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

DEEPFAKE TECHNOLOGY: THE NEXT GLOBAL CRISIS?

AUTHORED BY - SANKHA BRATA MITRA[1]

ABSTRACT

In the digital age, deepfake technology driven by sophisticated AI and machine learning—has become a double-edged sword. Despite its creative potential for innovation and entertainment, its abuse has presented significant socio-legal issues on a global scale.

*Through empirically recorded instances involving prominent global figures—such as Ukrainian President **Volodymyr Zelenskyy**, U.S. House Speaker **Nancy Pelosi**, technology entrepreneur **Elon Musk**, and internationally recognized celebrities including **Taylor Swift** and **Scarlett Johansson,** this article critically examines the multifaceted ways in which deepfake technology has been weaponized to spread false information, carry out online fraud, and create sexually explicit content without consent. As the technology becomes more advanced and accessible, it is becoming increasingly difficult to distinguish between real and fake content In order to effectively combat the increasing threat of deepfakes, this article emphasizes the urgent need for a multifaceted approach that includes targeted legislation, strong enforcement measures, AI-driven detection tools, and public digital literacy. Given how quickly deepfakes are permeating corporate settings, politics, entertainment, and individual privacy, it is critical to address not only the technological and legal shortcomings but also the moral, constitutional, and societal ramifications. Protecting individual dignity, information privacy, and the integrity of democratic processes necessitates both proactive governance and an informed, watchful public as synthetic media continues to grow in sophistication and scale.*

KEYWORDS: *Deepfake, Sophisticated AI, Technology, Weaponized, Democracy.*

[1] Author is a student at Xavier Law School, St. Xavier's University, Kolkata, India.

 ISSN: 2582-6433

I. INTRODUCTION

The rapid development of artificial intelligence (AI) has become a growing concern for governments, international bodies, and the global public alike. Its expanding capabilities raise critical issues related not only to national security but also to ethics, surveillance, and transparency. In a world already challenged by misinformation and public distrust, AI now offers increasingly sophisticated ways to create content that appears authentic but is entirely false content that can potentially escalate political unrest, incite violence, or even contribute to international conflict.

Deepfakes, which are made with advanced machine learning algorithms and facial mapping technology, can easily insert a person's voice or likeness into text, audio, or video without that person's knowledge or consent. These manipulations can result in incredibly realistic recordings or clips where someone seems to say or do things they never did. Therefore, deepfakes pose major threats to truth, trust, and security globally as they are a potent tool for digital impersonation and the dissemination of false narratives.

II. WHAT IS A DEEPFAKE?

Deepfakes are highly realistic synthetic media, typically videos or audio, generated by artificial intelligence (AI) to manipulate a person's likeness or voice with striking authenticity. Deepfake technology relies on two important breakthroughs in machine learning and artificial intelligence. The first is a neural network. The more information these algorithms are exposed to, the more accurately they can repeat it back.[2] The second is Generative Adversarial Networks (GANs), which essentially combine two neural networks together and make them compete against one another to produce a better final product[3]. It was introduced by Ian Goodfellow[4] and his team in 2014 and they have transformed how computers generate images, videos, music and more. Unlike traditional models that only recognize or classify data, they take a creative way by generating entirely new content that closely resembles real-world data. This ability helped various fields such as art, gaming, healthcare and data science. In this article, we will

[2] Abby MacDonald, The Uses and Abuses of Deepfake Technology, Canadian Global Affairs Institute, https://www.cgai.ca/the_uses_and_abuses_of_deepfake_technology#_ftn6 (last visited June 21, 2025).

[3] Konstantin A. Pantserev, "The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability," in *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Jahankhani, Hamid, Stefan Kendzierskyj, Nishan Chelvachandran and Jaime Ibarra, eds., (Cham, Switzerland: Springer, 2020) 39–40.

[4] Wikipedia contributors, Ian Goodfellow, Wikipedia, https://en.wikipedia.org/w/index.php?title=Ian_Goodfellow&oldid=1295652914 (last visited June 21, 2025).

 ISSN: 2582-6433

see more about GANs and its core concepts[5].

Deepfakes can fabricate scenarios where individuals appear to say or do things they never did. Originally conceived for benign applications like entertainment, film dubbing, or creative artistry, this technology has evolved into a powerful instrument for malicious purposes. Its misuse now fuels disinformation campaigns, defamation, harassment, and sophisticated fraud, posing significant threats to personal reputations, societal trust, and global information integrity.

III. ORIGIN

Photo manipulation was developed in the 19th century and soon applied to motion pictures. Technology steadily improved during the 20th century, and more quickly with the advent of digital video.[6]

The term **"Deepfake"** was coined in 2017 by a Reddit[7] user with the same screen name, who created a subreddit for sharing AI-generated pornography using celebrity images and open-source face-swapping tools. Though the forum was later banned, the term deepfake endured as a label for this emerging form of synthetic media.[8]

The concept of deep faking originated in the 1990s when researchers attempted to create realistic human images using computer-generated imagery (CGI). The "Video Rewrite" program, which was released in 1997, was a significant early endeavor. In order to show someone mouthing the words from a different audio track, the program altered pre-existing video footage of a person speaking.[9] It was the first system to fully automate this type of facial reanimation, and it accomplished this by using machine learning techniques to establish relationships between the subject's facial shape and the sounds they produced in a video.

