Library Progress International *Print version ISSN 0970 1052*
Vol.43, No.2, Jul-Dec 2023: P. 739-750 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

SAFEGUARDING REPUTATION IN THE AGE OF ARTIFICIAL INTELLIGENCE: ADDRESSING THE CHALLENGES OF DEEPFAKES AND MORPHING THROUGH A CRITICAL LEGISLATIVE FRAMEWORK IN INDIA

***Bharti**
Research scholar
Maharshi Dayanand University, Rohtak, Haryana
E-mail: bhartis1130@gmail.com

***Dr. Kavita Dhull**
Professor
Maharshi Dayanand University Rohtak Haryana
E-mail:dhullkavita@gmail.com

Abstract

The rapid advancement of Artificial Intelligence generated content morphing and deepfakes technology has raised significant concerns about individual rights, particularly Reputation ,privacy, identity, and dignity. This paper critically analyses existing legal frameworks and regulatory responses to address morphing and deepfakes-related harms. This research identifies gaps in current laws and proposes reforms to ensure adequate protection of individual rights.

Keywords: Artificial Intelligence, Deepfakes, Morphing, , Reputation. Cybercrimes

Research Questions:

1. How do Artificial Intelligence generated content morphing and deepfakes impact individual rights, particularly Reputation Privacy, Identity, and Dignity?
2. What are the existing legal frameworks and regulatory responses to address Artificial Intelligence ?
3. How effective are current laws in protecting reputation from morphing and deepfakes?
4. What reforms or new regulations are necessary to ensure adequate protection of individual rights?

Introduction

Artificial Intelligence generated content Morphing and deepfakes technologies have revolutionized the digital world, which has enabled audio-visual manipulation capabilities.[1]These developments effectively affect a number of businesses, including national security, advertising, and entertainment.[2]However, there are also serious concerns to individual rights like privacy, reputation, identification, and dignity from this technology.. Using artificial intelligence (AI), they produced lifelike but fake films of peoples.Generative AI like ChatGPT has revolutionized the way we interact with and view AI.There is an inherent risk of affecting the individual Rights includes hallucinations, deepfakes, data privacy, copyright issues and cyber security. Ai can create fake text, audio,vedios , content of an individual and diminishing the credibility of that person with deepfakes and misinformation.[3]This paper examines the

[1]Ajder, H., et al. (2020). Deepfakes and Morphing: A Review. IEEE Transactions on Information Forensics and Security, 15, 3993-4006.

[2]Kemelmacher - Shlizerman, I., et al (2016). The State of Deepfakes. IEEE Transactions on Pattern Analysis and Machine Intelligence, 38(1), 132-135.

[3]Anandi, 11 January ,2023,deepfakes deeper impact:Ai roll in the 2023 Indian genral election and beyond..visted on(11 january,2023). Available on :https://gnet-research.org/2023/01/02/deep-fakes-deeper-impacts-ais-role-in-the-2023-indian-general-election-and-beyond/.

impact of morphing and deepfakes on individual rights and assesses the effectiveness of existing legal frameworks and regulatory responses.

Morphing and Deepfakes Technology: Morphing and deepfakes technologies leverage artificial intelligence (AI) and machine learning (ML) to alter digital content, creating synthetic media that can closely resemble real life. These developments carry significant consequences across multiple sectors.[4]

Morphing Technology: Morphing is the process of changing one image or video into a different one, typically utilizing a blend of algorithms and manual editing techniques.This method is frequently employed in visual effects for films and television, as well as in advertising and on social media platforms.

Deepfakes Technology: Deepfake technology utilizes artificial intelligence (AI) and machine learning algorithms to generate media that appears realistic yet is fabricated, capable of altering or creating audio, video, or images. The term "deepfakes" highlights the deceptive qualities of this content, merging the concepts of "deep learning," a subset of artificial intelligence.[5]Artificial Intelligence and machine learning are employed in creating compelling synthetic media known as Deepfakes, commonly applied in facial recognition and voice synthesis. These Deepfakes serve various purposes such as entertainment (e.g., video games, movies), education (e.g., historical figure simulations), and social engineering (e.g., phishing, impersonation).

