ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/akshat-gupta/666

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 9 & Iss: 1

Research Article

Navigating the Legal Landscape of Deepfake Technology in Indian Political Dimension

Akshat Gupta*

Citation: Gupta A. Navigating the Legal Landscape of Deepfake Technology in Indian Political Dimension. *J Artif Intell Mach Learn & Data Sci 2026* 9(1), 3313-3322. DOI: doi.org/10.51219/JAIMLD/akshat-gupta/666

Received: 23 February, 2026; **Accepted:** 03 March, 2026; **Published:** 05 February, 2026

***Corresponding author:** Akshat Gupta, India, E-mail: akshatgupta232005@gmail.com; saxenarudraksh11@gmail.com

ABSTRACT

This paper, Navigating the Legal Landscape of Deepfake Technology in the Indian Political Dimension, discusses how deepfake technology, powered by Generative Adversarial Networks (GANs), is transforming political communication and creating new challenges to democratic stability in India. Deepfakes distort public perception and spread misinformation, especially during elections, because of their ability to produce hyper-realistic manipulated content. Key incidents, like the use of deepfakes in the 2020 Delhi election, demonstrate the potential for such technology to shape the perception of voters and erode public trust. The proliferation of deepfakes in a pluralistic digital environment with heterogeneity of literacy poses risks of dimensions of significant proportions in India, particularly within regional languages on social media platforms. Presently, the legal framework in India would comprise the Information Technology Act, IT Rules 2021, and Election Commission of India initiatives. The existing paper covers some of the issues with deepfakes, but it lacks full attention to the new threat. Research in this direction proposes legislation that would make malicious use of deepfakes criminal, along with the adoption of preventive measures such as AI-based detection systems, content watermarking, public awareness campaigns, and international cooperation. That, in turn, requires strategies that will save the democratic fabric from pernicious synthetic media effluvia.

1. Introduction

In this quick world, every individual is looking for methods to enhance productivity and lighten his life. The new star of the human labor replacement industry is nothing but artificial intelligence, abbreviated as AI. Students in particular are embracing the promise of this digital enterpriser that has quickly emerged into becoming the favorite reply for all. The setback is that, apart from the hype, most people really don't know much about artificial intelligence. Well, it's like carrying a supercomputer around. Since people still have not known yet what AI can actually do, its true extent has been unknown to many.

According to two American computer scientists, Marvin Lee Minsky and John McCarthy, artificial intelligence occurs when a machine uses its own intelligence to complete a task. Artificial intelligence is intended to mimic human-like qualities such as planning, reasoning, problem solving, speech recognition, thinking, and many other activities; h

While AI technology was originally designed to reduce human effort, it has evolved to the point where it can replicate any person's face, voice, and personality traits. This subset of artificial intelligence is known as Deepfake technology.

Deepfakes are an example of a leap made in artificial intelligence, where highly realistic synthetic media can be created to manipulate video and audio content with ease in this digital age. This technology, based on the principles of Generative Adversarial Networks, may open tremendous possibilities for great innovation use or devastating misuse. GANs, first

introduced by Ian Goodfellow in 2014, consist of a dual-network system: a generator, which is capable of generating fake content, and a discriminator, which determines its authenticity. This technology's the unprecedented ability to change faces, voices, and even the entire body movement is unprecedented, especially about information integrity and trust in public institutions.

First introduced in 2017 by a Reddit user for altering explicit videos, the term "Deepfake" has since expanded to cover a wide array of uses, including political manipulation and commercial or creative purposes. The quick spread of accessible tools like FakeApp has made deepfake technology more widely available, amplifying worries about its potential misuse. The 2018 viral video featuring a manipulated version of Barack Obama demonstrated the technology's ability to twist reality, which raised grave concerns about its impact on democratic systems and public figures.

