

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

DEEPFAKES AND MISAPPROPRIATION OF IDENTITY: LEGAL REMEDIES AND CHALLENGES

AUTHORED BY - SONAM¹

Abstract:

The emergence of deepfake technology, driven by rapid advancements in artificial intelligence, has created unprecedented challenges for the protection of identity and personal rights in the digital era. Deepfakes refer to hyper-realistic manipulated audio, video, or images that falsely depict individuals engaging in acts they never performed. While this technology has legitimate applications in entertainment, education, and innovation, its misuse has led to serious concerns such as identity misappropriation, defamation, privacy violations, cyber harassment, and financial fraud. This paper examines the legal implications of deepfakes with a particular focus on the misappropriation of identity. It analyses how existing legal frameworks, especially in India, address such issues through provisions under information technology law, criminal law, and data protection principles. The study also explores relevant global approaches, including regulatory developments in jurisdictions such as the United States and the European Union, to highlight comparative perspectives. Despite the availability of certain legal remedies, the paper identifies significant challenges, including the absence of specific legislation on deepfakes, difficulties in detection and attribution, jurisdictional complexities, and the rapid evolution of AI technologies outpacing legal responses. Furthermore, enforcement mechanisms often remain inadequate due to technical and procedural limitations.

The paper concludes by emphasizing the urgent need for a comprehensive legal framework, incorporating technological safeguards, stricter liability norms, and international cooperation. Strengthening awareness and digital literacy is also essential to mitigate the risks associated with deepfakes and ensure effective protection of individual identity rights in the digital age.

Keywords: Deepfakes; Identity Misappropriation; Privacy Rights; Cyber Law; Artificial Intelligence.

¹ Research Scholar, Department of Laws, Panjab University, Chandigarh.

1. Introduction

Deepfake technology, driven by rapid advancements in artificial intelligence (AI)² and machine learning, particularly through the use of Generative Adversarial Networks (GANs), has significantly transformed the nature of digital content creation. These technologies enable the generation of highly realistic but entirely fabricated audio, video, and image content, often making it nearly impossible for an average viewer to distinguish between authentic and manipulated material.³ While deepfakes have legitimate applications in fields such as entertainment, cinema, education, and virtual reality, their misuse has emerged as a serious concern, especially in relation to identity theft, financial fraud, defamation, and violations of privacy. The ability to replicate an individual's face, voice, and personality without consent creates unprecedented risks in the digital era.⁴

In India, the risks associated with deepfake technology are particularly pronounced due to the country's rapidly expanding digital ecosystem. With increasing internet penetration, widespread use of smartphones, and the growth of digital payment systems, India has become highly susceptible to cyber-enabled crimes. Deepfakes have already begun to be used in fraudulent schemes such as voice cloning scams, where perpetrators impersonate trusted individuals to deceive victims into transferring money or disclosing sensitive information. Similarly, manipulated videos and images are used to spread misinformation, damage reputations, or exploit individuals through non-consensual content. The scale and speed at which such content can be disseminated through social media platforms amplify the harm caused to victims.⁵

The misuse of deepfake technology raises serious concerns regarding the protection of fundamental rights, particularly the right to privacy, dignity, and reputation under Article 21 of the Indian Constitution. The landmark judgment in Justice **K.S. Puttaswamy v. Union of India**⁶ recognized the right to privacy as a fundamental right, including informational privacy and control over personal data. Deepfakes directly violate this principle by enabling unauthorized use and manipulation of an individual's identity, thereby undermining personal autonomy and

² Jones, Valencia A. *Artificial intelligence enabled deepfake technology: The emergence of a new threat*. Utica College, 2020.

³ Mohammed, Anwar. "Deep Fake Detection and Mitigation: Securing Against AI-Generated Manipulation." *Journal of Computational Innovation* 4.1 (2024).

⁴ Kılıç, Büşra, and Mehmet Emin Kahraman. "Current usage areas of deepfake applications with artificial intelligence technology." *İletişim ve Toplum Araştırmaları Dergisi* 3.2 (2023): 301-332.

⁵ Panwar, Kuldeep Singh, and Nilutpal Deb Roy. "Rising menace of deepfakes with the help of AI: Legal implications in India." *Indian Journal of Integrated Research in Law Volume IV Issue III* | ISSN 2583 (2024): 0538.

⁶ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India)

consent. The technological capability to fabricate realistic representations of individuals without their knowledge or approval poses a direct challenge to constitutional protections.⁷

Indian courts have increasingly begun to address issues arising from deepfake-related misuse, even in the absence of a dedicated statutory framework. In *Ankur Warikoo v. John Doe*⁸, the Delhi High Court granted a John Doe injunction against unknown persons who had created and circulated deepfake videos using the plaintiff's likeness for fraudulent purposes. The Court acknowledged the potential of such content to mislead the public and cause financial and reputational harm, thereby recognizing deepfake-based impersonation as a serious legal issue. This case marked an important step in extending existing legal remedies to emerging technological threats.