[5] Geeksforgeeks, Generative Adversarial Network (GAN), https://www.geeksforgeeks.org/generative-adversarial-network-gan/ (last visited June 21, 2025).
[6] Wikipedia contributors, Deepfake, Wikipedia, https://en.wikipedia.org/w/index.php?title=Deepfake&oldid=1296463970 (last visited June 21, 2025).
[7] Wikipedia contributors, Reddit, Wikipedia, https://en.wikipedia.org/w/index.php?title=Reddit&oldid=1296164375 (last visited June 21, 2025).
[8] Gabe Regan, A Brief History of Deepfakes, Reality Defender, https://www.realitydefender.com/insights/history-of-deepfakes (last visited June 21, 2025).
[9] Jeremy Norman's HistoryofInformation.com, Video Rewrite, Origins of Deepfakes, https://www.historyofinformation.com/detail.php?id=4792 (last visited June 21, 2025).

 ISSN: 2582-6433

IV. AI'S EXPANDING GLOBAL FOOTPRINT

New avenues for creativity, entertainment, and customized content production have been made possible by the development of generative AI. The impact of this technology is both widespread. The global artificial intelligence market size was valued at USD 279.22 billion in 2024 and is projected to reach USD 1,811.75 billion by 2030, growing at a CAGR of 35.9% from 2025 to 2030.[10] The rapid advancement of AI is changing not only cybersecurity environments but also the larger digital economy, according to a recent joint fact sheet released by the FBI[11], NSA[12], and Cybersecurity and Infrastructure Security Agency (CISA)[13].

AI-powered visual effects are now a standard feature of high-end productions in the entertainment sector. Deepfake-style technology is being used more and more by Hollywood studios for artistic purposes, like digitally de-aging actors, re-creating historical characters, or filling in scenes with unavailable actors. While many writers and actors are opposing the use of Artificial Intelligence, there are some in the industry who are embracing the technology. In the recently released *Indiana Jones and the Dial of Destiny*[14], the creators, with the help of Industrial Light and Magic visual effect company, de-aged the lead actor Harrison Ford[15] now eighty-two, appears decades younger in a lengthy flashback sequence[16].

Deepfake generation is now available to the general public outside of the film industry thanks to consumer-level applications. Users can bring historical figures or departed family members to life with startling realism by animating old photos using apps like MyHeritage's "Deep

[10] Artificial Intelligence Market Size, Share & Trends Analysis Report By Solution, By Technology (Deep Learning, Machine Learning, NLP, Machine Vision, Generative AI), By Function, By End-Use, By Region, And Segment Forecasts, 2025 – 2030, https://www.grandviewresearch.com/industry-analysis/artificial-intelligenceaimarket#:~:text=The%20global%20artificial%20intelligence%20market,35.9%25%20from%202025%20to%202030 (last visited June 21, 2025).

[11] Wikipedia contributors, Federal Bureau of Investigation, Wikipedia, https://en.wikipedia.org/w/index.php?title=Federal_Bureau_of_Investigation&oldid=1295915545 (last visited June 21, 2025).

[12] Wikipedia contributors, National Security Agency, Wikipedia, https://en.wikipedia.org/w/index.php?title=National_Security_Agency&oldid=1295280000 (last visited June 21, 2025).

[13] Wikipedia contributors, Cybersecurity and Infrastructure Security Agency, Wikipedia, https://en.wikipedia.org/w/index.php?title=Cybersecurity_and_Infrastructure_Security_Agency&oldid=1295048915 (last visited June 21, 2025).

[14] Imbd, Indiana Jones and the Dial of Destiny, https://www.imdb.com/title/tt1462764/ (last visited June 21, 2025).

[15] Wikipedia contributors, Harrison Ford, Wikipedia, https://en.wikipedia.org/w/index.php?title=Harrison_Ford&oldid=1295302552 (last visited June 21, 2025).

[16] Priya Singh, Hollywood going the AI way: How the new Indiana Jones movie de-aged actor Harrison Ford, Business Today, https://www.businesstoday.in/technology/news/story/hollywood-going-the-ai-way-how-the-new-indiana-jones-movie-de-aged-actor-harrison-ford-390481-2023-07-19 (last visited June 21, 2025).

 ISSN: 2582-6433

Nostalgia."[17]

There are also programs that let you perform what's known as a "video-to-video" swap, where the software records your voice and facial expressions and replaces them with the voice and face of a different person.

In addition, audio-based deepfake creation apps known as **deep-voice** software can be leveraged to generate not just speech but emotional nuances, tone, and pitch to closely mimic the target voice[18].