Types of Deepfakes:

- • Face swap involves creating photos where a person's face is replaced with another individual's features, including their expression, lighting, and background.
- • Voice cloning, a cutting-edge development in machine learning powered by artificial intelligence, enables the precise replication of a person's voice through an extensive database of audio recordings of various people. lies in their ability to imitate and
- Video synthesis, also referred to as video generation or creation, utilizes artificial intelligence (AI) and machine learning (ML) algorithms to produce authentic-looking videos.

- - Video, audio, text, image synthesis involves generating new video content either from scratch or by using existing sources like text, images, audio, or other videos. This process transforms original text into entirely different output videos. The technology finds applications in communication, education, entertainment, and simulation. The current trend in video synthesis involves deepfakes, artificial videos employing deep learning models to replace a person's voice or face. While these videos can be humorous or satirical, they also raise ethical and legal concerns. The advancement nature of these models lies in their ability to imitate and replicate distinctive voice characteristics such as intonation, pitch, and regional accents. When it comes to speech-to-text technology, they excel at mimicking a person's voice.[6]
- Video synthesis: Video synthesis, also known as video generation or video creation, uses artificial intelligence (AI) and machine learning (ML) algorithms to generate realistic videos.
- Types of Video Synthesis

[4] Chesney, R., & Citron, D. (2019). Deepfakes: A Primer. In Deepfakes and Beyond (pp. 1-14). Cambridge University Press.

[5] Chesney, R., & Citron, D. (2019). Deepfakes: A Primer. In Deepfakes and Beyond (pp. 1-14). Cambridge University Pres.

[6]Fatima mohsin inamdar et all (2023) voice cloning using artificial intelligence and machine learning :A review ,journal of advanced zoology. 44 s7.419-427.

- Deepfakes videos: Deepfakes videos are artificially created videos that appear highly realistic, manipulating individuals. These videos make it challenging to discern reality as machines alter faces, expressions, or voices in existing clips solely through algorithmic processes.
- Video, audio ,text, image synthesis involves generating new video content either from scratch or by using existing sources like text, images, audio, or other videos. This process transforms original text into entirely different output videos.[7] The technology finds applications in communication, education, entertainment, and simulation. The current trend in video synthesis involves deepfakes, artificial videos employing deep learning models to replace a person's voice or face. While these videos can be humorous or satirical, they also raise ethical and legal concerns.[8]

Applications: deepfakes and morphing has various practical applicablity such as

- Film and video producers utilize AI to improve special effects and create more lifelike characters.[9]
- Virtual reality (VR) and augmented reality (AR):Augmented reality is more effective than virtual reality as a branding and gaming tool since it is accessible to almost anyone with a smartphone. By using a phone's camera or video viewer to project virtual images and characters, augmented reality (AR) transforms the ordinary, physical world into a vibrant, visual one. Simply said, augmented reality enhances the user's experience of the real world.[10]
- Advertising and marketing: This technology innovation itself can be in the marketing and advertising. Unfortunately this is become very popular to bullying the people, create the fake content, hate speech,child abused manipulating videos etc.[11]
- Education and training: in the education and training field Artificial Intelligence also used to enhance the quality of content.
- Social media and entertainment: Artificial Intelligence is using rapidly in the social media platforms for the entertainment purpose.Artiticial intelligence helps people to discover new stuff and also can predict for the future concept also.

Concerns and Risks:

Misinformation and Disinformation: Deepfakes can spread false information, manipulating public opinion through various means and mode such as fake podcast, false speech false audio.Videos can be altered to show individual saying or doing they never did.[12]

Reputation Damage: Morphed content can defame individuals, damaging their reputation.[13]

Social Manipulation:

[7] Cheris frauts,james albert silvoza(2023) . what are the current trends and challenges in vedio synthesis and editing. Available at :https://www.linkedin.com/advice/0/what-current-trends-challenges-video-synthesis

[8]Wang, T., et al. (2018). Video-to-video synthesis. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 6663-6672.

[9] Kemelmacher ,shilzerman et all (2016). Face reconstruction from voice transaction on pattern anylisis and machine intelligence.38(10).1941-1953.