In a country like India, with over 500 million social media users and with very variable levels of digital literacy. The spread of misinformation through these synthetic media can erode public trust, manipulate political discourse, and prove especially difficult to democracy and individual rights. Recognizing that these risks are urgent, regulatory and legal measures are being explored to curb the proliferation of deepfake technology which in future will going to safeguard public's right.

1.1. Understanding deepfake technology

The word "fake" is put with "deep learning," or deepfakes, and it applies to an advanced AI tool that is an amalgam of highly realistic but synthesized media. In manufacturing audio, video, and images that are actually counterfeited, it depends on the deep learning application, whereas the deep learning techniques, specific to this kind of media creation are GANs. This promotes the elaboration of the production of the synthetic media as GAN neural architecture which is competitive in terms of refinement. The GANs framework consists of two main neural networks. The first one is called the generator, which actually creates synthetic outputs. And the second one is a discriminator, which evaluates the work of the generator by discerning whether the output resembles authentic media. The generator repetitious way adjusts its output based on the discriminator's feedback, leading to very hyper-realistic final results. This cycle just keeps repeating and forces the generator to create outputs so similar to actual footage that makes it really hard to make a distinction between a deepfake and actual footage through perfect mimicry of facial expressions, voice intonation, and even minor movements. Creating deepfakes involves a technical process in its stages, which include very large data collection, training a model, and refinement by furthering deep learning models. The models are first trained on large datasets of target images, videos, or audio clips, which often require diverse samples that capture various angles, lighting conditions, and expressions. After the data is collected, GANs are applied to create initial synthetic media. The generator network begins by producing a basic version of the fake, and the discriminator evaluates its authenticity. Due to continuous iterations, the output improves based on feedback, and one gets a near-photo realistic result. Another technique under deep learning is auto encoders that help in facial manipulation by compressing and reconstructing facial structures, which is particularly very handy in applications like face-swapping. This technique makes it possible for the system to encode a face and to overlay this face onto another person's face in a realistic manner. Open-source DeepFaceLab and FaceSwap give even non-experts who have minimal technical knowledge or expertise the ability to work with deepfake technology at a much lower level of technology. This has democratized the technology, making feasible for anyone with basic computer knowledge and resources to produce realistic media. There are different types of deepfake content, all with their applications and risks: audio, video, and image manipulation. Audio deepfakes, for instance, can mimic a person's voice by analyzing the vocal characteristics in terms of pitch, rhythm, and inflection. The technique needs massive voice samples to model and mimic the speech patterns of the target. Audio deepfakes are very dangerous because they can be used to impersonate people in cases of fraud or identity theft, creating audio clips of people saying things they never said. Video deepfakes probably stand out as the most visually appealing because they utilize GANs and autoencoders to put a person's face on another person's body, simulate facial expressions, and replicate natural body movements. Video deepfakes are especially difficult to detect and have sparked concerns over their potential use for political propaganda, character assassination, and breaches of privacy. Lastly, the manipulation involved in deepfakes is concerning image manipulation; this affects static pictures where techniques are being used to change facial expressions, superimpose features of one person on another, or change age characteristics to age a person forward or backward. While these edits are highly requested for making people's photos more presentable on social media and entertainment, they could be applied to distort information with manipulated images meant to spread false information around the social networks or any other news-gathering agencies.

The technical complexities and accessibility of deep fake technology raise a series ethical and legal questions, especially when such technologies are used in politics, social media activities, or criminal activities. The further advanced the algorithms, the more challenging it becomes to trace them, so regulation and finding a balance between innovation and accountability are questioned within new areas like this one[1].

1.2. Government advisory on deepfakes

Prime Minister Narendra Modi has expressed his stance on the growing deep fake technology on social media, saying these are very realistic images and videos created by AI. Here, he said that even very advanced technology, though it can be a real boon if used responsibly, creates a serious problem if people misuse it, especially for passing on false information. PM Modi urged citizens to check facts about digital content before one accepts or shares it. He spoke about the dangers of deepfakes during the virtual G20 summit on November 22, 2023 and called upon the public to be cautious and critically analyze the content of media houses.