Over the years, many political figures and celebrities have had their voices cloned to fabricate false statements or promote misinformation without their knowledge or permission. Though some have been generated for satire and parody, the potential for the abuse of such manipulations is profound and cannot be ignored.

V. HOW MATURE IS IT?

According to Government Accountability Office[19], a deepfake can be made by anyone with a home computer and rudimentary computer knowledge. There are freely accessible computer programs online that provide instructions for making deepfake videos. Celebrities and public figures are the most frequently used subjects for these applications, which typically still need hundreds or thousands of training photos of the faces to be switched or altered in order to produce a reasonably realistic deepfake. More sophisticated technical knowledge and resources are needed to produce more realistic deepfakes using GANs[20]. Realistic deepfakes have become possible as artificial neural network technologies have developed quickly in tandem with more potent and plentiful computing.[21]

[17] Blackberry Blog, Deepfakes and Digital Deception: Exploring Their Use and Abuse in a Generative AI World, https://blogs.blackberry.com/en/2024/08/deepfakes-and-digital-deception (last visited June 21, 2025).
[18] Kaggle, DEEP-VOICE: DeepFake Voice Recognition, https://www.kaggle.com/datasets/birdy654/deep-voice-deepfake-voice-recognition (last visited June 21, 2025).
[19] Government Accountability Office (GAO), Government Accountability Office, https://www.usa.gov/agencies/governmentaccountabilityoffice#:~:text=Government%20Accountability%20OfficeGovernment%20Accountability%20Office%20(GAO),agencies%20are%20doing%20their%20jobs (last visited June 21, 2025).
[20] *Supra 5.*
[21] Government Accountability Office, Science, Technology Assessment, and Analytics, SCIENCE & TECH SPOTLIGHT: DEEPFAKES, https://www.gao.gov/assets/gao-20-379sp.pdf (last visited June 21, 2025).

 ISSN: 2582-6433

VI. REAL-WORLD CASES: DEEPFAKES IN POLITICS, CYBERCRIME, AND CONFLICT

Across the globe, deepfakes are no longer theoretical threats—they are actively being used to deceive, manipulate, and exploit. From impersonating global leaders to orchestrating financial scams, these examples illustrate the alarming real-world impact of synthetic media.

A. Elon Musk Cryptocurrency Scam

A recent video circulated across multiple social media platforms claimed that billionaire entrepreneur Elon Musk[22] had launched a new initiative offering free bitcoins to anyone who joined the program. The video appeared highly convincing, featuring realistic visuals and audio suggesting Musk's[23] direct involvement. However, the Cyber Crime Wing of the Tamil Nadu Police later issued a public warning, clarifying that the video was entirely fabricated. Authorities revealed that the clip was part of a broader cyber fraud scheme, in which deepfake technology was used to falsely portray the Tesla[24] and SpaceX[25] CEO endorsing cryptocurrency trading platforms, with the intent to deceive users and extract personal or financial information.[26]

B. Political Manipulation During the Russia-Ukraine Conflict

In one widely circulated instance, a deepfake video of Russian President Vladimir Putin[27] appeared on social media, falsely depicting him announcing peace. Around the same time, Meta and YouTube removed a manipulated video of Ukrainian President Volodymyr Zelensky[28], which falsely showed him calling on Ukrainian troops to surrender. Although the Zelensky video was quickly identified as a fake featuring noticeable visual inconsistencies such as a disproportionate head and altered voice it raised serious concerns about the weaponization of

[22]Wikipedia contributors, Elon Musk, Wikipedia, https://en.wikipedia.org/wiki/Elon_Musk (last visited 21.06.2025).

[23] *Supra 21.*

[24] Wikipedia contributors, Tesla Inc., Wikipedia, Tesla Inc., https://en.wikipedia.org/w/index.php?title=Tesla,_Inc.&oldid=1296618697 (last visited June 21, 2025).

[25] Wikipedia contributors, SpaceX, Wikipedia, https://en.wikipedia.org/w/index.php?title=SpaceX&oldid=1296605148 (last visited June 21, 2025).

[26]The Hindu Bureau, T.N. Police issue advisory on fake videos of Elon Musk endorsing crypto sites, The Hindu, https://www.thehindu.com/news/national/tamil-nadu/tn-police-issue-advisory-on-fake-videos-of-elon-musk-endorsing-crypto-sites/article69522022.ece (last visited 21.06.2025).

[27]Wikipedia contributors, Vladimir Putin, Wikipedia, https://en.wikipedia.org/w/index.php?title=Vladimir_Putin&oldid=1296504716 (last visited June 21, 2025).

