INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN:2582-6433

DISCLAIMER

 ISSN:2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN:2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN:2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN:2582-6433

THE RISE OF DEEPFAKE TECHNOLOGY: SOCIETAL, ETHICAL, AND LEGAL CHALLENGES IN THE DIGITAL AGE

AUTHORED BY - ANKITA KHAMARI[1]

Abstract

Deepfake technology, driven by advancements in AI and machine learning, allows for the creation of highly realistic synthetic content. While this innovation has positive uses in areas like entertainment, education, and marketing, it is often misused to spread misinformation, create non-consensual explicit material, commit identity theft, and carry out financial scams. Such misuse can cause serious harm, including reputational damage and emotional distress for victims. Legal concerns related to deepfakes include privacy violations, defamation, hate speech, and the difficulties of prosecuting offenders due to anonymity and cross-border jurisdiction issues. To address these challenges, various countries have introduced laws, such as the U.S. Deepfakes Accountability Act, the EU's GDPR and DSA, and China's regulations requiring clear labeling of synthetic content. In India, provisions under the IT Act, Bharatiya Nyaya Sanhita (BNS), and the Digital Personal Data Protection Act aim to tackle deepfake misuse, though enforcement remains a significant challenge. Cases involving celebrities like Anil Kapoor and Amitabh Bachchan underscore the importance of protecting personality rights from unauthorized digital manipulation. To reduce the risks posed by deepfakes, India needs specific laws, stronger international collaboration, and better cybersecurity measures. Public awareness campaigns, improved detection technologies, and balanced regulations are also essential to address this issue effectively. Managing the dual nature of deepfakes—harnessing their benefits while preventing harm—requires robust legal frameworks, global cooperation, and proactive efforts to educate the public and promote ethical use.

Keyword: Deepfake technology, Artificial Intelligent, Advancement.

[1] Faculty, P.G. Department of Law, Sambalpur University, Odisha.

 ISSN:2582-6433

Introduction

Deepfake technology marks a major advancement in artificial intelligence (AI) and machine learning, enabling the creation of highly realistic but completely fake visual and audio content. By combining "deep learning" with the concept of "fake," this technology can modify or produce media that convincingly imitates real people's appearances or voices. Often exploited in cybercrime, deepfakes are used to spread false information by mimicking someone's identity. The increasing use of digital platforms, along with easy access to advanced tools like AI, Photoshop, and machine learning software, has made it simpler for bad actors to create lifelike fake videos and audio clips. These tools allow cybercriminals to manipulate media—often sourced from social media—by altering facial features, voices, or body movements. This makes it challenging to tell apart genuine content from fabricated material.[2]

Deepfake creation usually starts with facial mapping technology to gather data on facial symmetry. This is followed by the use of Generative Adversarial Networks (GANs) to smoothly replace one person's face with another's. Additionally, voice cloning tools are used to accurately imitate the target's voice. The outcome is so realistic that it becomes extremely difficult to determine whether the audio or video is real or fake.[3] Several studies have highlighted the risks associated with deepfake technology, especially its potential for misuse. The University College London (UCL) has even ranked it among the most serious threats of the modern age.

While deepfakes enable a wide range of crimes, making them challenging to regulate, this does not mean the technology should be completely banned. It has many legitimate and beneficial applications. For instance, the *Malaria Must Die* campaign used deepfake technology to make David Beckham deliver awareness messages in nine different languages. Similarly, deepfakes are being utilized in various sectors, including government programs, interviews, and public awareness campaigns in regional languages, showcasing their potential for positive contributions.[4] As a result, it is essential for legal frameworks to evolve and address the challenges posed by this rapidly advancing technology.

[2] The rise of artificial Intelligence and deepfakes, https://buffett.northwestern.edu/documents/buffett-brief_the-rise-of-ai-and-deepfake-technology.pdf.
[3] Jaiman A, The danger of deepfakes, The Hindu, January 01, 2023, Available at: https://www.thehindu.com/sci-tech/technology/the-danger-of-deepfakes/article66327991.ece.
[4] Lalla V, Mitrani A and Harned Zach , Artificial Intelligence: deepfakes in the entertainment industry (June 19, 2022), https://www.wipo.int/web/wipo-magazine/articles/artificial-intelligence-deepfakes-in-the-entertainment-industry-42620.

 ISSN:2582-6433

The Rise and Risks of Deepfake Technology

Deepfake technology initially found positive applications in fields like entertainment, education, and healthcare. It was used to enhance special effects, create immersive learning experiences, and simulate patient interactions. However, the widespread availability of AI tools has led to its misuse. Deepfakes have been exploited to spread false information, blackmail individuals—especially women—and produce non-consensual explicit content, causing serious harm to victims' reputations and mental health.