Following these warnings, the government issued an advisory to social media and internet- based services such as WhatsApp, Instagram, Facebook, and Google to comply with IT regulations that would counter misinformation spurred by deepfake technology. Further, emphasis on responsible usage of technology and stricter adherence to IT rules, Former minister Rajeev Chandrashekar said that an advisory is issued to the digital platforms to proactively help in containing the spread

of deepfake content, pointing out the importance of digital authenticity and alerting the intermediaries about their role in minimizing the harm caused by content, including deceptive ads like illegal loan and betting apps[1].

1.3. Global overview of deepfakes in politics

Deepfake have begun to propagate itself across the political landscape of this world, mostly with troublesome implications. These AI-driven manipulations have been employed to mimic the voices and images of public figures in a bid to influence opinions and sow distrust, and in some cases, even intervened in democratic processes. For instance, in the United States, a recent deepfake robocall mimicking the voice of President Joe Biden had misled New Hampshire voters to postpone their voting. Another area by which deepfakes can mislead political participation in different countries is through their belief-though-audit-but-mostly constructed-audio-recordings. On another front, deepfakes that attribute statements to any position of a politician will be seen in almost other nations as it is an aid in influencing the polls by election manipulation. It emerged, for instance, during the Slovak and Indonesian nationalistic election campaigns; deepfakes emerged casting politicians against the will and wish, in protests such as elections. The point here was to bring light to its complexity concerning integrity in an election process.

Public opinion will have a major impact, with deepfakes making inroads in the political setup as an extension of the issue of misinformation. Deepfakes are able to blur lines and make false content seem true, which further causes an erosion of public trust in media and political discourse. It is difficult to make distinctions in this new kind of technology, making most viewers question the credibility of information. As public trust flounder, citizens find it even harder to differentiate between credible and fake sources, which only further disables them from effectively making a well-informed voting choice. The public's lost trust not only weakens political engagement but could also deepen polarization within a community since deepfakes only tend to strengthen existing prejudices and fuel divisive narratives. This creates a loop of distrust where both misinformation gets fed, and the political climate is seriously affected negatively.

To cater this threat to social and political stability, many countries have started regulatory and legislative measures. In the United States, lawmakers are specifically looking at policies to counter the misuse of AI-driven content, including deepfakes, before they are used to subvert the process of any election cycle. The Digital Services Act of the European Union focuses on online misinformation through the encouragement of digital platforms to identify or remove deepfakes and penalizing circulation without proper disclosure. On this issue, China has shown its very hard stance by making requisition to the makers of deepfakes to declare it to be artificial, thus protecting the public from deception. Japan is also reviewing legal frameworks to contain the negative power of deepfakes to affect social stability. Thus, these global developments become a sign of growing concern towards tighter control to limit destructive powers of deepfakes in opposition to public perception, democracy, and social integration[3].

1.4. Cases of deepfakes in political settings worldwide

Deepfakes are gaining popularity in the political fields of the world as the video, image, and audio clips are manipulated and are sent to the leaders of political campaigns and the electoral processes. For example, the recent case in the United Kingdom was that of the image of Former Prime Minister Rishi Sunak that had gone viral and brought doubts about his stand on a number of key issues. The same deepfake can mislead the public with full confidence, creating suspicion and spreading false narratives. For instance, in the United States, deepfakes have appeared in the elections whereby politicians are shown under manipulated or even totally manufactured conditions to influence public opinion and voters' decisions over who to vote for, having projected that the politician possesses certain ideas or conducts overestimating them. Such occurrences were not witnessed only in the Western world, and the AI-generated videos wherein a politician is seemingly unconditional approval of controversial matters and posted online with a focus on changing the public view on those leaders. With advanced deepfake technology, these media artifacts become harder to detect and increase the potential for damaging reputations, influencing elections, and deepening political divides.