[28] Wikipedia contributors, Volodymyr Zelenskyy, Wikipedia, https://en.wikipedia.org/wiki/Volodymyr_Zelenskyy (last visited 21.06.2025).

synthetic media during armed conflict.[29]

In response, Zelensky[30] posted a video on his official Instagram account, dismissing the fake video as a "childish provocation." However, the incident validated earlier warnings by the Ukrainian Center for Strategic Communications, which had cautioned that deepfakes might be deployed by Russian entities to mislead Ukrainian citizens and sow confusion on the battlefield.[31] These cases reveal how deepfakes, even when poorly executed, can become tools of psychological warfare and information manipulation during times of crisis.

C. Corporate Deception Through Deepfakes: The Arup Case

The British engineering company Arup[32] was the victim of a deepfake fraud at the beginning of 2024, which resulted in a total loss of over USD $25M.

A staff member was tricked into making 15 transactions totaling HK $200M (nearly USD $26M) to five Hong Kong bank accounts during a video conference call that was attended by deepfakes posing as the company's CFO and other staff members.

The Arup global chief information officer at the time, Rob Greig, told The Guardian:

"Like many other businesses around the globe, our operations are subject to regular attacks, including invoice fraud, phishing scams, WhatsApp voice spoofing and deepfakes. What we have seen is that the number and sophistication of these attacks has been rising sharply in recent months."[33]

D. Deepfakes in Electoral Manipulation

There are countless instances of deepfakes being used to rig elections, such as the AI-generated robocall that impersonated Joe Biden[34] and urged Democrats not to cast ballots in the January Democratic primary in New Hampshire.[35] Because voters are so vulnerable to false information, there has been a persistent push for governments to control the use of this

[29] Jane Wakefield, Deepfake presidents used in Russia-Ukraine war, BBC https://www.bbc.com/news/technology-60780142 (last visited 21.06.2025).

[30] *Supra 27.*

[31] *Supra 28.*

[32] Wikipedia contributors, Arup Group, Wikipedia, https://en.wikipedia.org/w/index.php?title=Arup_Group&oldid=1293476804 (last visited June 21, 2025).

[33] Dan Milmo, The Guardian, UK engineering firm Arup falls victim to £20m deepfake scam, https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video (last visited 21.06.2025).

[34] Wikipedia contributors, Joe Biden, Wikipedia, https://en.wikipedia.org/w/index.php?title=Joe_Biden&oldid=1296455646 (last visited June 21, 2025).

[35] Martin Pengelly & Rachael Leingang The Guardian, Democrats sound alarm over AI robocall to voters mimicking Biden, https://www.theguardian.com/us-news/2024/jan/22/biden-fake-robocalls-new-hampshire (last visited 21.06.2025).

 ISSN: 2582-6433

technology in political campaigns. The Federal Election Commission (FEC)[36] in the United States was urged to regulate the use of artificial intelligence (AI) in political advertisements by the advocacy group Public Citizen. However, in September 2024, the FEC responded by announcing that they would forgo new rulemaking on AI, citing a lack of authority to limit or prohibit the use of the developing technology in federal elections. In August 2024, Reuters reported that Lingo Telecom, the voice service provider that distributed the artificial intelligence-generated robocalls through "spoofed" phone numbers, agreed to pay a USD $1M fine for its role in the Joe Biden deepfake scam.[37]

E. Sexual Exploitation of Public Figures

Global pop sensation Taylor Swift[38] was the subject of explicit AI-generated photos that went viral in early 2024 on sites like Reddit[39], X[40] (formerly Twitter), and others.[41] Before tech companies started taking down the posts, the deepfake content, which was completely made up without Swift's permission, received millions of views. Urgent concerns regarding the sexual exploitation of celebrities through synthetic media were raised by the incident, which caused outrage on a global scale. Global trending hashtags linked to the photos further highlighted the infraction and sparked new demands for platform responsibility and legal protections against non-consensual deepfake material.

F. The Tom Cruise Illusion

In 2021, a series of highly realistic TikTok[42] videos stunned millions of users worldwide by seemingly featuring Hollywood actor Tom Cruise[43] performing everyday activities playing golf, performing magic tricks, and speaking directly to the camera with his trademark charm.

---

[36] Wikipedia contributors, Federal Election Commission, Wikipedia, https://en.wikipedia.org/w/index.php?title=Federal_Election_Commission&oldid=1289151533 (last visited June 21, 2025).

[37] Shannon Bond, npr, A political consultant faces charges and fines for Biden deepfake robocalls, https://www.npr.org/2024/05/23/nx-s1-4977582/fcc-ai-deepfake-robocall-biden-new-hampshire-political-operative (last visited 21.06.2025).

[38] Wikipedia contributors, Taylor Swift, Wikipedia, https://en.wikipedia.org/w/index.php?title=Taylor_Swift&oldid=1295380567 (last visited June 21, 2025).

[39] *Supra 7.*

[40] Wikipedia contributors, Twitter, Inc., Wikipedia, https://en.wikipedia.org/w/index.php?title=Twitter,_Inc.&oldid=1296411307 (last visited June 21, 2025).