Similarly, in *Gaurav Bhatia v. Naveen Kumar & Ors.*⁹, the Court restrained the circulation of defamatory deepfake videos, emphasizing that manipulated digital content can cause irreparable harm to an individual's reputation. The decision reinforced the importance of protecting personality rights and highlighted the judiciary's willingness to intervene in cases involving digital impersonation and misinformation. Such judicial responses indicate a growing recognition of the unique challenges posed by deepfake technology.

The courts have also shown sensitivity towards the protection of celebrity rights in the digital space. In cases involving public figures such as Anil Kapoor, Indian courts have granted injunctions against the unauthorized use of their name, image, or voice through AI-generated content. These decisions underscore the concept of personality rights, which safeguard an individual's commercial and reputational interests against unauthorized exploitation. The misuse of celebrity identities through deepfakes not only leads to economic loss but also erodes public trust in digital media.

Recent incidents further highlight the growing prevalence of deepfake-related offences in India. The misuse of the identity of Gautam Gambhir through AI-generated content demonstrates how even prominent public figures are not immune to such technological manipulation. Such cases illustrate the evolving nature of cybercrime and the increasing sophistication of tools used by offenders. They also emphasize the urgent need for effective legal mechanisms to address these challenges.

Despite these developments, India currently lacks a comprehensive legal framework specifically designed to regulate deepfake technology. Existing laws, such as the Information

⁷ Chopra, Aahana, and Ms Ananya Shukla. "Exploring the Misuse of Deepfake Technology in India: Implications for Society." (2024).

⁸ *Ankur Warikoo v. John Doe*, Delhi High Court, 2023.

⁹ *Gaurav Bhatia v. Naveen Kumar & Ors.*, Delhi High Court, 2023.

Technology Act, 2000, and provisions relating to cheating, defamation, and obscenity, are applied in a fragmented manner to address deepfake-related offences. However, these laws were not originally designed to deal with the complexities of AI-generated content, leading to gaps in enforcement and interpretation.¹⁰

Therefore, the rise of deepfake technology presents a complex intersection of law, technology, and ethics. It challenges traditional legal concepts of identity, consent, and accountability, while exposing the limitations of existing regulatory frameworks. In this context, there is an urgent need to critically examine the adequacy of current legal remedies and identify regulatory gaps, so as to develop a robust and forward-looking legal regime capable of effectively addressing deepfake-driven identity theft in India.¹¹

2. Concept of Deepfakes and Identity Theft

Deepfake technology refers to the use of artificial intelligence, particularly deep learning techniques, to create manipulated audio-visual content that convincingly imitates real individuals. By training algorithms on extensive datasets of images, videos, and voice recordings, it becomes possible to replicate a person's facial expressions, voice patterns, and overall appearance with remarkable accuracy. As a result, deepfakes blur the distinction between reality and fabrication, making it increasingly difficult to verify the authenticity of digital content. When such technology is used without consent to manipulate a person's likeness—whether face, voice, or identity—it raises serious legal, ethical, and social concerns.¹²

At its core, a deepfake involves the unauthorized appropriation of an individual's identity. Identity is not limited to visible physical traits but includes voice, expressions, and other unique personal characteristics. The misuse of these attributes through deepfake technology constitutes a violation of personal autonomy, dignity, and informational privacy. When such manipulation is carried out with the intent to deceive, defraud, or harm an individual, it falls within the scope of identity theft.¹³

¹⁰ Chakrabarty, Shambhu Prasad, and Shrabana Chattopadhyay. "Criminal Liability of Artificial Intelligence-Generated Deepfakes in India." *International Ethical Hacking Conference*. Singapore: Springer Nature Singapore, 2024.

¹¹ Meenakshi, Meenakshi. "Deepfake Technology and Legal Challenges in India: An Analysis." *International Journal of Teaching, Learning and Education* 3.2: 18-24.

¹² Chopra, Aahana, and Ms Ananya Shukla. "Exploring the Misuse of Deepfake Technology in India: Implications for Society." (2024).

¹³ Panda, Biranchi Naryan P., and Isha Sharma. "Deepfake Technology in India and World: Foreboding and Forbidding." *Law and Humanities Quarterly Reviews* 4.3 (2025): 18-28.

Identity theft, in legal terms, refers to the fraudulent use of another person's identifying information without consent. In India, this offence is specifically recognized under Section 66C of the Information Technology Act, 2000, which penalizes the dishonest or fraudulent use of electronic signatures, passwords, or any other unique identification feature. Deepfake technology significantly expands the scope of identity theft by enabling offenders to replicate not just static identifiers such as passwords or IDs, but dynamic human traits like voice and facial expressions. This makes impersonation far more convincing and dangerous.