The impact of deepfakes on public perception and misinformation is highly significant because synthetic media can mimic real individuals very closely, which undermines the public's trust in content. Deepfake videos and images spread out so fast that it blurs the line between reality and fiction, making it difficult for the public to know what is real and what is manipulated. This makes an environment that is ready for misinformation, where the public may easily be misled by distorted representations of political figures. Such misinformation not only misleads but also erodes the credibility of legitimate news sources and amplifies general skepticism. This impact on public perception alters opinions and leads to false narratives through which decisions will be taken, hence directly going against the democratic process. Next, ongoing exposure to deepfakes desensitizes persons to question credible information; hence deepfakes lead to lowered trust in media sources as well as other official communications relating to it.

In response to this newly-emerging threat of deepfakes, many countries began building regulatory frameworks addressing deepfakes, particularly about political integrity. The EU is utilizing its Digital Services Act to set rules requiring online platforms to take the initiative against disinformation, which is a form of deepfakes. This law has established statutory law for identifying and monitoring deepfakes that could potentially cause political instability. In the United States, California and Texas the government have already enacted laws prohibiting malicious use of deepfakes, especially during election time, since it is a criminal offense that aims to deceive voters. China has also become very strict in handling synthetic media by compelling all digital platforms to explicitly label what kind of media is being distributed to prevent possible misuse of deepfakes, and South Korea is studying a similar approach. In essence, these are national laws that can be considered the first efforts in rectifying this anomaly; however, global implications regarding the threats from deepfakes require joint efforts from all nations towards arriving at some form of common standard. Regulations like these do not fight only against the wrong uses of deepfake technology but protect the integrity, openness, and safety of elections everywhere in the world[4].

1.5. Deepfake technology in Indian politics

1.5.1. The Delhi BJP Incident (2020): During the Delhi legislative assembly elections of 2020, the Bharatiya Janata

Party (BJP) etched its name in history by first experimenting with the use of deepfake technology to heighten voter outreach. It is one of the earliest recorded cases in the Indian political scenario. Through the use of deepfake software, the BJP facilitated their party leader, Manoj Tiwari, to address campaign rallies in Haryanvi and English, aside from his mother tongue of Hindi by digital manipulation of videos. This innovative approach enabled the party to reach a much more multilingual and diverse audience-audience, in essence, who could understand it in their own local dialect. But this move made quite a lot of dust and brought forth some healthy debate and ethical issues of its own. Even though the BJP might have hoped to leverage deepfakes to reach more people, the use of synthetic media in a political campaign did, by default, call into question issues of transparency and authenticity as well as risk.

According to the critics, it may create public deception due to the presentation of manipulated digital content as real and blur the lines between the actual and manufactured media. This is an important issue in current discourses of politics that a very thin line exists between technological innovation and moral responsibility. In fact, clearer guidelines and public awareness on deepfakes used in electoral and political context will be more helpful for better use.

1.5.2. The rashmika mandanna incident (2023): Such has been the case with 2023, when the Indian actress Rashmika Mandanna became the latest victim of this deepfake technology. Non-political in nature, controversy and outrage associated with the circulation of a video about the actress made it discussable in the Indian Parliament on the need for regulating this synthetic media. The video spread like wildfire across the media platform, damaging her reputation and giving an emotional distress to the actress within a matter of hours. Such incidents give evidence to the deeper threat deepfakes pose not only to public figures but to individuals and society as a whole. Since technology is advancing in a highly fast and accessible manner, deepfake misuse and exploitation particularly among women and public personalities will surely surface because they are victims most of the time maliciously used by these ill-willed individuals.

