNS[31] specifically addresses acts intended to insult the modesty of a woman, including words, gestures, or acts that intrude upon her privacy. Deepfake pornography and

[27] The Information Technology Act, 2000, Sec. 66,67A
[28] Vanshika Kapoor, "Section 67 of Information Technology Act, 2000" *iPleaders*, 2024 *available at*: https://blog.ipleaders.in/section-67-of-information-technology-act-2000/ (last visited April 25, 2026).
[29] Bharatiya Nyaya Sanhita, 2023, Sec. 356
[30] Lisa Ward and Julia Day, "Defamation and social media law" *Research Handbook on Social Media and the Law* (Edward Elgar Publishing, 2025).
[31] Bharatiya Nyaya Sanhita, 2023, Sec. 79

manipulated explicit content fall squarely within the scope of this provision, as they often involve the non-consensual use of a woman's image in a sexually degrading manner. The creation and circulation of such content can be interpreted as an affront to dignity and modesty, making Section 509 a crucial legal tool in addressing gendered misuse of deepfakes.[32]

5.4. Intermediary Guidelines & IT Rules (2021, amended 2025)

1. Due Diligence Obligations on Platforms

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose significant responsibilities on intermediaries such as social media platforms, messaging services, and digital content hosts. These rules require platforms to exercise due diligence in monitoring and regulating user-generated content to prevent the circulation of unlawful material, including deepfakes. Intermediaries are obligated to publish clear policies, user agreements, and community guidelines that prohibit harmful or misleading content. They must also establish grievance redressal mechanisms, appoint grievance officers, and respond to user complaints within prescribed timelines. In cases involving non-consensual or explicit content, platforms are required to act promptly to remove or disable access once notified. Failure to comply with these obligations may result in the loss of safe harbour protection, thereby exposing platforms to legal liability.[33]

2. Mandatory Labelling and Takedown of AI-Generated Content

With the growing concerns surrounding synthetic media, recent amendments—often referred to as the 2025 updates—have emphasized greater accountability in dealing with AI-generated content. These developments require intermediaries to take reasonable steps toward identifying and, where feasible, labelling manipulated or synthetic media to inform users about its artificial nature. Additionally, platforms are expected to ensure swift takedown of content that violates legal provisions, particularly in cases involving deepfake pornography, impersonation, or misinformation. This includes proactive measures such as deploying automated detection tools and cooperating with law enforcement agencies. However, practical challenges persist. The detection of deepfakes remains technologically complex, and the vast volume of content uploaded daily makes comprehensive monitoring difficult. Moreover, balancing content

[32] Advocate Chikirsha Mohanty, "BNS Section 79 - Word, gesture or act intended to insult the modesty of a woman" *LawRato*, 2024 *available at*: https://lawrato.com/bharatiya-nyaya-sanhita/bns-section-79 (last visited April 25, 2026).
[33] Newsonair, "MeitY Notifies IT Rules Amendment 2025 to Strengthen Intermediary Due Diligence and Content Removal" *DD News On Air*, 23 October 2025.

regulation with freedom of expression raises concerns about potential over-censorship.[34]

5.5 Absence of Specific Deepfake Legislation

1. Reliance on Existing Fragmented Laws

Despite the growing misuse of deepfake technology, India does not yet have a dedicated legal framework specifically addressing synthetic media. Authorities currently rely on a combination of provisions under the Information Technology Act, 2000 and the Indian Penal Code to tackle offences such as obscenity, defamation, identity theft, and privacy violations. While these laws provide some degree of protection, they were enacted before the emergence of advanced AI technologies and therefore operate in a fragmented and indirect manner. This reliance on multiple statutes often leads to overlapping provisions, interpretational inconsistencies, and procedural delays. Victims may be required to invoke several legal provisions simultaneously, making the process complex and burdensome. Additionally, enforcement agencies may face difficulties in categorizing deepfake-related offences within traditional legal definitions, thereby weakening the effectiveness of legal remedies.[35]