[41] Emine Saner, The Guardian, Inside the Taylor Swift deepfake scandal: 'It's men telling a powerful woman to get back in her box', https://www.theguardian.com/technology/2024/jan/31/inside-the-taylor-swift-deepfake-scandal-its-men-telling-a-powerful-woman-to-get-back-in-her-box (last visited June 21, 2025).

[42] Wikipedia contributors, TikTok, Wikipedia, https://en.wikipedia.org/w/index.php?title=TikTok&oldid=1296347145 (last visited June 21, 2025).

[43] Wikipedia contributors, Tom Cruise, Wikipedia, https://en.wikipedia.org/w/index.php?title=Tom_Cruise&oldid=1296085432 (last visited June 21, 2025).

 ISSN: 2582-6433

However, the figure in the videos was not Tom Cruise[44]. The clips were the product of deepfake technology, created by Belgian visual effects artist Chris Ume using a skilled impersonator and advanced AI tools. Ume digitally mapped Cruise's facial features onto the impersonator and used voice-matching techniques to replicate his speech with astonishing accuracy.[45] Uploaded to the TikTok handle "@deeptomcruise," the videos quickly went viral, amassing over 11 million likes and sparking widespread discussion about the capabilities and risks of synthetic media. While the creators insisted their intention was to showcase the creative potential of AI rather than deceive or defraud the incident raised global awareness about how easily public perception can be manipulated using deepfake technology.[46]

VII. RISE OF DEEPFAKES IN INDIA

A. First Instance

Vice reported that Deepfakes entered Indian politics during the Delhi Assembly Election campaign. According to Vice[47], two videos featuring BJP[48] Delhi president Manoj Tiwari[49] disparaging the AAP[50] Government and former chief minister Arvind Kejriwal[51] began making the rounds on WhatsApp in February, just before the elections. Manoj Tiwari[52], the president of BJP[53] Delhi, was featured in two videos, one in Haryanvi and the other in English. According to the report, the original video was of the BJP[54] state unit leader speaking in Hindi; the English and Haryanvi versions were allegedly fake. The report implies that the video was manipulated to edit lip-syncing and give the impression that Tiwari[55] was speaking, rather than being

[44] *Supra 43.*
[45] Rachel Metz, How a deepfake Tom Cruise on TikTok turned into a very real AI company, CNN Business, https://edition.cnn.com/2021/08/06/tech/tom-cruise-deepfake-tiktok-company (last visited June 21, 2025).
[46] Mark Corcoran & Matt Henry, The Tom Cruise deepfake that set off 'terror' in the heart of Washington DC, Australian Broadcasting Corporation, https://www.abc.net.au/news/2021-06-24/tom-cruise-deepfake-chris-ume-security-washington-dc/100234772 (last visited June 21, 2025).
[47] Wikipedia contributors, Vice News, Wikipedia, https://en.wikipedia.org/w/index.php?title=Vice_News&oldid=1287690200 (last visited June 21, 2025).
[48] Wikipedia contributors, Bharatiya Janata Party, Wikipedia, https://en.wikipedia.org/w/index.php?title=Bharatiya_Janata_Party&oldid=1296589563 (last visited June 21, 2025).
[49] Wikipedia contributors, Manoj Tiwari (Delhi politician), Wikipedia, https://en.wikipedia.org/w/index.php?title=Manoj_Tiwari_(Delhi_politician)&oldid=1292408902 (last visited June 21, 2025).
[50] Wikipedia contributors, Aam Aadmi Party, Wikipedia, https://en.wikipedia.org/w/index.php?title=Aam_Aadmi_Party&oldid=1296554618 (last visited June 21, 2025).
[51] Wikipedia contributors, Arvind Kejriwal, Wikipedia, https://en.wikipedia.org/w/index.php?title=Arvind_Kejriwal&oldid=1294426653 (last visited June 21, 2025).
[52] *Supra 49.*
[53] *Supra 48.*
[54] *Supra 48.*
[55] *Supra 49.*

 ISSN: 2582-6433

authentic.[56]

B. RASHMIKA MANDANNA DEEPFAKE INCIDENT

In late 2023, a disturbing deepfake video featuring popular Indian actress Rashmika Mandanna[57] surfaced online, showing a woman dressed provocatively entering a lift, with Rashmika's face convincingly superimposed onto the individual. The high-quality face-swapping initially led many viewers to believe the footage was genuine. However, after the video spread widely on social media, fact-checkers and digital investigators confirmed that it was a manipulated deepfake, falsely portraying the actress in a fabricated scenario.[58]

C. FINANCIAL MISINFORMATION THROUGH DEEPFAKES: THE RATAN TATA INCIDENT

The former chairman of the Tata Group[59], Ratan Tata[60], publicly responded in December 2023 to a deepfake video that was making the rounds on social media and purportedly showed him giving financial advice. Originally posted by user Sona Agarwal, the manipulated video purported to show Tata[61] endorsing a "risk-free" investment plan. The video, accompanied by deceptive captions, took advantage of Tata's[62] reputation and public trust to trick viewers into thinking the investment opportunity was real. Tata[63] clarified on Instagram that the video was completely fake, highlighting the increasing abuse of deepfake technology to enable financial fraud.[64]

D. PRIYANKA CHOPRA DEEPFAKE

As the Indian government intensifies efforts to address the rise of deepfake content, yet another

---

[56] Nilesh Christopher, We've Just Seen the First Use of Deepfakes in an Indian Election Campaign, Vice, https://www.vice.com/en/article/the-first-use-of-deepfakes-in-indian-election-by-bjp/ (last visited June 21, 2025).