¹⁴Deepfakes can be misused in multiple ways, each posing distinct legal challenges. One of the most prominent uses is financial fraud, especially through voice cloning scams. Criminals can create AI-generated voice replicas of trusted individuals—such as employers, family members, or company executives—and use them to manipulate victims into transferring money or disclosing sensitive information. Due to the realistic nature of such voice simulations, victims often fail to detect the fraud until it is too late.

Another serious misuse is political misinformation. Deepfakes can fabricate speeches or videos of political leaders, potentially influencing public opinion and disrupting democratic processes. In a country like India, where elections and public discourse play a crucial role, such manipulation can undermine the integrity of democratic institutions and spread large-scale misinformation.

Deepfakes have also emerged as a major tool for non-consensual pornography, which disproportionately affects women. In such cases, an individual's face is superimposed onto explicit content without their consent, leading to severe violations of privacy and dignity. A widely reported incident involved Rashmika Mandanna, whose face was morphed into a viral deepfake video that spread rapidly across social media platforms. The incident sparked nationwide outrage and drew attention from government authorities, highlighting the vulnerability of even public figures to such exploitation. It also demonstrated how easily deepfake content can be created and disseminated, causing irreversible reputational and emotional harm.

Similarly, instances involving celebrities such as Alia Bhatt and Katrina Kaif have surfaced, where manipulated images or videos circulated online, raising concerns about privacy and digital safety. These incidents underscore the broader societal risk, as if well-known personalities can be targeted, ordinary individuals with fewer resources for legal recourse are even more vulnerable.

¹⁴ Asawat, Vikas. "Information technology (Amendment) act, 2008: A new vision through a new change." *Available at SSRN 1680152* (2010).

In addition to exploitation and fraud, deepfakes are frequently used for defamation and reputational harm. Fabricated content can depict individuals in false or compromising situations, leading to social stigma, professional consequences, and psychological distress. The speed at which such content spreads online further aggravates the damage, often making it difficult to contain or reverse.

Judicial developments have reinforced the recognition of identity and personality rights in this context. In Justice *K.S. Puttaswamy v. Union of India*,¹⁵ the Supreme Court affirmed that individuals have a fundamental right to control their personal data and identity. Deepfakes directly undermine this principle by enabling unauthorized manipulation and dissemination of personal attributes.

In conclusion, deepfakes represent an advanced and evolving form of identity theft, where artificial intelligence enhances the ability to impersonate individuals with alarming precision. The combination of technological sophistication and malicious intent has expanded the traditional boundaries of identity theft, making it more complex and harmful. Real-life incidents involving public figures clearly illustrate the seriousness of the issue and highlight the urgent need for stronger legal and regulatory mechanisms to address the challenges posed by deepfake technology in India.

2. Concept of Deepfakes and Identity Theft

Deepfake technology refers to the use of artificial intelligence to create manipulated audio, video, or images that realistically imitate a person's identity. By using deep learning techniques, especially Generative Adversarial Networks (GANs), individuals' faces, voices, and expressions can be replicated with high precision. This makes it difficult to distinguish between real and fabricated content. When such technology is used without consent, it leads to serious violations of privacy, dignity, and identity.¹⁶

At its core, a deepfake involves the unauthorized use of a person's likeness. Identity is not limited to name or identification numbers but includes facial features, voice, and behavioral traits. When these are misused to deceive others, it amounts to identity theft. In India, identity theft is legally recognized under Section 66C of the Information Technology Act, 2000, which penalizes the fraudulent use of another person's unique identification features. Deepfakes expand this concept by enabling highly convincing impersonation, making fraud and deception

¹⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

¹⁶ Saxena, Divya, and Jiannong Cao. "Generative adversarial networks (GANs) challenges, solutions, and future directions." *ACM Computing Surveys (CSUR)* 54.3 (2021): 1-42.

more effective.¹⁷

Deepfakes are used in various harmful ways, including:

- **Financial Fraud (Voice Cloning Scams):**

Criminals use AI-generated voices to impersonate trusted individuals such as company executives or relatives. Victims are tricked into transferring money or sharing confidential information, believing the request to be genuine.

- **Political Misinformation:**

Deepfake videos can show political leaders making false statements or speeches. Such content can mislead the public, influence elections, and disturb democratic processes.

- **Non-Consensual Pornography:**

This is one of the most serious misuses of deepfake technology. A notable example is Rashmika Mandanna, whose face was morphed into a viral video without consent. The incident highlighted how deepfakes can violate dignity and cause emotional and reputational harm.¹⁸

- **Defamation and Reputational Harm:**

Deepfake content can falsely depict individuals in compromising situations. Celebrities like Alia Bhatt have also faced manipulated content online, showing how such technology can damage reputation and public image.

These examples demonstrate that deepfakes are not merely technological tools but instruments of potential harm. They enable offenders to exploit identities in ways that were previously difficult or impossible.