[10] Avilable at:https://sopa.tulane.edu/blog/whats-difference-between-ar-and-vr visited on (22 January,2023).

[11] The legal implications of Deepfakes in marketing, Available at:https://blog.ipleaders.in/the-legal-implications-of-deepfakes-in-marketing-an-insight/(visited on 22 Jan,2023).

[12] Kemelmacher-Shlizerman, I., Seitz, S.M., Miller, D.B. & Brossard, E. (2016)

[13] Tulyakov, S., Liu, M.-Y., Yang, X., & Kautz, J. (2018). MoCoGAN: Decomposing motion and content for video generation. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 5627-5636.

Deepfakes can influence elections, political discourse, and social movements.[14]
Cyberbullying: Morphing can facilitate online harassment, intimidation, and bullying.[15]

- **Psychological Concerns**

  Emotional Distress: Deepfakes can cause anxiety, depression, and trauma.
  Identity Theft: Morphing can compromise individuals' identity, leading to psychological distress.
  Trust Erosion: Deepfakes can undermine trust in institutions, media, and relationships.

- **Security Concerns**
- National Security: Deepfakes can compromise classified information; threatening national security because deepfakes and morphing manipulates the public opinion. These two can creates false narratives. Deepfakes can deceive government and their agencies. Also spread wrong propaganda among masses.
- Financial Fraud: Morphing can facilitate financial scams, identity theft, and phishing attacks
- Biometric Spoofing: Deepfakes can bypass biometric authentication systems.

- Ethical **C**oncerns Consent and Privacy: Morphing and deepfakes often violate individuals' consent and privacy

- Objectification: Deepfakes can perpetuate objectification, exploitation, and harassment
- Cultural Appropriation: Morphing can misrepresent cultural heritage

Social Concerns

Cyber bullying: Morphing can facilitate online harassment, intimidation, and bullying.[16]

Technical Concerns

Detection Difficulty: Deepfakes are steadily More tough to detect.
Malware and Cyberattacks: Morphing and deepfakes can promote malware dispersal and cyberattacks.
Deepfakes Detection Bias: Detection algorithms may display biases, troublesome accuracy.

Difference between morphing and deepfakes

Despite being technologies for reshaping images and videos, morphing and deepfakes differ strongly in their capabilities, uses, and processes. Here's an overview of the key differences between the two:

[14]Hwang, Y., Kim, J., Kwak, N., & Lee, J. (2019). FaceNet++: Unified dimensionality reduction for face recognition and clustering. IEEE Transactions on Pattern Analysis and Machine Intelligence, 41(11), 2633-2644.
[15] Dinakaran, M., Suresh, S., & Rajendran, S. (2020). Deepfake detection using deep learning techniques: A survey. Journal of Intelligent Information Systems, 57(2), 257-275.
[16]Dinakaran, M., Suresh, S., & Rajendran, S. (2020). Deepfake detection using deep learning techniques: A survey. Journal of Intelligent Information Systems, 57(2), 257–275.

- **Deepfakes**

Technology:

Deepfakes primarily facilitate artificial intelligence and machine learning, specifically techniques like Generative Adversarial Networks (GANs). These models are instructed on large datasets of images and videos to learn how to regenerate realistic representations.

Functionality:

Deepfakes can create highly realistic videos that alter one individual's likeness with another's. They can also alter speech to match the new face, making it emerge that the person is saying something they never said.

Complexity:

The process involves ultra modern algorithms and a substantial amount of data (images, videos, audio) to produce a persuasive findings . This means it can take significant digital resources and time.

Common Applications

Deepfakes are often used in entertainment (e.g., movies, memes), education, and sometimes for nefarious purposes, such as creating fake news or misleading videos.

Detection

Researchers are working on ways to detect deepfakes, as their true nature makes them difficult to identify.

Morphing

Technology

Morphing is a simpler digital image processing technique that creates a smooth transition between two or more images. It involves image manipulation rather than advanced AI models.

Functionality:

Morphing blends features of different images to create a seamless transition or transformation. For example, you might morph the face of one person into another over several frames.