[57] Wikipedia contributors, Rashmika Mandanna, Wikipedia https://en.wikipedia.org/w/index.php?title=Rashmika_Mandanna&oldid=1296576102 (last visited June 21, 2025).

[58] India Today News Desk, Rashmika Mandanna deepfake case: Delhi Police tracks down 4 who uploaded video, India Today, https://www.indiatoday.in/india/story/rashmika-mandanna-deepfake-case-delhi-police-action-bollywood-deepfake-videos-2478222-2023-12-20 (last visited June 21, 2025).

[59] Wikipedia contributors, Tata Group, Wikipedia, https://en.wikipedia.org/w/index.php?title=Tata_Group&oldid=1296572989 (last visited June 21, 2025).

[60] Wikipedia contributors, Ratan Tata, Wikipedia, https://en.wikipedia.org/w/index.php?title=Ratan_Tata&oldid=1296253197 (last visited June 21, 2025).

[61] *Supra 60.*

[62] *Supra 60.*

[63] *Supra 60.*

[64] Ratan Tata slams deepfake video that features him giving 'risk-free' investment advice, The Economic Times, https://economictimes.indiatimes.com/magazines/panache/ratan-tata-slams-deepfake-video-that-features-him-giving-risk-free-investment-advice/articleshow/105805223.cms?from=mdr (last visited June 21, 2025).

 ISSN: 2582-6433

public figure has fallen victim. Following incidents involving Rashmika Mandanna[65], Katrina Kaif[66], and Alia Bhatt[67], a manipulated video featuring Priyanka Chopra[68] has surfaced online. Unlike prior deepfakes that involved controversial visual edits, this video retained Chopra's original appearance but altered her voice and dialogue. The fabricated clip falsely depicted her promoting a brand and disclosing her annual income an act intended to mislead viewers and exploit her public image for commercial deception.[69]

VIII. INDIA'S READINESS IN TACKLING THE ISSUE

India currently does not have specific legislation aimed directly at combating deepfake content, leaving a considerable gap in its legal framework. While certain provisions under the Information Technology Act, 2000 such as Sections 66D[70] (impersonation using electronic means), 66E (non-consensual publication of private images), and 67[71]/67A[72]/67B[73] (transmission of obscene or explicit content) cover some aspects of deepfake misuse, they are not equipped to address the broader and evolving challenges posed by synthetic media. Issues like political manipulation, misinformation, and defamation often remain outside the scope of existing laws. Recognizing the growing threat, the Union Government has begun exploring policy reforms, including the possible introduction of deepfake-specific regulations. These may involve stricter penalties, AI-based content detection mandates for digital platforms, and public awareness campaigns aimed at promoting digital literacy and responsible media consumption. According to an article by Chambers and Partners[74] The role of private stakeholders, many of whom are significant investors in artificial intelligence (AI), is critical in implementing preventative measures against deepfakes. Google[75], a proponent of responsible AI

[65] *Supra 57.*
[66] Wikipedia contributors, Katrina Kaif, Wikipedia, https://en.wikipedia.org/w/index.php?title=Katrina_Kaif&oldid=1295168227 (last visited June 21, 2025).
[67] Wikipedia contributors, Alia Bhatt, Wikipedia, https://en.wikipedia.org/w/index.php?title=Alia_Bhatt&oldid=1296009824 (last visited June 21, 2025).
[68] Wikipedia contributors, Priyanka Chopra, Wikipedia, https://en.wikipedia.org/w/index.php?title=Priyanka_Chopra&oldid=1296547194 (last visited June 21, 2025).
[69] India News, Priyanka Chopra Latest Deepfake Victim, Days After Katrina Kaif, Alia Bhatt, NDTV, https://www.ndtv.com/india-news/deepfake-videos-priyanka-chopra-latest-deepfake-victim-days-after-katrina-kaif-alia-bhatt-4639282 (last visited June 21, 2025).
[70] Information Technology Act, No. 21 of 2000, § 66D (India).
[71] Information Technology Act, No. 21 of 2000, § 67 (India).
[72] Information Technology Act, No. 21 of 2000, § 67A (India).
[73] Information Technology Act, No. 21 of 2000, § 67B (India).
[74] Wikipedia contributors, Chambers and Partners, Wikipedia, https://en.wikipedia.org/w/index.php?title=Chambers_and_Partners&oldid=1295988418 (last visited June 21, 2025).
[75] Wikipedia contributors, Google, Wikipedia, https://en.wikipedia.org/w/index.php?title=Google&oldid=1296508468 (last visited June 21, 2025).