From a legal perspective, the misuse of deepfakes also violates the right to privacy recognized in Justice *K.S. Puttaswamy v. Union of India*¹⁹, where the Supreme Court affirmed that individuals have control over their personal data and identity.

In conclusion, deepfakes represent a modern and sophisticated form of identity theft. By combining artificial intelligence with malicious intent, they pose significant threats to individuals and society. Understanding their concept and misuse is essential for developing effective legal responses in India.

¹⁷ Pan, Zhaoqing, et al. "Recent progress on generative adversarial networks (GANs): A survey." *IEEE access* 7 (2019): 36322-36333.

¹⁸ De Angeli, Antonella, et al. "Reporting non-consensual pornography: clarity, efficiency and distress." *Multimedia Tools and Applications* 82.9 (2023): 12829-12858.

¹⁹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

3. Legal Framework Governing Deepfakes in India

The regulation of deepfake technology in India is currently governed through a combination of existing cyber laws, criminal statutes, and data protection frameworks. Although there is no specific legislation exclusively addressing deepfakes, various legal provisions are applied analogically to deal²⁰ with offences arising from their misuse. This fragmented approach reflects both the adaptability and the limitations of the Indian legal system in responding to emerging technological challenges.

3.1 Information Technology Act, 2000²¹

The Information Technology Act, 2000 serves as the primary legislation governing cyber offences in India and plays a crucial role in addressing deepfake-related crimes. Several provisions of the Act are particularly relevant:

- **Section 66C – Identity Theft:**

This provision penalizes the fraudulent use of another person's electronic signature, password, or unique identification feature. Deepfakes that replicate a person's face or voice for impersonation can fall within its ambit.

- **Section 66D – Cheating by Personation:**

It criminalizes impersonation using computer resources. Deepfake videos or voice clones used to deceive individuals for financial gain clearly attract liability under this section.

- **Section 66E – Violation of Privacy:**

This section addresses the unauthorized capturing, publishing, or transmission of private images. Deepfake content involving manipulated personal visuals may constitute a violation of privacy.

- **Sections 67 & 67A – Obscene Content Transmission:**

These provisions deal with publishing or transmitting obscene or sexually explicit content. They are particularly relevant in cases of deepfake pornography.

- **Section 69A – Blocking of Unlawful Content:**

This empowers the government to block public access to unlawful online content, including harmful deepfake material.

²⁰ Vig, Shinu. "Regulating Deepfakes." *Journal of Strategic Security* 17.3 (2024): 70-93.

²¹ Iyer¹, Malathi Sundaram, et al. "Critical Analysis of the Information Technology Act 2000, Its Amendments, and the Emerging Digital Personal Data Protection Act 2023 in the Context of Global Regulatory Benchmarks." *Evolution* 3.3 (2026).

- **Section 79 – Intermediary Liability:**

This section provides conditional immunity to intermediaries such as social media platforms, provided they exercise due diligence and comply with takedown requirements.

Although the Act does not explicitly refer to deepfakes, courts and enforcement agencies have interpreted these provisions broadly to cover AI-generated content, thereby ensuring some level of accountability.

3.2 Bharatiya Nyaya Sanhita, 2023 (BNS)

In addition to cyber laws, traditional criminal law provisions under the **Bharatiya Nyaya Sanhita, 2023** are also applicable to offences arising from deepfake technology. Although the BNS does not explicitly mention artificial intelligence or deepfakes, several of its provisions relating to cheating, defamation, obscenity, and privacy can be effectively invoked. These provisions demonstrate that even in the absence of specific legislation, general criminal law continues to provide remedies against deepfake misuse.

Defamation – Section 356 BNS:

Deepfake content that falsely portrays an individual in a negative or compromising manner may attract criminal liability under Section 356 (Defamation) of the BNS (earlier Section 499 IPC). Since deepfakes create highly realistic fabricated content, they can cause severe reputational harm. The evidentiary value of video and audio makes such defamation more damaging than traditional forms, as the public is more likely to believe visual representations.

Cheating and Personation – Sections 318 & 319 BNS:

Where deepfakes are used to deceive individuals for wrongful gain, provisions relating to cheating become applicable. Section 318 (Cheating) covers acts involving deception leading to wrongful loss or gain, while Section 319 (Cheating by Personation) specifically applies when a person is impersonated using digital means such as AI-generated videos or voice cloning. For instance, deepfake technology can be used to impersonate company officials or relatives to fraudulently obtain money, making these provisions highly relevant in cyber fraud cases.

Obscenity and Sexual Exploitation – Section 294 BNS:

The creation or circulation of sexually explicit deepfake content without consent may be punishable under Section 294 (Obscene Acts and Songs) and other related provisions dealing with obscenity. Deepfake pornography, which involves morphing a person's face onto explicit content, is a serious violation of dignity and can lead to criminal liability. Such acts are

particularly harmful as they disproportionately target women and cause long-term psychological and social consequences.