The easy access to deepfake creation tools has raised significant ethical, legal, and social concerns. While the technology started with beneficial uses, its malicious applications have sparked debates about accountability and the need for stronger regulations. Safeguards are essential to prevent abuse while still allowing for constructive uses.

Deepfake technology offers great potential but also poses serious risks. Although it has been applied in creative and educational settings, its harmful misuse creates ethical and legal challenges. Governments, international bodies, and tech companies are working to counter these issues through laws, regulations, and improved detection methods. As the technology continues to advance, the key challenge will be balancing innovation with the need to protect against its misuse.

Legal Issues and Challenges

- **Violation of Privacy:** Deepfakes, especially those created without an individual's consent, violate the right to privacy, which is a fundamental right under the Indian Constitution. The unauthorized use of a person’s likeness for malicious purposes—such as defamation or exploitation—can significantly harm the individual’s personal and professional life.[5]
- **Lack of Consent:** Deepfakes are often created without the consent of the individuals involved, exposing them to reputational damage, emotional distress, and financial losses. The absence of specific laws addressing deepfakes complicates legal recourse for victims.
- **Cross- Border Jurisdiction Issues:** Since deepfakes can be created and distributed from any part of the world, it is often difficult for Indian authorities to hold perpetrators

[5] K.S. Puttaswamy (Retd.) v. Union of India, (2017)10 SCC 1.

 ISSN:2582-6433

accountable. Cross-border jurisdiction challenges hinder effective prosecution and enforcement, requiring international cooperation to regulate and manage the spread of deepfake content.[6]

- **Defamation and Damage to reputation:** Defamation laws in India are designed to protect individuals from harm caused by false statements. However, deepfakes complicate this framework, as offenders often operate anonymously, making it difficult to identify and prosecute them. Furthermore, the rapid viral spread of deepfakes exacerbates reputational damage, and proving that a deepfake caused harm can be legally challenging.[7]
- **Hate speech and incitement to Violence:** Deepfakes can be manipulated to spread hate speech, leading to social unrest and even violence. Fake videos that falsely depict individuals making provocative statements can incite communal or political tensions. Legal provisions, such as sections under the IPC (Indian Penal Code), address hate speech, but the anonymous nature of deepfake creators makes enforcement challenging.
- **Challenges in prosecution and evidence:** The technical complexity of deepfakes presents obstacles in legal proceedings. Judges and law enforcement often lack the necessary expertise to assess digital evidence accurately, which can affect the fairness of trials. Additionally, proving the authenticity of deepfake content in court is difficult, especially when the creators are anonymous or based in other jurisdictions.[8]

Global Response to Deepfakes

The global response to deepfakes has been multifaceted, as governments, legal systems, and international organizations work to address the risks associated with the technology.

1. **United States:** In the U.S., both federal and state governments have enacted measures to combat the harmful effects of deepfakes. Key legislative steps include the Deepfakes Accountability Act, which requires digital watermarks on synthetic media and proposes penalties for malicious use. California has banned the distribution of manipulated videos close to elections and criminalized non-consensual deepfake pornography. Similarly, Texas has made the creation of election-related deepfakes illegal. Major tech

[6] Gupta Indranath and Srinivasan Lakshmi, "Evolving Scope of Intermediary Liability in India," INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY (2023): 1-31.
[7] Ibid.
[8] Chesney Robert and Citron Danielle, "Deepfakes and the New Disinformation War: THE COMING AGE OF POST-TRUTH GEOPOLITICS," FOREIGN AFFAIRS,98, 147(2019).

 ISSN:2582-6433

companies, like Facebook and Google, have also taken action by promoting deepfake detection tools and initiatives.[9]

2. **European Union (EU):** The EU addresses deepfakes through its broader regulatory frameworks, including the General Data Protection Regulation (GDPR), which protects personal data and privacy. The Digital Services Act (DSA) holds online platforms accountable for illegal content, including deepfakes. Furthermore, the EU has funded research projects such as Social Truth, aimed at improving media verification to combat deepfake content.
3. **China**: China has adopted strict regulations via the Cyberspace Administration of China (CAC), requiring synthetic media, including deepfakes, to be clearly labeled. These rules help prevent the misuse of deepfakes, particularly in ways that could harm national security or social order. Violations are met with significant penalties, reflecting China's rigorous stance on deepfake technology.[10]
4. **Other Countries**