Complexity

The morphing process typically uses key frames and interpolation techniques, which are generally less computationally intensive than training a deep learning model.

Common Applications

Morphing is often used in animation, film effects, art, and graphic design. It is primarily for visual effects rather than for creating convincingly deceptive media.

Detection

As morphing often yields less realistic outputs compared to deepfakes, detection can be less of a concern. The goal is usually artistic rather than deceptive.

Table for difference between deepfakes and morphing:

Features	**Deepfakes**	**Morphing**
Underlying technology	AI machine learning	Image processing
Functionality	Replace faces, alter speech high realms	Smooth transitions between images
Complexity	More complex requires large database	Less complex uses fewer resources
Common use cases	Entertainment, misinformation	Animation, visual art, graphic

Detection uses	Harder to detect	Generally more recognisable

Literature Review

Morphing and deepfakes technology has been used in various contexts, including entertainment, politics, and cybercrime. Research has highlighted the potential harms of morphing and deepfakes, including identity theft, defamation, and emotional distress.

Deep learning-based detection: Chawla et al. (2020) proposed a convolutional neural network (CNN) approach for detecting deepfakes.[17] Audio-visual inconsistencies: Li et al. (2019) identified inconsistencies between audio and visual cues to detect deepfakes.[18]Digital watermarking: Zhu et al. (2020) explored digital watermarking techniques for authenticating digital media.[19]Defamation and misinformation: Kumar et al. (2020) analyzed Indian laws addressing defamation and misinformation related to deepfakes.[20]Intellectual property rights: Singh et al. (2019) discussed copyright infringement issues arising from deepfakes.[21]Data protection :Garg et al. (2020) examined the impact of deepfakes on data protection laws.[22]

Revenge porn and harassment: Citron (2019) discussed the devastating effects of deepfakes on victims of revenge porn.[23]Political misinformation: Benkler et al. (2018) analyzed the role of deepfakes in spreading misinformation during elections.[24]

Social media regulation: Gillespie (2018) explored the challenges of regulating social media platforms amidst deepfakes proliferation.[25]Generative Adversarial Networks (GANs): Goodfellow et al. (2014) introduced GANs, enabling sophisticated deepfakes creation.[26]Face recognition technology: Taigman et al. (2014) developed face recognition algorithms vulnerable to deepfakes manipulation.[27]Indian Cyber Law: Kumar et al. (2020) analysed India's cyber laws addressing deepfakes .[28]Digital India Initiative: Sharma et al. (2020) discussed India's digital governance initiatives amidst deepfakes concerns.[29]

Methodology

This research employs a doctrinal approach, analyzing existing laws and policies related to Artificial Intelligence generated content morphing and deepfakes.

[17]Chawla, et al. (2020). Deepfake Detection using Convolutional Neural Networks. IEEE Transactions on Information Forensics and Security, 15, 3313-3323

[18]Li, et al. (2019). Audio-Visual Inconsistencies for Deepfake Detection. ACM Multimedia, 241-249.

[19] Zhu, et al. (2020). Digital Watermarking for Deepfake Detection. IEEE Signal Processing Letters, 27, 133-137.

[20] Kumar, et al. (2020). Deepfakes and Indian Cyber Law. Journal of Intellectual Property Rights, 25(3), 147-156.

[21] Singh, et al. (2019). Copyright Infringement in the Era of Deepfakes. Journal of Copyright Society of India, 36(2), 131-140.

[22]Garg, et al. (2020). Deepfakes and Data Protection Laws in India. Journal of Cybersecurity Law, 1(1), 1-12.

[23] Citron, D. K. (2019). Deepfakes and the Future of Truth. Journal of Criminal Law and Criminology, 109(3), 517-542.

[24]Benkler, et al. (2018). Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. Oxford University Press.

[25] Gillespie, T. (2018). Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. Yale University Press.

[26] Goodfellow, et al. (2014). Generative Adversarial Networks. arXiv:1406.2661.