Voyeurism – Section 75 BNS:

Deepfake content simulating private or intimate acts without consent may fall under provisions relating to voyeurism and invasion of privacy. Even though the content is artificially created, it represents a violation of personal dignity and autonomy, making it punishable under the law.

Forgery and Fabrication of Evidence – Sections 336 & 340 BNS:

Deepfakes may also be used to create false digital evidence, such as fabricated video or audio recordings. Section 336 (Forgery) and Section 340 (Using forged documents or electronic records as genuine) apply where such manipulated content is used to mislead courts, authorities, or individuals. This misuse poses a serious threat to the integrity of the justice system, as it undermines the reliability of digital evidence.

In conclusion, the Bharatiya Nyaya Sanhita, 2023 provides a broad and adaptable framework to address offences arising from deepfake misuse through provisions on defamation, cheating, obscenity, and forgery. However, the absence of explicit references to AI-generated content necessitates interpretative application by courts, highlighting the urgent need for specific legislation targeting deepfakes and synthetic media.

3.3 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 represents a significant step toward regulating the processing of personal data in India. Deepfake technology often relies on the unauthorized collection and use of personal data such as images, videos, and voice samples.

Under this Act:

- Individuals (data principals) have rights over their personal data.
- Consent is required for data processing.
- Unauthorized use or manipulation of personal data can attract penalties.

However, challenges remain in enforcement, particularly in identifying offenders and regulating cross-border data misuse. The Act does not directly address deepfakes, but its principles of consent and data protection are highly relevant.

3.4 IT Rules, 2021 (Amended 2025)

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, along with subsequent amendments, impose obligations on intermediaries to regulate online content more effectively.

Recent developments include:

- **Mandatory Labeling of AI-Generated Content:**
Platforms are encouraged or required to identify and label synthetic or manipulated media.
- **Faster Takedown Mechanisms:**
Harmful content, including deepfakes, must be removed within a specified timeframe (generally 24–36 hours upon notice).
- **Enhanced Due Diligence by Intermediaries:**
Social media platforms are required to act responsibly, appoint grievance officers, and ensure compliance with legal directives.

These rules aim to create a safer digital environment by placing greater accountability on intermediaries, who play a key role in the dissemination of deepfake content.

Real-Life Incidents of Deepfake Misuse

The growing accessibility of artificial intelligence tools has led to a significant rise in real-life incidents involving deepfake technology. These incidents highlight the serious risks posed by deepfakes in terms of identity misappropriation, privacy violations, reputational harm, financial fraud, and threats to democratic processes. Unlike theoretical concerns, these real-world cases demonstrate how deepfakes have already begun to impact individuals and society at large, making it imperative to address them through effective legal and regulatory mechanisms.

One of the most widely discussed incidents in India is the deepfake video involving Rashmika Mandanna. In 2023, a manipulated video surfaced online in which her face was superimposed onto another individual's body using AI technology. The video quickly went viral on social media platforms, raising serious concerns about consent, privacy, and digital safety. Although the video was later identified as fake, the damage to dignity and public perception had already occurred. This incident sparked nationwide debate and prompted government authorities to consider stricter regulations on deepfake content.

Another category of real-life misuse involves deepfake pornography, which has disproportionately targeted women across the globe. In such cases, the faces of individuals—often celebrities or private persons—are morphed onto explicit content without their consent. Victims of such crimes suffer immense psychological trauma, social stigma, and reputational harm. The anonymity of the internet and the rapid spread of such content make it extremely difficult to control or remove once it has been uploaded. These incidents highlight the gendered nature of deepfake abuse and the urgent need for stronger protective mechanisms.

Deepfake technology has also been increasingly used in financial fraud and cybercrime. There have been reported cases where scammers used AI-generated voice cloning to impersonate company executives or family members. In one notable instance, fraudsters mimicked the voice of a corporate executive to instruct an employee to transfer large sums of money, resulting in significant financial loss. Such cases demonstrate how deepfakes can enhance traditional cyber fraud techniques by making them more convincing and harder to detect.

In the political sphere, deepfakes pose a serious threat to democratic integrity and public trust. Manipulated videos of politicians have been circulated to spread misinformation, influence public opinion, and disrupt electoral processes. These videos can portray leaders making statements they never actually made, thereby misleading voters and undermining confidence in democratic institutions. Given the visual realism of deepfakes, it becomes increasingly difficult for the general public to distinguish between authentic and fabricated content, leading to the phenomenon often referred to as “information disorder.”

Another concerning trend is the use of deepfakes for defamation and personal vendetta. Individuals have used AI tools to create false videos or audio clips of others to settle personal disputes or damage reputations. In some cases, students, professionals, and even private citizens have been targeted, showing that deepfake misuse is no longer limited to celebrities or public figures. The widespread availability of deepfake applications has democratized the ability to create such content, increasing the risk of misuse at all levels of society.