- Australia has enacted the Enhancing Online Safety Act, aimed at protecting individuals from image-based abuse, including deepfakes.
- In the United Kingdom, the Law Commission has proposed legal reforms targeting non-consensual deepfake pornography, while the Online Safety Bill holds online platforms accountable for harmful content, including deepfakes.[11]
- International organizations, such as Interpol and the United Nations, are working to foster global cooperation on developing detection tools and regulatory frameworks to address the cross-border challenges posed by deepfakes.[12]

Deepfake Technology in India: Positive and Negative Applications

Deepfake technology, while still in its nascent stage in India, is being explored in both beneficial and harmful ways. Below is a summary of its diverse applications across different

[9] Paarth Neekhara, Brian Dolhansky, Joanna Bitton, and Cristian Canton Ferrer, Adversarial Threats to Deepfake Detection: A Practical Perspective, in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition,923-932, (2021).
[10] Hwang Yoori, Ji Youn Ryu, and Se-Hoon Jeong, Effects of Disinformation Using Deepfake: The Protective Effect of Media Literacy Education, 3 CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING 24,188-193, (2021).
[11] Chesney Robert and Citron Danielle, Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics,Foreign Affairs 98 147, (2019).
[12] Carl Öhman, Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography,2, ETHICS AND INFORMATION TECHNOLOGY 22, 133- 140, (2020).

 ISSN:2582-6433

sectors, showcasing both the positive and negative uses of deepfake technology.[13]

Positive Applications of Deepfakes in India

Sector	Use Case
Entertainment Industry	Filmmakers use deepfakes to enhance special effects, create realistic digital avatars, and ensure safety in dangerous stunts. The technology helps integrate actors' faces into risky scenes without compromising realism.
Education and Training	Educational institutions are leveraging deepfakes to create immersive and interactive learning experiences. This includes subjects like history, physics, and geography, where virtual educators engage students more effectively.
Startups and Innovation	Indian startups like Rephrase.ai and SimYog Technologies are utilizing deepfake technology to create personalized synthetic videos for marketing, enabling businesses to scale communication and produce customized messages using digital avatars.

Negative Applications of Deepfakes in India

Sector	Misuse Case
Political Manipulation	Deepfakes have been used in Indian politics to spread disinformation, especially during elections. In one instance, a deepfake video was allegedly circulated to misrepresent an opponent, damaging their credibility.
Non-Consensual Explicit Content	Deepfakes have been misused to create fake pornographic videos of women by superimposing their images onto explicit content. These videos are used for blackmail, harassment, and revenge, with devastating personal and social consequences for victims.
Fraud and Impersonation	Deepfakes have been employed in scams to impersonate high-profile individuals or even family members to trick people into revealing confidential financial information. These fraudulent activities often lead to significant financial losses.

[13] Abdul-Rahman, Kabbara. Bots & Deepfakes, NSI Intern Integration Project, August 2021. https://nsiteam.com/social/wpcontent/uploads/2021/08/IIJO_eIntern-IP_Bots-andDeepfakes_Kabbara_FINAL.pdf.

 ISSN:2582-6433

Deepfake technology in India has a dual nature, with significant potential for innovation and creativity in sectors like entertainment, education, and marketing. However, its increasing misuse in politics, non-consensual content, and financial fraud is raising alarms. As both positive and negative applications grow, the need for regulation, awareness, and technological safeguards is becoming ever more critical to mitigate the risks associated with deepfakes.[14]

By addressing these concerns through stricter laws, technology solutions, and public education, India can better harness the positive potential of deepfakes while curbing their harmful effects.[15]

Managing Deepfakes in India: Legal and Technological Framework

India is increasingly recognizing the risks and misuse associated with deepfake technology. As awareness grows, there are calls for stronger legal frameworks and technological measures to manage its spread and mitigate its harmful effects.[16] India's existing legal provisions and regulatory infrastructure offer several avenues for addressing deepfake-related challenges, which are highlighted below:

1. Information Technology Act, 2000 (IT Act)

The IT Act serves as the primary legal framework for cyber activities in India and provides provisions relevant to deepfake misuse:

- **Section 66E**: Addresses privacy violations, such as manipulating or sharing private images or videos without consent.[17]
- **Section 67**: Criminalizes the publication of obscene material, including sexually explicit deepfakes.[18]
- **Section 67A**: Focuses on stricter penalties for transmitting sexually explicit content, relevant for deepfakes depicting explicit acts without consent.[19]