 ISSN: 2582-6433

development, is in talks to collaborate with the Indian government to organize a "multi-stakeholder discussion" to address the challenges in dealing with deepfake content. Additionally, Google[76] has partnered with the Indian Institute of Technology, Chennai, to establish a think-tank aimed at formulating policies and guidelines for responsible use of AI technologies.[77]

In the case of *Anil Kapoor Vs Simply Life & Ors. 2023*[78], celebrated actor Mr. Anil Kapoor sought protection of his name, image, publicity, persona, voice, and other attributes of his personality against misuse on the internet. In Mr. Kapoor's case, the defendants used AI deepfake technology to produce derogatory content with his face, personality, and movie dialogues morphed onto the torsos of celebrities to create deepfake images and fake pornographic videos to sell merchandise and services. Delivered by Justice Prathiba M. Singh, the Delhi High Court ruled that the actor's case satisfied the three-prong test for granting an injunction, restraining the defendants from using Mr. Kapoor's name, image, voice, personality, etc., by using technological tools such as AI, machine learning, deepfakes, and face morphing, either for monetary gain or otherwise.[79]

The malicious use of deepfakes often leads to serious reputational harm and psychological distress for the individuals targeted. In the landmark case of *K.S. Puttaswamy v. Union of India*[80], the Supreme Court declared the right to privacy as a fundamental right under Article 21[81] of the Constitution of India, with *informational privacy*, the right to control one's personal data recognized as a crucial element. The Court observed that in the digital era, threats to privacy can emerge not just from the State but also from private entities. It emphasized the need for the Union Government to establish a comprehensive data protection framework that balances individual rights with legitimate state interests such as national security, crime prevention, innovation, and welfare delivery.

[76] *Supra 75*.
[77] Sayobani Basu & Durga Priya Manda of AZB & Partners, Generative Artificial Intelligence – India's Attempt at Controlling "Deepfakes", Chambers and Partners, https://chambers.com/legal-trends/controlling-deepfakes-in-india (last visited June 21, 2025).
[78] Anil Kapoor Vs Simply Life & Ors., CS (Comm) 652/2023.
[79] Times of India Tech Desk, How this 'court case' resulted in Anil Kapoor making it to T0 Time's list of most Influential people in AI, Times of India, https://timesofindia.indiatimes.com/technology/tech-news/how-this-court-case-resulted-in-anil-kapoor-making-it-to-times-list-of-most-influential-people-in-ai/articleshow/113154447.cms (last visited June 21, 2025).
[80] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
[81] INDIA CONST. art. 21.

 ISSN: 2582-6433

This ruling not only permits the State to impose reasonable restrictions on free speech but also places a duty on the government to protect individuals' personal data from misuse. In the context of deepfakes, it underscores the constitutional responsibility of the State to address the harmful effects of synthetic media and safeguard citizens' digital identities and privacy.

Recognizing the gravity of such offences, the *Bharatiya Nyaya Sanhita, 2023* includes specific provisions that can be invoked in relevant cases. Section 356[82] penalizes defamation defined as making imputations with the intent or knowledge that they will harm someone's reputation. Additionally, Section 351[83] criminalizes threats or intimidation intended to cause alarm or compel someone to act against their will. Deepfakes that capture or distribute images of a woman involved in a private act, without her consent or expectation of being observed, fall under Section 77[84], which specifically protects women's privacy and dignity in such situations. In addition to penal law, the *Digital Personal Data Protection Act, 2023* (DPDP Act) offers another layer of protection. It governs the processing of personal data, ensuring that individuals termed as *data principals* retain control over how their data is used. The Act also outlines the responsibilities of *data fiduciaries*, i.e., entities that determine the purpose and means of processing personal data. In the context of deepfakes, the DPDP Act can be instrumental in addressing the misuse of personal images, voices, or other identifiers, offering a regulatory framework for both prevention and accountability.

IX. HOW TO DETECT A DEEPFAKE

In an era where digital content proliferates across social media platforms, messaging apps, and video-sharing websites, AI-generated synthetic media pose a growing challenge. From WhatsApp forwards and viral X posts to YouTube videos and AI-crafted Instagram content, manipulated media can originate from virtually anywhere, making it increasingly difficult to discern reality from fabrication. As deepfake technology becomes more sophisticated and accessible, individuals must remain vigilant and equipped to identify these deceptive creations. Below are effective strategies to detect deepfakes and safeguard against their impact: -

A. EXAMINE VISUAL INCONSISTENCIES

Subtle visual irregularities that become noticeable upon close inspection are frequently how

[82] Bharatiya Nyaya Sanhita, Act No. 45 of 2023, § 356 (India).
[83] Bharatiya Nyaya Sanhita, Act No. 45 of 2023, § 351 (India).
[84] Bharatiya Nyaya Sanhita, Act No. 45 of 2023, § 77 (India).