2. Lack of Clear Definition and Criminalisation

A major gap in the current legal framework is the absence of a clear statutory definition of "deepfake" or "synthetic media." Without precise legal terminology, it becomes challenging to uniformly identify, regulate, and prosecute such content. The lack of explicit criminalisation also creates ambiguity regarding the scope of liability, particularly in distinguishing between malicious misuse and legitimate applications of the technology. Furthermore, key elements such as consent, intent, and harm are not specifically tailored to address AI-generated content. This results in uncertainty in legal proceedings and limits the ability of courts to respond effectively to evolving technological harms. The absence of targeted legislation thus highlights the urgent need for a comprehensive legal approach that directly addresses the unique characteristics and risks associated with deepfake technology.[36]

---

[34] VisionIAS, "Government notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026" *Current Affairs | Vision IAS*, 2026 *available at*: https://visionias.in/current-affairs/news-today/2026-02-11/science-and-technology/government-notif ied-the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-amendment-rules-2026 (last visited April 25, 2026).

[35] Record Of Law, "Regulation of Deepfake Technology: Can Existing Laws Cope" *Record Of Law*, 2026*available at*: https://recordoflaw.in/regulation-of-deepfake-technology-can-existing-laws-cope/ (last visited April 25, 2026).

[36] Datasecure, "Deep Fake Technology in India: Legal Framework for Misinformation and Image Rights" *Datasecure*, 2025 *available at*: https://datasecure.ind.in/blogs/deepfake-india/ (last visited April 25, 2026).

6. Judicial Responses and Case Laws

1. Anil Kapoor v. Simply Life India & Ors. (2023)

The decision in Anil Kapoor v. Simply Life India & Ors. (2023)[37] marks a significant judicial development in recognizing and protecting personality rights in the digital era. The case arose when the likeness, voice, and identity of Anil Kapoor were being misused across various online platforms, including through emerging technologies capable of replicating his image and persona without consent. The Delhi High Court acknowledged that a celebrity's personality including their name, image, voice, and distinctive attributes, constitutes a valuable and protectable right. The Court emphasized that unauthorized use of these elements, especially through technologies resembling deepfakes, amounts to a violation of personality rights and can lead to both reputational and commercial harm.[38]

Importantly, the Court recognized personality as a form of intellectual property-like right, capable of protection against misuse even in the absence of explicit statutory codification. It granted a broad injunction restraining unknown defendants ("John Doe") from using the actor's identity in any unauthorized manner, including through digital manipulation and AI-generated content. This judgment is particularly relevant in the context of deepfake misuse, as it establishes that the unauthorized digital replication of a person's likeness whether for commercial gain or otherwise can attract legal consequences. It also reflects the judiciary's proactive approach in adapting existing legal principles to address technological advancements, thereby strengthening the protection of individual identity in the digital space.[39]

2. Akshay Hari Om Bhatia vs John Doe and Ors[40]

In this case, the unauthorized use of Akshay Kumar's likeness through AI-generated deepfake content prompted judicial intervention by the Bombay High Court. The Court took cognizance of the serious implications of such misuse, particularly the potential harm to reputation, identity, and personal dignity. Recognizing the urgency of the situation, the Court directed the immediate takedown of the impugned content from digital platforms to prevent further circulation and damage. The case underscored that deepfake misuse violates the fundamental

[37] 2023 SCC OnLine Del 6914
[38] Ms. Savni D. Endlaw and Ms. Arushi Mann, "An Analytical Review of the Anil Kapoor Case: Balancing Fame and Privacy" *Saikrishnaassociatesavailable at*: https://www.saikrishnaassociates.c om/an-analytical-review-of-the-anil-kapoor-case-balancing-fame-and-privacy/.
[39] *Ibid.*
[40] 2025 SCC OnLine Bom 4044

rights guaranteed under Article 21 of the Constitution of India, including the rights to privacy, dignity, and reputation. Additionally, the Court acknowledged that the unauthorized replication of a person's image and persona may also attract protection under copyright law, especially where original content or performance is involved. This decision reflects the judiciary's willingness to extend constitutional and intellectual property protections to address the challenges posed by AI-generated content and reinforces the need for swift remedial measures in such cases.[41]