[27] Taigman, et al. (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification. IEEE Conference on Computer Vision and Pattern Recognition, 1701

[28] Sharma, A., Gupta, B. B., & Alnumay, W. S. (2020). "Digital India Initiative: Challenges and Opportunities in the Era of Deepfakes." Journal of Information Security and Applications, 50, 102393. DOI: 10.1016/j.jisa.2020.102393

[29] Sharma, A., Gupta, B. B., & Alnumay, W. S. (2020). "Digital India Initiative: Challenges and Opportunities in the Era of Deepfakes." Journal of Information Security and Applications, 50, 102393. DOI: 10.1016/j.jisa.2020.102393

This study employed a secondary research approach, utilizing existing literature to investigate deepfakes and morphing in India.

Secondary data was sourced from academic journals, newspapers, books, government reports (Ministry of Electronics and Information Technology), and online databases Google Scholar, A systematic literature review was conducted, searching keywords ("deepfakes," "India," "cyber law") included Articles, Government reports, and publications . Data was categorized into legal, social, and technological aspects.

Limitations

The study's reliance on secondary data may limit generalizability, and publication biases may influence findings.

Individual rights impacted by morphing and deepfakes (Reputation,Privacy, Identity, Dignity)

Morphing and deepfakes technology impacts individual rights in several ways:

Reputation: information is integral part of our life as well in the social life .Artificial Intelligence (AI) is being used in many fields including all types of Media, healthcare, education, agriculture, industry, women power, climate change, security and governance in India. In these fields by using AI, the words, body movements or gestures spoken by one person are relocate to another person. Deepfakes can harm anyone's image. Deepfakes technology can and is being used to create fake news and misleading, false videos. Fake videos can be made by taking photos from any individual's social media profile. MMS of any famous or notable person can be created. Its word can also be changed. Through this, someone can be defamed or even threatened by making a video of them for cheating. These are prepared with such precision that the person seen in the video looks real.[30]The creation of deepfakes content and misinformation in the election can create confusion and manipulation among voters.

Deepfakes videos of rivals can be prepared using AI, which can tarnish their image and affect the perception of voters towards them. This can give rise to the concept of 'Deepfakes Election'. This risk increases due to social media platforms where efforts to maintain fact-checking and electoral integrity are weakened. Deepfakes can also be used to spread automated disinformation attacks, such as conspiracy theories and false theories about political and social issues. A clear example of deepfakes being used in this way is a fake video of Facebook founder Mark Zuckerberg claiming he has "complete control of the data of billions of people", A major threat posed by deepfakes is non-consensual pornography, which accounts for up to 96% of deepfakes on the Internet. Mostly females and married persons are targeted. Deepfakes technology is also used to create revenge porn.Cybercriminals can use deepfakes technology to create scams, false claims, and hoaxes that subotage and weakened organizations.[31]Impersonations of any person , celebrity, politician highlight the potential dangers of uncontrolled AI.There use of deepfakes in elections raises ethical questions regarding privacy/confidentiality, transparency and fairness.[32]

Privacy: Since deepfakes pose greater risks to the individual, people are facing a lot of issues due to morphed and deepfakes contents. Everyone's privacy on social media is now at risk. Unauthorized use of personal data and images raises significantly ethical legal and social concern. It becomes a source Exposure of sensitive information. manipulated content cause anxiety distress, depression and other loss of personal identity.[33]

---

[30] Available at:https://www.bhaskar.com/madhurima/news/deepfake-can-show-truth-as-lie-and-lie-as-truth-know-how-dangerous-it-is-and-how-to-avoid-it-130660117.html(visited on:20 Jan 2023).

[31] Available at: https://www.fortinet.com/resources/cyberglossary/deepfake (visited on:20Jan,2023).

[32] Available at:https://www.drishtiias.com/hindi/daily-updates/daily-news-editorials/deepfakes-in-elections-challenges-and-mitigation(visited on:20Jan,2023).

[33] Maliha Fatima jakir,cover story, Available at:https://auramag.in/deepfakes-are-womens-privacy-at-risk/(visited on:20 Jan,2023).

Identity

Identity theft and impersonation has long lastic and serious effect on individual .this lead and severely Damage person credit. It also leads financial as well as emotional damage to a person. This can creates Confusion and misunderstanding

Dignity

Morphing and deepfakes can levy irreparable harm, causing defamation, emotional distress, humiliation, embarrassment, and loss of self-esteem."