Additionally, deepfakes have raised concerns in the context of national security and public order. Fabricated videos of military officials or government authorities could potentially be used to spread panic, incite violence, or manipulate public perception during sensitive situations. The potential misuse of deepfakes in warfare or propaganda further underscores the seriousness of this issue on a global scale.

In conclusion, real-life incidents of deepfake misuse clearly demonstrate that this technology is not merely a futuristic threat but a present and growing challenge. From celebrity harassment and gender-based abuse to financial fraud and political manipulation, deepfakes have far-reaching consequences that affect individuals, institutions, and society as a whole. These incidents underscore the urgent need for robust legal frameworks, technological safeguards, and public awareness to mitigate the risks associated with deepfake technology.

Constitutional Perspective

The rapid emergence of deepfake technology has raised complex constitutional questions in India, particularly concerning the protection of fundamental rights under Part III of the

Constitution. Deepfakes, by enabling unauthorized manipulation of a person's identity, directly affect core constitutional values such as privacy, dignity, reputation, and freedom of expression. The constitutional framework thus plays a crucial role in evaluating both the harms caused by deepfakes and the limits of permissible regulation.

At the heart of this discussion lies Article 21 of the Constitution of India, which guarantees the right to life and personal liberty. The scope of Article 21 has been expansively interpreted by the Supreme Court to include the right to privacy, as recognized in the landmark judgment of *Justice K.S. Puttaswamy v. Union of India (2017)*. The Court held that privacy includes informational control, bodily autonomy, and the right to be left alone. Deepfake technology directly violates these principles by allowing the unauthorized use of an individual's face, voice, and identity to create fabricated content. Such misuse strips individuals of control over their personal identity and representation, thereby infringing their autonomy and dignity.

Closely linked with privacy is the right to reputation, which has also been recognized as an integral part of Article 21. The Supreme Court has consistently held that reputation is a valuable asset and an essential component of a dignified life. Deepfakes, especially those portraying individuals in false or compromising situations, can cause irreparable harm to reputation. Unlike traditional defamation, deepfakes are more persuasive because of their visual realism, making it difficult for victims to disprove the fabricated content. This amplifies the constitutional injury and necessitates stronger legal safeguards.

Another significant constitutional dimension is the right to freedom of speech and expression under Article 19(1)(a). At first glance, the creation and dissemination of deepfake content may appear to fall within the ambit of free speech. However, this right is not absolute and is subject to reasonable restrictions under Article 19(2), including defamation, public order, decency, morality, and incitement to an offence. Deepfake content that spreads misinformation, damages reputation, or incites harm clearly falls within these restricted categories. Therefore, the misuse of deepfake technology cannot be justified as an exercise of free speech.

The constitutional challenge lies in maintaining a balance between innovation and regulation. Excessive restrictions on deepfake technology may stifle creativity, technological development, and legitimate uses such as satire, parody, or artistic expression. On the other hand, insufficient regulation may lead to widespread abuse, erosion of trust in digital media, and violation of fundamental rights. Courts must therefore adopt a proportionality-based approach, ensuring that restrictions on deepfakes are reasonable, necessary, and narrowly tailored to achieve legitimate objectives.

In addition to privacy and free speech, Indian jurisprudence has also begun to recognize

personality rights, which protect an individual's name, image, voice, and likeness from unauthorized use. In cases such as *Anil Kapoor v. Simply Life India (2023²²)* and *Amitabh Bachchan Personality Rights Case (2022²³)*, the courts acknowledged that individuals have a right to control the commercial and public use of their identity. Deepfake technology directly infringes these rights by replicating a person's likeness without consent, often for profit or malicious purposes.

Furthermore, deepfakes pose a threat to constitutional democracy by enabling the spread of misinformation and manipulation of public opinion. Fabricated videos of political leaders can influence electoral outcomes, undermine free and fair elections, and disrupt public order. Such misuse indirectly affects the basic structure of the Constitution, which includes democracy and the rule of law.

In conclusion, deepfake technology presents a serious constitutional challenge by intersecting with multiple fundamental rights. While the Constitution provides a robust framework for protecting individual liberties, the evolving nature of AI requires dynamic judicial interpretation and proactive legislative measures. A careful balance must be struck to ensure that technological innovation does not come at the cost of privacy, dignity, and democratic integrity.

Judicial Precedents

The issue of deepfakes and identity misappropriation, though relatively recent, finds its legal grounding in a series of judicial precedents delivered by Indian courts. While there is no direct Supreme Court ruling specifically on deepfakes, courts have developed a strong jurisprudential framework through cases dealing with privacy, reputation, free speech, and personality rights. These principles are highly relevant in addressing the legal challenges posed by deepfake technology.