3. Ankur Warikoo v. John Doe[42]

In this case, the unauthorized use of the identity and likeness of Ankur Warikoo through AI-generated content led to concerns of impersonation and online fraud. The matter came before the Delhi High Court, which recognized the serious risks posed by such misuse, particularly in misleading the public and exploiting the credibility of well-known individuals. The Court granted interim relief by issuing directions to restrain unknown persons ("John Doe") from creating or circulating deepfake or AI-manipulated content that impersonates the plaintiff. It also ordered the removal and blocking of such content across digital platforms to prevent further harm. The decision highlights the judiciary's proactive approach in addressing AI-driven impersonation, acknowledging that such acts not only infringe personality rights but can also facilitate financial fraud and deception.[43]

6. Conclusion

Deepfake technology represents a complex intersection of innovation and risk, fundamentally altering how digital content is created and perceived. As highlighted throughout this paper, while the technology offers legitimate and creative applications, its misuse, particularly against women has emerged as a serious concern in India. The increasing accessibility of deepfake tools and the rapid spread of manipulated content through social media have intensified issues such as cyber harassment, non-consensual pornography, impersonation, and reputational harm. These developments not only violate individual rights but also reinforce existing gender

[41] The Hindu Bureau, "Actor Akshay Kumar seeks Bombay High Court's protection against deepfake misuse" *The Hindu*, 2025 *available at*: https://www.thehindu.com/news/cities/mumbai/actor-akshay-kumar-seeks-bombay-high-courts-protection-against-deepfake-misuse/article70168087.ece (last visited April 25, 2026).
[42] 2025 SCC OnLine Del 3727
[43] Arunima, "Delhi HC grants john doe injunction to Ankur Warikoo from Deepfake & AI Misuse" *SCC Times*, 2025 *available at*: https://www.scconline.com/blog/post/2025/05/29/delhi-high-court-ankur-warikoo-john-doe-injunction-deepfake-ai-misuse-legal-news/ (last visited April 25, 2026).

inequalities and discourage women's participation in digital spaces. The current legal framework in India, primarily based on the Information Technology Act, 2000, the Indian Penal Code, and constitutional protections under Article 21, provides some level of redressal. However, these laws were not designed to address the unique challenges posed by AI-generated content. As a result, enforcement remains fragmented, and victims often face procedural and evidentiary difficulties. The absence of a clear legal definition of deepfakes and the lack of specific criminal provisions further weaken the effectiveness of the existing framework.

Judicial responses have played a crucial role in bridging these gaps. Courts have increasingly recognized personality rights and extended protection against unauthorized use of an individual's identity, image, and voice. Cases involving public figures demonstrate a progressive approach toward granting injunctions, ordering takedowns, and acknowledging the broader implications of deepfake misuse. Additionally, recent directions for policy-level intervention indicate judicial awareness of the need for comprehensive regulation. Despite these developments, reliance on existing laws and judicial interpretation alone is insufficient. There is a pressing need for a dedicated legal framework that clearly defines deepfakes, establishes liability, and ensures timely remedies. Strengthening platform accountability, improving detection mechanisms, and promoting digital literacy are equally essential. Ultimately, addressing the challenges posed by deepfake technology requires a balanced approach that protects individual rights without hindering technological progress. A coordinated effort between lawmakers, courts, technology platforms, and society is necessary to ensure a safer and more equitable digital environment.

Bibliography

Books

1. Konstantin A. Pantserev, *The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability* Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity (Springer International Publishing, 2020).

2. Akshay Agarwal and Nalini Ratha, "Chapter 8 - Manipulating faces for identity theft via morphing and deepfake: Digital privacy," in *Deep Learning* (Elsevier, 2023).
3. Alisha Gilbert and Zhigang Gong, "Digital Identity Theft Using Deepfakes" *Information Technology Security and Risk Management* (CRC Press, 2024).
4. Rahul Kailas Bharati, "Violation of Privacy in Cyberspace (Section 66E of the IT Act, 2000)" *Handbook on the Information Technology Act, 2000* (Deep Science Publishing, 2025).
5. Lisa Ward and Julia Day, "Defamation and social media law" *Research Handbook on Social Media and the Law* (Edward Elgar Publishing, 2025).