The unauthorized creation and dissemination of deepfakes can lead to devastating consequences, including defamation and emotional trauma. Morphing technology leads to online harassment, resulting in severe emotional disblance and loss of rationality among victims. Morphing and deepfakes pose significant threats to individual, long-term emotional scars. This affects individual personal and professional life. The morphed video and content leads to social isolation .

Other impacted rights:

Freedom of expression: deepfakes and morphing technologies have serious concern regarding freedom of speech and expression. When deepfakes are prevalent people may start to distrust legitimate sources Morphed content leads to distrust in the media and public figure.unexpected public criticism results in the humiliation.

Right to autonomy and Right to security also harm by the deepfakes and morphing.

- Real-life examples**:**

Revenge porn and deepfakes sextortion: 96% of deepfakes are pornographic, with India being significant contributor .India ranks 4th globally in deepfakes porn creation and consumption. In December 2023, Ratan Tata, former chairman of the Tata Group recently debunked a deepfakes video circulating on Instagram. The manipulated clip falsely portrayed Tata Providing investment advice, accompanied by a caption from user Sona Agarwal claiming 'risk-free' investment opportunities. This incident highlights growing concerns about deepfakes technology's potential for misinformation and financial scams.[34]

In January 2024, Sachin Tendulkar, a cricketer, warns his followers those deepfakes videos of fake videos using his image to promote mobile apps.[35]

In 2020, the first time AI-generated deepfakes were used in political campaigning,

Potential consequences: deepfakes and morphing lead to Psychological harms social isolationon,Financial loss, Reputation damage, Loss of trust in institutions

Existing Legal Frameworks and regulatory response

- Defamation law in India belonging to Morphing and deepfakes is under various sections of the Act 2000 Information Technology Act. In particular, Section 66D is related to copying and deception using computer resources or communication devices, carrying three years imprisonment and a fine of a fine of/or fine of ₹ 1 lakh. Additionally, Section 66E talks about violations of privacy, which is related to capturing, publishing or transmitting images of a person in large media, which is through deepfakes, punishable with imprisonment of up to three years or fine of ₹ 2 lakh. The Indian Copyright Act of 1957 also contributes significantly to a role in protecting from unauthorized use of works, allowing copyright owners to take legal action, especially Section 51. In addition, the Ministry of Information and Broadcasting issued an advice on January 9, 2023, urging media organizations to practice the contents of deviation and vigilance of exercise. It is worth noting that while these laws provide some support

[34]

[35]https://www.google.com/search?q=real+life+example+deepfakes+porn+in+india&client=ms-android-motorola.

against deepfakes issues, a lack of a clear legal definition obstructs the referred prosecution. The World Intellectual Property Organization (WIPO) suggests that copyright, in itself, is not an optimal tool against deepfakes due to the absence of copyright interest for the victims. Instead, the victims are encouraged to turn to the right to personal data protection, taking advantage of "right to forget rights" under Article 21. The Government of India has implemented various measures to regulate deepfakes, including censorship approaches, punitive approaches, and arbitration regulation approaches. Censorship Approach

The government sometimes issue orders to intermediaries and publishers to block public access to misinformation. This approach aims to prevent the spread of harmful or false information.

Punitive Approach

This approach imposes liability on individuals or organizations that originate or disseminate misinformation. The goal is to deter people from creating and sharing deepfakes.

- Intermediary Regulation Approach

  Online intermediaries are bound to remove misinformation from their platforms. If they fail to do so, they can prevent liability under Section 69-A and 79 of the Information Technology Act, 2000.

  In the context of defamation laws, India has provisions to address deep-related issues. For example:

  • Identity theft and virtual forgery: Sections 66 and 66-C of IT Act deal with crimes related to computer and identity.

  • misinformation against governments to wage war against 66-F and IT Act 121 sections and Penal Code to wage war against cyber terrorism and government.

  • Destructive language and online defamation: Arbitration guidelines of IT Act and digital media morality code Amendment Rules, 2022, Section 153-A, 153-B, and 499 with 499 of the Penal Code, deal with hatred speeches and defamation.