One of the most significant judgments in this context is Justice *K.S. Puttaswamy v. Union of India (2017²⁴)*, where the Supreme Court recognized the right to privacy as a fundamental right under Article 21. The Court held that individuals have the right to control their personal information and identity. This judgment laid the constitutional foundation for challenging deepfakes, as the unauthorized use of a person's face, voice, or likeness directly violates informational privacy and personal autonomy. Deepfakes, by creating fabricated

²² *Anil Kapoor v. Simply Life India & Ors.*, Delhi High Court, 2023.

²³ *Amitabh Bachchan v. Rajat Nagi & Ors.*, Delhi High Court, 2022.

²⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

representations of individuals, clearly infringe upon this right.

Another important precedent is *Shreya Singhal v. Union of India (2015)*²⁵, where the Supreme Court struck down Section 66A of the IT Act for being unconstitutional. The Court emphasized the importance of freedom of speech and expression under Article 19(1)(a) while also recognizing that reasonable restrictions under Article 19(2) must be narrowly tailored. This case is relevant in the deepfake context because it highlights the need to balance free speech with the prevention of harmful and misleading content. While deepfakes may sometimes be defended as expression, their misuse for defamation or misinformation falls outside constitutional protection.

The judiciary has also significantly contributed to the recognition of personality rights, which are central to addressing deepfake misuse. In *Anil Kapoor v. Simply Life India (2023)*²⁶, the Delhi High Court granted protection to the actor's name, image, voice, and likeness against unauthorized commercial exploitation. The Court acknowledged that these attributes form part of an individual's personality and deserve legal protection. This ruling is particularly important in the context of deepfakes, where a person's identity is digitally replicated without consent.

Similarly, in *Amitabh Bachchan Personality Rights Case (2022)*²⁷, the Delhi High Court recognized the exclusive right of a celebrity over their identity, including voice and image. The Court issued an injunction restraining unauthorized use of the actor's personality traits. This case reinforces the idea that identity is a valuable legal interest, and its misuse—whether through traditional means or advanced technologies like deepfakes—can be legally challenged. In addition, defamation jurisprudence under Sections 499 and 500 (now reflected in the Bharatiya Nyaya Sanhita, 2023) provides remedies where false statements harm an individual's reputation. Courts have consistently held that reputation is an integral part of the right to life under Article 21. Deepfakes, by presenting false visual or audio evidence, can cause far greater reputational harm than written or spoken defamation, making these precedents highly relevant. Another relevant case is *R. Rajagopal v. State of Tamil Nadu (1994)*²⁸, where the Supreme Court recognized the right of individuals to control the publication of their personal life stories without consent. This principle directly applies to deepfakes, as they involve unauthorized depiction of individuals in fabricated scenarios.

Collectively, these judicial precedents demonstrate that Indian courts have already developed a robust legal foundation to address issues arising from deepfake technology, even in the

²⁵ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

²⁶ *Anil Kapoor v. Simply Life India & Ors.*, Delhi High Court, 2023.

²⁷ *Amitabh Bachchan v. Rajat Nagi & Ors.*, Delhi High Court, 2022.

²⁸ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 (India).

absence of specific legislation. The recognition of privacy, personality rights, and reputation provides victims with legal avenues for redress. However, the application of these principles to deepfakes requires continuous judicial innovation and interpretation.

In conclusion, while deepfake-specific jurisprudence is still evolving, existing judicial precedents offer strong guidance in addressing identity misappropriation and digital harm. Courts must continue to expand these principles to effectively respond to the challenges posed by rapidly advancing AI technologies.

Conclusion and Suggestions

The emergence of deepfake technology marks a critical turning point in the relationship between law, technology, and individual rights. While artificial intelligence has brought remarkable advancements in fields such as entertainment, education, and communication, its misuse in the form of deepfakes has created unprecedented challenges. The ability to fabricate highly realistic audio-visual content has not only blurred the line between truth and falsehood but has also intensified the risks of identity misappropriation, privacy invasion, reputational harm, and cyber fraud.

The analysis of the Indian legal framework reveals that although statutes such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023 provide certain remedies, they are inherently inadequate and fragmented when applied to deepfake-related offences. These laws were enacted without anticipating the rise of AI-driven synthetic media and therefore fail to address the unique characteristics of deepfakes, such as their realism, scalability, and rapid dissemination. Additionally, issues like lack of clear definitions, evidentiary challenges, intermediary liability, and cross-border jurisdiction further complicate enforcement.

From a constitutional perspective, deepfakes pose a serious threat to fundamental rights, particularly the right to privacy, dignity, and reputation under Article 21, as well as the balance with freedom of speech under Article 19. Judicial precedents have laid a strong foundation by recognizing personality rights and informational privacy, yet the absence of a specialized legal framework leaves significant gaps in protection.

In light of these concerns, a multi-dimensional and forward-looking approach is necessary. The following suggestions are proposed:

1. Enactment of a Dedicated Deepfake Law

India should introduce specific legislation that clearly defines deepfakes and categorizes their malicious uses as distinct offences. The law should provide clear penalties, outline civil and

criminal liabilities, and include provisions for compensation to victims.