 ISSN: 2582-6433

deepfakes manifest themselves. Common signs include unnatural facial movements, such as stiff, robotic head turns, mismatched lip-syncing, or irregular blinking. Particularly when the fake face is superimposed on the original video, blurring or visual artefacts may show up around important facial features like the mouth, eyes, or hairline.

In 2022 when a deepfake video falsely showing Ukrainian President Volodymyr Zelenskyy[85] calling on his troops to surrender went viral. While the video shows a passable lip-sync, viewers quickly pointed out that the President's accent was off and that his head and voice did not appear authentic upon close inspection. [86]

B. Analyze Audio Cues

Careful examination of audio cues can also be used to identify deepfakes. Unnatural speech patterns that imply manipulation include robotic intonations, irregular pacing, or abrupt tone changes. Anomalies of background noise, such as sudden shifts in background noise or an audio environment that isn't appropriate for the scene, can also be signs that the content has been altered. When compared to confirmed recordings, voice irregularities such as changes in cadence, accent, or pitch can also be revealing.

A striking real-world example of an audio deepfake scam occurred in 2019, involving a UK-based energy firm. According to *The Wall Street Journal*, the company's CEO believed he was speaking on the phone with the chief executive of their German parent company, who instructed him to urgently transfer €220,000 (approximately $243,000) to a Hungarian supplier. In reality, the voice belonged to a fraudster using AI-generated audio to mimic the German executive's voice, complete with a convincing accent and speech pattern. Rüdiger Kirsch of Euler Hermes Group SA, the firm's insurer, noted that the impersonation was so precise it even captured the executive's unique "melody" of speech. The scammer made three calls first to order the transfer, second to claim reimbursement had occurred, and a third seeking another payment. It was during this final call that the CEO became suspicious, noticing both the lack of reimbursement and the fact that the call originated from an Austrian number, eventually exposing the fraud. This incident illustrates how advanced deepfake audio can deceive even experienced professionals and underscores the importance of verifying audio communications.[87]

---

[85] *Supra 28.*

[86] Jane Wakefield, Deepfake presidents used in Russia-Ukraine war, BBC, https://www.bbc.com/news/technology-60780142 (last visited 21.06.2025).

[87] Deepfakes Expected to Magnify Bank Fraud, The Wall Street Journal, https://deloitte.wsj.com/cio/deepfakes-expected-to-magnify-bank-fraud-c500b0a2 (last visited 21.06.2025).

 ISSN: 2582-6433

C. Leverage Technology Tools

A range of technological solutions can greatly improve detection efforts in the battle against deepfakes. Artificial intelligence (AI)-based detection tools, like Microsoft's Video Authenticator and Deepware Scanner, are made especially to examine videos and images for minute indications of manipulation, such as pixel irregularities or compression artefacts. Furthermore, by determining whether an image or video has been altered or previously published, programs like Google Reverse Image Search can assist in tracking down the source of questionable media. Digital forensic analysis tools that can identify minute differences that might not be apparent to the human eye, like erratic lighting patterns or strange shadow placements, are available for more thorough verification.

D. Promote Media Literacy

Building awareness and critical thinking skills is essential for navigating today's digital landscape, where misinformation and manipulated content are increasingly common. Educating oneself about how deepfake technology works and where it's typically used can make it easier to spot red flags. Always cross-check information with reputable sources, such as verified news platforms or official government statements, before accepting it as fact. Most importantly, maintain a healthy level of skepticism, particularly when encountering sensational, emotionally charged, or unusually positive content. If something appears too shocking or too perfect to be true, it often is.

X. CONCLUSION

The advent of deepfake technology represents a critical juncture in the digital age, where the boundary between innovation and deception is increasingly blurred. Once limited to experimental labs and niche online spaces, deepfakes have permeated mainstream platforms, proliferating across social media, messaging apps, and even news outlets. Their heightened realism and accessibility amplify their potential for harm, driving political misinformation, financial fraud, identity theft, and the erosion of public confidence. From fabricated videos of world leaders to counterfeit celebrity endorsements and AI-driven scams, deepfakes are being weaponized to manipulate emotions, influence behavior, and distort reality. The rapid virality of such content often reaching millions before verification compounds the challenge, making it a pressing global concern.

 ISSN: 2582-6433

In this dynamic digital landscape, fostering media literacy and critical thinking is no longer optional but imperative. Individuals must exercise caution in consuming and sharing content, verify sources diligently, and recognize the psychological tactics employed in digital manipulation. Equally important is understanding one's digital footprint, as personal images and data can be exploited to create convincing deepfakes.

Addressing the deepfake threat demands a unified effort, bringing together policymakers, technologists, educators, journalists, and the public. As artificial intelligence reshapes our world, the collective responsibility to protect truth, trust, and transparency grows ever more urgent. In an age where visual evidence can no longer be trusted, awareness is not merely a defense rather a powerful tool for resilience.