  • Practices affecting elections: Sections 66-D and 66-F, Section 123 (3-A), 123, and 125 of the IT Act, with 125 of the representation of 125, focus on cheating by individuals and cyber terrorism.

  • Violation of privacy/vulgarity and vulgar literature: Section 66-E, 67, 67-A, and 67-B IT Act to violate the punishment for violation of secrecy, publish or transmit pornographic materials and to paint children in sexually clear acts.

  These laws and rules display efforts to combat India's challenges and protect their citizens from defamation and other harmful consequences.

  In India, the status of the current laws related to artificial intelligence caused Deepfeck and Morping in India

  There are limitations of Indian laws addressing Deepfeck and Morfing: these are:

  • boundaries

  Lack of specificity: There is no specific law in India to deal with the content of artificial intelligence deepfac and morning.

  Jurisdiction Issues: Deepfac and morning can be jurisd by across the border. This is a complex issue and India has no specific law to deal with this type of issue.

Anonymity: it is very difficult to find cyber criminals because cyber space is vast area so due to anonymity it is very Difficult to trace fake content creators.
Technological advancements: Laws struggle to keep pace.
Enforcement challenges: in India there are Inadequate resources and infrastructures are there to deal with the negative impact of Artificial Intelligence.
Free speech concerns: with the using of Artificial Intelligence people are creating fake content of another person. This leads defamtion, misinformation and disinformation among masses. People are doing all this activity either unethical or illegal on the name of free speech and expression so there is problem and concern for Balancing regulation with freedom of expression.

Difficulty proving intent: it is very Challenging to identify the criminals and also to prove their intention.

Case Studies deepfakes and morphing in India

Case studies of morphing and deepfakes-related harms highlight the inadequacy of current laws. Here are notable Indian court cases related to deepfakes and morphing:

- Criminal Cases

State of Gujarat vs. Kishore (2019): Gujarat High Court directed YouTube to remove defamatory deepfakes videos.[36]
Radhika Apte vs. Anonymous (2019): Bombay High Court ordered removal of deepfakes pornographic content featuring actress Radhika Apte.[37]
Delhi Police vs. Anonymous (2020): Delhi Court convicted a person for creating and sharing morphed explicit videos.[38]
State of Telangana vs. Sai Kumar (2018): Telangana High Court addressed fake videos circulating during elections.[39]

- Civil Cases

Shreya Singhal vs. Union of India (2015): the Supreme Court of India declared that Section 66A of the Information Technology Act, 2000, which made sending offensive messages online illegal, was unconstitutional and invalidated it completely. In essence, the court said that the provision was too ambiguous to qualify as a "reasonable restriction" under Article 19(2) of the Constitution.[40]

3. Rajya Sabha MP Priyanka Chaturvedi vs. Twitter (2020): this case Highlighted concerns about deepfakes content.[41]

- High Court Judgments

1. KamleshVaswani vs. Union of India (2017): Delhi High Court addressed online obscenity, including morphed content.[42]
2. Swami Ramdev vs. Facebook (2019): Delhi High Court issued interim order against Facebook/Google /YouTube and twitter for removal of defamatory content.[43]

Recommendations for Reform

[36]State of Gujarat vs. Kishore (2019): Gujarat High Court, R/Special Criminal Application No. 3574 of 2019. - Available at: https://indiankanoon.org/doc/127069293/
[37]Radhika Apte vs. Anonymous (2019): Bombay High Court, Notice of Motion (L) No. 1426 of 2019.
[38] Delhi police vs anonymous (2020)
[39]State of Telangana vs Sai Kumar (2018).
[40] Shreya Singhal vs. Union of India (2015): Supreme Court of India, Writ Petition (Civil) No. 167 of 2012.
[41]Priyanka Chaturvedi vs. Twitter (2020): Bombay High Court, Notice of Motion (L) No. 1426 of 2020.
[42] Kamlesh Vaswani vs. Union of India (2017): Delhi High Court, W.P.(C) 785/2015.
[43]Swami Ramdev vs. Facebook (2019): Delhi High Court, CS (OS) 27/2019.