2. Mandatory Disclosure and Labeling

All AI-generated or manipulated content should be required to carry clear labeling or watermarking, ensuring transparency and enabling users to distinguish between real and synthetic media.

3. Strengthening Intermediary Accountability

The safe harbor provision under Section 79 of the IT Act should be revisited to impose stricter due diligence obligations on intermediaries. Platforms must deploy proactive detection systems and ensure swift removal of harmful deepfake content.

4. Investment in Detection Technology

The government should promote research and development of AI-based deepfake detection tools. Collaboration between public institutions, private companies, and academic bodies is essential to stay ahead of evolving technologies.

5. Recognition of Personality Rights in Statutory Law

Although courts have recognized personality rights, there is a need to codify these rights through legislation to provide clearer protection against unauthorized use of identity.

6. Capacity Building and Law Enforcement Training

Police, judiciary, and cybercrime units must be trained in handling AI-related offences, including detection, evidence collection, and digital forensics.

7. Public Awareness and Digital Literacy

Awareness campaigns should be conducted to educate citizens about deepfakes, their risks, and methods to verify digital content. An informed public is the first line of defense against misinformation.

8. International Cooperation

Given the borderless nature of cybercrime, India should actively participate in international frameworks and agreements to combat deepfake misuse and ensure effective cross-border enforcement.

REFERENCES

1. Statutes and Legislative Materials (Alphabetical Order)

1. Digital Personal Data Protection Act, 2023.
2. Information Technology Act, 2000.
3. Information Technology (Amendment) Act, 2008.

2. Research Papers, Books and Academic Publications Asawat, Vikas, “Information Technology (Amendment) Act, 2008: A New Vision Through a New Change,” Available at SSRN 1680152 (2010).

1. Chakrabarty, Shambhu Prasad, and Shrabana Chattopadhyay, “Criminal Liability of Artificial Intelligence-Generated Deepfakes in India,” International Ethical Hacking Conference (Springer Nature Singapore, 2024).
2. Chopra, Aahana, and Ananya Shukla, “Exploring the Misuse of Deepfake Technology in India: Implications for Society” (2024).
3. De Angeli, Antonella, et al., “Reporting Non-Consensual Pornography: Clarity, Efficiency and Distress,” Multimedia Tools and Applications 82, no. 9 (2023): 12829–12858.
4. Iyer, Malathi Sundaram, et al., “Critical Analysis of the Information Technology Act 2000, Its Amendments, and the Emerging Digital Personal Data Protection Act 2023 in the Context of Global Regulatory Benchmarks,” Evolution 3, no. 3 (2026).
5. Jones, Valencia A., Artificial Intelligence Enabled Deepfake Technology: The Emergence of a New Threat (Utica College, 2020).
6. Kılıç, Büşra, and Mehmet Emin Kahraman, “Current Usage Areas of Deepfake Applications with Artificial Intelligence Technology,” İletişim ve Toplum Araştırmaları Dergisi 3, no. 2 (2023): 301–332.
7. Meenakshi, Meenakshi, “Deepfake Technology and Legal Challenges in India: An Analysis,” International Journal of Teaching, Learning and Education 3, no. 2: 18–24.
8. Mohammed, Anwar, “Deep Fake Detection and Mitigation: Securing Against AI-Generated Manipulation,” Journal of Computational Innovation 4, no. 1 (2024).
9. Pan, Zhaoqing, et al., “Recent Progress on Generative Adversarial Networks (GANs): A Survey,” IEEE Access 7 (2019): 36322–36333.
10. Panda, Biranchi Naryan P., and Isha Sharma, “Deepfake Technology in India and World: Foreboding and Forbidding,” Law and Humanities Quarterly Reviews 4, no. 3 (2025): 18–28.
11. Panwar, Kuldeep Singh, and Nilutpal Deb Roy, “Rising Menace of Deepfakes with the Help of AI: Legal Implications in India,” Indian Journal of Integrated Research in Law IV, no. III (2024).
12. Saxena, Divya, and Jiannong Cao, “Generative Adversarial Networks (GANs): Challenges, Solutions, and Future Directions,” ACM Computing Surveys 54, no. 3 (2021): 1–42.

13. Vig, Shinu, "Regulating Deepfakes," *Journal of Strategic Security* 17, no. 3 (2024): 70–93.

3. Case Laws

1. Amitabh Bachchan v. Rajat Nigam & Ors., Delhi High Court (2022).
2. Anil Kapoor v. Simply Life India & Ors., Delhi High Court (2023).
3. Ankur Warikoo v. John Doe, Delhi High Court (2023).
4. Gaurav Bhatia v. Naveen Kumar & Ors., Delhi High Court (2023).
5. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
6. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
7. Shreya Singhal v. Union of India, (2015) 5 SCC 1.