Hence, this incident brought strong appeals to the members of parliament as well as other various stakeholders to reform the current law against the increasing malpractices of deepfakes. The Rashmika Mandanna case provided an urgent call for discussions on the policy about how to control the usage and distribution of deepfakes in India. Lawmakers and legal experts felt there is a need for an adequate legal framework that can address issues related to ethics, privacy, and security in the realm of synthetic media. It further generated discussion on the control social media platforms should exercise on harmful content and how the involvement of technological solutions such as AI-based detection tools may identify and flag deepfakes before they hit massive audiences. All said, the incident pointed towards the urgent need for extensive legislations that could, from day one, protect one and all against the abuse of the deepfake technology while further paving the way forward towards future regulatory efforts of upholding digital integrity and people's rights in the era of media manipulation through AI technologies.

1.6. Spread of political misinformation

Deepfakes tend to propagate through channels like WhatsApp groups and social media, especially in regional languages, thus making these channels potent amplifiers of misinformation. Rapid and widespread propagation across these networks might delay the detection and removal of this false content, which allows deepfakes to spread unchecked and significantly shape public perception. Deepfake technology presents serious challenges for elections in the context of affecting the electoral process and democracy. For example, deepfakes can be used to alter voter perceptions about candidates through the creation of false narratives that may influence the opinions of voters based on fabricated content rather than actual information. Such fake media pieces may also disrupt campaigns, especially when released during the last stages of an election, as they may spread damaging disinformation about candidates right before voters go to the polls. This may end up having a cumulative impact on public trust as it is contributing to increasing distrust about whether political content is real or created. This increases the vulnerability of voters, who can no longer discern differences between real and fabricated news. What this does is affect not just the fake sources but real news sources too because the credibility of what is true becomes suspect.

Recent elections have seen a spate of AI-generated deepfakes secretly used, causing immense challenges to both the authorities and voters to know what is real and what is not. Deepfake manipulation can pose a serious threat to democratic processes since the spread of such deepfakes will undermine the credibility of political communication. As a result, the ECI has taken up several measures to counter these risks. Among these, the statutory duty of disclosing any potential use of AI-generated contents by political parties is included. Besides this, political election advertisements are also authenticated before the public access them. ECI installs quick response teams that strictly monitor the diffusion of false information during an election phase. These teams proactively make efforts to detect and respond accordingly to any deepfake-related incidence. Through this, it would strive for the constraint of spreading wrong information immediately. All these steps collectively aim for the prevention of deepfakes from disrupting the smooth process of elections, promotion of transparency and trust among political communication[5].

1.7. Recent high-profile cases

1.7.1. Kejriwal BJP membership video (2024): A deepfake video of Delhi Chief Minister Arvind Kejriwal joining the Bharatiya Janata Party. Prepared by advanced deepfake technology, the video had passed all the checks as the highest quality that has misled the many into thinking that the video was true and so forth and created waves in society due to confusion and speculative issues that people raised, even when discussing it in discussions or on social media forums. This deepfake's realism was such that both AAP and BJP were quick to deny it saying the video is fake and has been done with a political agenda. It was a proof of the new risks presented by deepfake technology, especially to high-profile political figures and electoral integrity.

Deepfakes can be highly powerful tools for disinformation since they are capable of creating really very realistic visuals and audio, and with that capability, they can even be great weapons to change the perception of society and make the people vote against their conscience. The video of Kejriwal was merely an example where deepfakes can easily be exploited to create political

mileage and also there is an urgent need of proper mechanisms for detection and proper regulatory frameworks with which to make people more conscious of such spread of forged contents. Deepfakes are a very dangerous threat against democratic processes as they become more available and sophisticated. They could have extreme election cycle implications, as brief periods of misinformation might be enough to change the course of public opinion and destroy reputations. This case illustrates an important example of deepfake technology affecting politics: manipulation of digital content is entering mainstream political discourse very easily and thus needs to be understood with ethical considerations and, in some ways, policy intervention.