India's current laws are insufficient including the cyber laws to regulate the deepfakes and morphing so to address this issue here some suggestions and recommendation are there. These are followings:

Regulatory Reforms

- There must be an Act to deal with the Artificial Intelligence generated content deepfakes and morphing .These are the types of cyber crime and comes under the head cyber Defamation. There must be clear and establish laws
- There must be laws related to defamation, harassment, and identity theft to include deepfakes-specific provisions.
- The name of the Act may be cyber crime prevention and reputation protection Act
- The Act should define the all terms relating to cyber crimes and reputation.
- The aim of the Act should to prevent and mitigate the cyber crime and protection individuals and organizational reputation at the online platform
- There should be online platform intermediaries responsibilities to remove the defamatory Content from the online platform within 24 hours.
- Online platform must establish the reporting mechanism for the user to report reputation sabotage and online harassment with immediate action.
- Schools , colleges must include the subject reputation management at online platform in the school curriculum.
- There must be a panchayat cyber redressel committee at the village level consist 7 members having special knowledge of technology 5 from the panchayat including the head. And one member from the administration of district another one from the local concerned police station.
- Any person found guilty of cyber defamtion shall be punishable with imprisonment up to seven year and with fine upto 5 lakhs.
- Any person found guilty against woman and children shall be punishable with imprisonment for 10 years and fine upto 10 lakhs.
- Any person found guilty that causes death of the victim or any family members of the victim due to harm the reputation shall be punishable with life imprisonment or death and fine upto 10lakhs.
- Online platform shall also be liable if they fail to remove defamatory content from the online platform.
- public awareness campaigns should be conducted on deepfakes and defamtion risks.
- A review committee shall be established to review the matters time to time on the local level .
- Identity of Whistle-blower and victim must be keep confidential.
- International cooperation and collaboration should be there to develop harmonized regulations.
- Periodically review and update regulations should be there to address emerging threats.
- There must be a cyber centre in each village of India regulated by the government. Skilled and professional persons should be appointed to solve the problem of people who are victim of cyber crime.

Technological Reforms

- There should be Strong Detection Methods so that anyone can detect deepfakes and morphing through various means and modes such as Audio-visual analysis technics by this one can detect and comapre between the original and fake representation.
- There should be Machine learning-based detection method.

- Human can also evaluate deepfakes and morphing by eye movement blinking pattern, lip movement and speech pattern, facial expression emotions and through the background consistency
- **Educational Reforms**
- Media literacy programs: govt should provide means and mode to Educate citizens on deepfakes identification and critical thinking.
- In the India digital literacy should provide everyone from school to village level.
- Individual should develop emphasize critical thinking and skepticism.
- Governmental, nongovernmental and Local governance should Conduct public awareness campaigns on deepfakes risks.

- **Industry-Led Reforms**
- Industries should establish voluntary industry standards for deepfakes detection and mitigation.
- Industries should Improve content moderation practices.
- There should be collaboration to encourage harmony between tech companies, researchers, and policymakers.
- Business sector should promote transparency in AI-generated content.
- Business sector should hold accountability for Spreading deepfakes.

Research and Development Reforms

- Fund research: government should Allocate dedicated funds includings grants of academic and local levels of gram panchayats for research and should also established interdisciplinary research centres at village levels that brings together experts from law, computer science, Psychology and sociology to study cybercrime.
- Government should provide training regularly to the officials who deals with the cyber crime and capacity building programme to enhance their understanding of cyber crime.

Social Reforms

Users should have Social media literacy before sharing online Content verify its authenticity through reputable sources .users should regularly update operating system , social Media apps and browser to ensure security.

Mental health support: government should Provide mental health support for deepfakes victims' should offer online counselling services such as video or phone therapy sessions to provide convenient mental health support

Conclusion

Morphing and deepfakes technology pose significant risks to individual rights. The existing legal framework and regulatory responses are inadequate,

Multimedia manipulation has been transformed by deepfakes and morphing technologies, yet their nefarious uses present serious risks to people, communities, and governments. The spread of deepfakes content has serious repercussions, such as fraud, harm to one's reputation, and disinformation.

There is a great need to protect reputation privacy, identity, and dignity in the era of technology.