Journals / Articles

1. Meenakshi Meenakshi, "Deepfake Technology and Legal Challenges in India: An Analysis" (2024) 3 *International Journal of Teaching, Learning and Education* 18–24.
2. Mika Westerlund, "The Emergence of Deepfake Technology: A Review" (2019) 9 *Technology Innovation Management Review*.
3. Yifei Wang, "Synthetic Realities in the Digital Age: Navigating the Opportunities and Challenges of AI-Generated Content" (2023) *TechRxiv*.
4. Meghana Lokhande and Prajot Raut, "Artificial Intelligence for Detecting Cyber Attacks in Deepfake & Identity Theft" (2024) *8th International Conference on Computing, Communication, Control and Automation (ICCUBEA)*.
5. Ramamurthy Dhanyalakshmi and Gabriel Stoian, "A Survey on Face-Swapping Methods for Identity Manipulation in Deepfake Applications" (2025) 19 *IET Image Processing*.
6. M. S. Yessimova and T. V. Shevyakova, "Deep Fakes in the Digital Media Age: Opportunities and Threats" (2024) 73 *Herald of Journalism*.
7. Dr. Arif Khan, "Deepfake Governance: AI-Generated Misinformation and the Future of Electoral Trust" (2025) 3 *Advance Social Science Archive Journal* 2208–2220.
8. Thuy Dung Le and Nicola Döring, "Perspectives on Non-consensual Deepfake Pornography: A Content Analysis of Reddit Discussions Initiated by Perpetrators, Victims, and Bystanders" (2026) *Sexuality & Culture* 1–25.
9. Pragya Sharma and Payodhi Daschaudhuri, "Synthetic Faces, Real Disrepute: Deepfake and the Quest to Safeguard Celebrity Rights and Reputation" (2025) 2 *Journal of Legal Research and Polity*.

10. Mattia Falduti and Sergio Tessaris, "Mapping the Interdisciplinary Research on Non-consensual Pornography: Technical and Quantitative Perspectives" (2023) 4 *Digital Threats: Research and Practice*.
11. Md. Zafar Sadique and Gaurav Yadav, "Psychological Trauma and Legal Challenges of Deepfake Technology" (2025) 37 *Sciences of Conservation and Archaeology* 143–150.
12. Mohammed, Fatima and Salam, A. F., "Towards a Theory of Digital Stigma and Deep Fake Video Technology Stigmatization in a Digitally Mediated Environment" (2022) *AMCIS Conference Proceedings*.
13. Jeffrey T. Hancock and Jeremy N. Bailenson, "The Social Impact of Deepfakes" (2021) 24 *Cyberpsychology, Behavior, and Social Networking*.
14. Emily Chapman, "Unveiling the Threat: AI and Deepfakes' Impact on Women" (2024) *Departmental Honors & Graduate Capstone Projects*.
15. Akanksha Singh, "Deepfake Technology and Personality Rights: A Cyberlaw Analysis of Identity, Consent, and Constitutional Protection" (2026) 8 *IJLLR Journal*.

Websites

1. Vanshika Kapoor, "Section 67 of Information Technology Act, 2000," *iPleaders* (2024)
2. Advocate Chikirsha Mohanty, "BNS Section 79 - Word, gesture or act intended to insult the modesty of a woman," *LawRato* (2024)
3. "MeitY Notifies IT Rules Amendment 2025 to Strengthen Intermediary Due Diligence and Content Removal," *DD News (Newsonair)* (23 October 2025).
4. "Government notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026," *VisionIAS* (2026)
5. "Regulation of Deepfake Technology: Can Existing Laws Cope," *Record Of Law* (2026)
6. "Deep Fake Technology in India: Legal Framework for Misinformation and Image Rights," *Datasecure* (2025)
7. Ms. Savni D. Endlaw and Ms. Arushi Mann, "An Analytical Review of the Anil Kapoor Case: Balancing Fame and Privacy," *Saikrishna & Associates*
8. The Hindu Bureau, "Actor Akshay Kumar seeks Bombay High Court's protection against deepfake misuse," *The Hindu* (2025)

9. Arunima, "Delhi HC grants John Doe injunction to Ankur Warikoo from Deepfake & AI Misuse," *SCC Times* (2025)

Details:

Guide: Ms. Gayatri

Student: Ms. Sakshi

Mobile no.: 9992273470

Email: sakshis7192@gmail.com

Address: Kalka, District Panchkula, Haryana

College Address: Rayat Bahra University, Mohali, Punjab 140104, India