[14]Chadha A, Kumar Vaibhav, Kashyap Sonu, and Gupta Mayank, "Deepfake: An Overview," in Proceedings of Second International Conference on Computing, Communications, and Cyber-Security: IC4S 2020, 557-566, (2021)
[15] Mika Westerlund, The Emergence of Deepfake Technology: A Review, 9, TECHNOLOGY INNOVATION MANAGEMENT REVIEW, no. 11 (2019).
[16] Vig, Shinu, "Regulating Deepfakes:an Indian Perspective,17, JOURNAL OF STRATEGIC SECURITY, volume17, no.3, 70-93, (2024) DOI: https://doi.org/10.5038/1944-0472.17.3.2245 Available at: https://digitalcommons.usf.edu/jss/vol17/iss3/5.
[17] The Information Technology Act, 2000, §66A
[18] The Information Technology Act, 2000, §67,
[19] The Information Technology Act, 2000, §67A,

 ISSN:2582-6433

- **Section 69A**: Empowers the government to block access to harmful content, including deepfakes, if they threaten national security or public order.[20]

2. Bharatiya Nyaya Sanhita, 2023 (BNS)

The IPC includes provisions that are applicable to deepfake-related offenses:

- **Defamation (Section 356)**: Criminalizes actions that harm a person's reputation, such as the creation and distribution of defamatory deepfakes.[21]
- **Criminal Intimidation (Section 351(1))**: Covers threats made through deepfakes, such as blackmail or coercion.[22]
- **Cheating by Personation (Section 318(1))**: Pertains to cases where deepfakes are used to impersonate individuals for fraudulent purposes.[23]
- **Voyeurism (Section 76)** and **Stalking (Section 77)**: Address the use of deepfakes to harass or stalk individuals, particularly in cases involving intimate content.[24]
- **Sexual Offenses**: Several sections protect against harassment, exploitation, and abuse, relevant for deepfakes that involve sexual content.[25]

3. Indecent Representation of Women (Prohibition) Act, 1986

This act prohibits the indecent representation of women in various media, including digital formats. It applies to deepfakes that depict women in derogatory or sexualized ways without consent. The act allows for imprisonment and fines for those involved in producing or distributing such content, though enforcement can be challenging due to the transnational nature of online platforms.[26]

4. Digital Personal Data Protection Act, 2023

The Data Protection Act strengthens privacy rights and regulates the processing of personal data in India:

[20] The Information Technology Act, 2000, §69A,
[21] Indian Penal Code 1860, § 499
[22] Indian Penal Code 1860, § 503
[23] Indian Penal Code 1860, § 416
[24] Indian Penal Code 1860, § 354c, 354d,
[25] Indian Penal Code 1860, § 509, 354,354A, 354B, 354C,354D, 375,
[26] Indecent Representation of Women (Prohibition) Act, 1986, § 2(C), 3,4,6,7.

 ISSN:2582-6433

- **Consent Requirement**: Entities must obtain explicit consent before processing personal data, including images or likenesses, making the unauthorized use of someone's image in deepfakes a violation.[27]
- **Data Principal Rights**: Individuals have the right to access, correct, and erase personal data, which allows victims of deepfake misuse to request the removal of unauthorized content.[28]
- **Penalties for Non-Compliance**: The act imposes significant fines for non-compliance, providing a deterrent against the misuse of personal data in creating deepfakes.[29]

5. Cybersecurity Framework in India

India's cybersecurity infrastructure plays an essential role in managing the risks posed by deepfakes:

- **CERT-In**: The national agency for cybersecurity issues, which provides advisories on mitigating cyber threats, including deepfakes, though it does not focus specifically on this area.[30]
- **Cyber Crime Investigation Cells**: State-level police units with the technical expertise to investigate cybercrimes, including those involving deepfakes.[31] These units face challenges in terms of resources and rapidly advancing technology.[32]
- **Intermediary Guidelines and Digital Media Ethics Code, 2021**: These rules place obligations on social media platforms to remove harmful content, including deepfakes, upon receiving appropriate orders. While platforms must act on content flagged by users, proactive detection of deepfakes remains difficult.[33]

India's legal and regulatory framework provides several tools to address deepfake misuse, including privacy protections, defamation laws, and penalties for the distribution of obscene or harmful content. However, the rapid evolution of deepfake technology, the anonymity of perpetrators, and the cross-border nature of online platforms present significant challenges. To effectively manage deepfakes, India will need continuous legislative reforms, enhanced

[27] Digital Personal Data Protection Act, 2023, §, 4.
[28] Digital Personal Data Protection Act, 2023, §, 11.
[29] Digital Personal Data Protection Act, 2023, §, 12,14,25.
[30] Information Technology Act, 2000, § 70B.
[31] Information Technology Act, 2000, § 78.
[32] Code of Criminal Procedure, 1973, §§ 154–176.
[33] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(1)(b), 3(2),4(4), Gazette of India, Feb. 25, 2021.