1.7.2. Congress party leader video manipulation (2024): In fact, one case emerged before the 2024 general election campaigns during which clips involving leading Congress party members showed the manipulation of video in altering the speeches that those people made. Altering included using deep fake technology while advancing editing capabilities for producing such altered output which resulted in making a distorted effect instead of the intended. These manipulations were critical and strategically released during the time of election, when the political tensions were at their highest, along with the level of sentiment of voters. It is thus deduced that these doctored videos tried to taint the name of the Congress Party and made voters mislead themselves on the wrong narrative around the party's agenda and policies. This case pointed to the vulnerability of political discourse to deepfake technology and underscored how manipulations of this kind could affect the democratic process in the most serious ways. Public perception influenced by these false representations has the potential to swing the results of elections and to subvert the integrity of the political landscape.

1.8. Earlier precedent-setting incidents

1.8.1. Delhi election campaign (2020): Deepfakes were used in Delhi Legislative Assembly election in the year 2020 and created a first in political campaigns. For the first time in Indian politics, it was the Bharatiya Janata Party (BJP) that used content generated by AI to alter the speeches of a leader into various regional languages while releasing multiple campaign videos. While doing so, the party intended to reach out across more voters by delivering its messages in tongues familiar to several communities. In a city like Delhi, it stands for one of the most diversified demographics in the country. However, many ethical and legal issues raised were a challenge for the campaign itself. Many questions were also raised against the authenticity of the political messages and whether the public opinion is being manipulated. This incident sparked a national debate over the responsible use of AI and synthetic media in politics. The incident also required immediate clear regulations governing the use of advanced technologies in political campaigns to avoid misuse and ensure the transparency of political discourse. This was a turning point, focusing attention on broader implications of emerging technologies in democratic processes.

1.8.2. The rashmika mandanna case impact: One of the most infamous deepfakes recently used actress Rashmika Mandanna's image without her permission and brought a national controversy by leaking the video. Since it was manipulated with leading digital tools, this video sparked so much outrage throughout the country in issues regarding privacy invasion as well as the misuse of ethical technology. This incident did not only have an impact in the entertainment industry but led to a much wider talk about the dangers of deepfake technology in many spheres, especially in politics. The public outcry and attention by the media in the case led lawmakers to recognize growing threats of such digital manipulations. This is what happened and soon the whole event had become the momentary impetus for much legislation related to the issue of addressing the abuse of deepfakes, and more pointedly with elections as the leading cause. Then the occurrence brought to light an even more pressing need for regulatory controls that would prevent deepfakes from convincingly swindling voters into not voting in certain ways precisely because they were deceived initially. This indirectly nudged the political leaders to think specifically about guidelines in handling manipulation of digital content to avoid compromising the integrity of the two: personal privacy and the public discourse.

1.9. Spread of political misinformation through deepfakes

The spread of political misinformation through deepfakes is thus considered an alarming issue where social media channels are becoming an important conduit for the exchange. WhatsApp, widely used for spreading deepfake videos, does not provide enough scope for monitoring or regulating content because of its end-to-end encryption facility. This encryption feature ensures that deepfake videos will spread quickly within a group chat, and tracking who created the content and determining whether it is accurate may become nearly impossible before its content reaches a wide audience. Other platforms, like Facebook and Twitter, add fuel to the fire, where algorithmic engagement prefers to give priority to sensational or high-engagement content. In this regard, Instagram is also emerging as an important area, for the reason that it holds much relevance to visual content, especially video, which would be a proper ground for deepfakes and other kinds of visual disinformation.

The impact of deepfakes in a multilingual country like India is more pronounced when they have been prepared in regional languages. Fact-checking sources are often limited for these languages, which makes it slightly harder to counter convincingly. Moreover, vernacular content is more trusted locally, especially in rural or linguistically isolated regions. Thus, deepfakes that are generated in regional languages are more likely to be believed and shared without proper scrutiny, which will maximize their potential impact on the political opinions of these communities.