 ISSN:2582-6433

enforcement, and stronger collaborations with tech companies and global partners. These efforts should focus on balancing the regulation of harmful content while preserving the potential for positive uses of AI technologies.

Recent Cases and Enforcement Challenges: Legal Precedents in India

As deepfake technology has grown, its misuse has prompted legal action to protect individuals' rights, particularly in cases involving the unauthorized use of images, voices, and personas.[34] Notably, the Delhi High Court has played a crucial role in addressing these issues through landmark rulings that set legal precedents for enforcing personality rights in the digital age.

1. **Anil Kapoor vs. Simply Life India and Ors[35]:**In this case, Bollywood actor Anil Kapoor took legal action against several defendants who had unlawfully used his likeness for commercial purposes without his consent. The court granted an ex-parte injunction, protecting his personality rights, which include his name, image, voice, and persona. The defendants had created and sold AI-generated deepfakes and other content using Kapoor's likeness. The court ordered the defendants to cease such activities, blocked infringing links, and directed the transfer of domain names like www.anilkapoor.in to Kapoor. This ruling marked a significant step in protecting celebrities' rights in the digital realm, particularly against the misuse of emerging technologies like deepfakes.
2. **Amitabh Bachan vs. Rajat Negi and Ors.[36]:** Similarly, in the case involving **Amitabh Bachchan**, the Delhi High Court addressed the unauthorized creation and dissemination of **deepfake content** that manipulated Bachchan's image and likeness without his consent. The court acknowledged that this violated Bachchan's **personality rights** and **privacy**, particularly when the deepfakes were used for commercial purposes or in a derogatory manner. The court issued an injunction preventing further misuse and ordered the removal of the deepfake content across online platforms. This case reinforced the need to protect individuals' privacy and personality rights against technological misuse.
3. **Impersonation of the Chief of India (CJI):** Fraudsters used deepfake technology to create realistic videos and audio clips, impersonating the CJI. These videos falsely

[34] Khushi Saraf, Akshay Sriram, "The Diemma of Deepfakes: Expanding the Ambit of Right to Personality to Regulate Deepfakes in India, LAW SCHOOL POLICY REVIEW, 2024.
[35] 2023 SCC Onl=Line Del 6914
[36] 2022 SCC online Del 4110.

 ISSN:2582-6433

endorsed certain legal services and investment schemes, deceiving victims into making financial transactions worth crores of rupees.

4. **Non-Consensual Explicit Content:** A prominent Indian actress became a victim of deepfake technology when her face was digitally inserted into sexually explicit videos. These deepfakes spread widely on social media platforms, leading to severe emotional distress and reputational harm for the actress. She filed a complaint with the cybercrime division to hold the perpetrators accountable.
5. **Political Deepfakes:** During the 2020 Delhi Legislative Assembly elections, a political party allegedly used deepfake technology to create a video of its leader speaking in languages the leader did not know. This raised concerns about the ethical implications of using deepfakes to influence voters and spread misinformation.

Conclusion

Deepfake technology poses serious threats to privacy, reputation, and public safety, highlighting the need for robust legal measures to tackle its misuse. India's current legal framework is not adequately prepared to address the challenges posed by deepfakes, as many existing laws do not cover this form of digital manipulation. There is a pressing need for specific laws that criminalize harmful deepfakes, clearly define malicious uses, and offer effective remedies for victims.[37]

The legal system must adapt to incorporate technical expertise for investigating and prosecuting deepfake-related crimes. International collaboration is also crucial to address the cross-border challenges posed by this technology. While safeguarding individual rights and preventing abuse, India should aim to strike a balance that permits legitimate uses of deepfake technology in areas like satire, art, and education.[38] India can address the challenges of deepfakes more effectively by strengthening its legal frameworks, raising public awareness, and fostering collaboration with international partners, all while protecting the rights and privacy of its citizens.

[37] Sandeep Singh mankoo, Deepfakes The Digital Threat in the Real world, 17, GYAN MANAGEMENT JOURNAL, issue-1,2023

[38] Shruti Kakkar, Hindustan Times, Aug 28, 2024, available at: https://www.hindustantimes.com/india-news/delhi-hc-urges-centre-to-frame-law-to-regulate-ai-deepfake-101724853407493.html.