Several factors that enhance deepfakes have led to making them extremely powerful weapons in the sphere of political disinformation. These factors include technological advancement of synthetic media at a pace which is increasing day by day. Quality of deepfakes has improved exponentially, and they are difficult to distinguish between authentic and fake footage. The cost of creating deepfakes is decreasing while tools to create them have become readily available. Because of these developments, current technological progress is no longer in the hands of high-ranking political actors but even more on the hands of the lower resource individuals who can easily produce convincing deepfakes. This makes political stability extremely vulnerable because it leaves fewer financial and technical barriers in the way of evil-doers to manipulate public opinion.

Social dynamics play an important role in spreading deepfakes. Videos are usually a success in the social media arena because, through the echo chamber effect, one is more engrossed

in content believed. Deepfakes mainly exploit confirmation bias to engage with manipulated content emotionally charged with beliefs that drive polarized political discourse. The emotional response evoked by such videos, many of which are sensationalistic in nature, puts a viewer in a position where he might share the content before validating its authenticity. Such action creates a self-sustaining cycle where deepfakes continue to proliferate rapidly, sowing disarray and confusion in the political landscape[6].

1.10. Impact of deepfakes on Indian democracy

Deepfakes are a challenge to the conduct of public discourse, particularly in Indian politics, where there is an increased consumption of media and strongly contested political campaigns. Where there is increased media consumption and strongly contested political campaigns, the reality could be tampered with to mislead voters. Deepfakes could create fake stories surrounding any candidate or a political party with the capacity to create massive influences over people's opinions. For instance, sharing false video footage where politicians involved in such activities get people losing full trust and confidence in such individuals to such an extent that even at the polling booths, people might end up electing a different party as a protest. As voters increase their reliance on digital channels for information, the prospect of encountering manipulated content will increase, raising concerns about the quality of informed decision- making within a democratic society.

Moreover, deepfake technology threatens to greatly destabilize India's political environment. Overall public mistrust in news sources can make polarization increase among voters, leading towards a polarized electorate with the potential to create discord among various political groups and may lead to violence. As such, it is probably going to be very critical during elections that are more emotive. The application of deepfakes as tools for misinformation campaigns makes the political terrain even more complicated because it disrupts democratic processes through confusion and fear among citizens. When people cannot tell what is real from what is fabricated, then the ability to meaningfully engage in democratic practices is considerably affected. This loss of trust not only saps confidence in media but also erodes confidence in political institutions, thus jeopardizing the stability of governance and further diluting the legitimacy of electoral outcomes.

The psychological and social impacts of deepfakes are much more profound than the immediate electoral consequences. They create a culture of fear and mistrust within society, as people face the reality of tampered content. Increasing fears of fake news and media have a result of people losing interest in political processes as citizens begin to lose faith in being able to tell reality from fiction. Socially, the expansion of deepfakes is likely to highlight already entrenched biases and prejudices in a community because information campaigns aimed at people leverage societal fault lines to cause social division. The outcome would be a fissuring of the social fabric that presents dangers not only to electoral integrity but to the broad cohesion of the society at large.

These interventions are profound avenues for novelty and expression, yet implications are deep into the democratic set-up for India. Tackling such problems demands strong legalese and active moves to support the management of democratic processes. Similarly, media literacy may be improved among citizens so as to encourage them to seek their places in a totally digital but manipulated information domain[7].

1.11. Legal and regulatory landscape in India

The proliferation of deepfake technology has raised significant issues concerning ethical and legal measures all around the world, as in the case of India. These deepfakes, using advanced AI algorithms that convincingly create audio, video, or images of someone making or saying things they never did in their entire lives, prove a gigantic threat to politics and the social landscape altogether. These hyper-realistic manipulations can very easily deceive the public, smear reputations, and rewrite political narratives in ways that can easily turn deepfakes into an even more dangerous instrument for spreading disinformation within India's kaleidoscopic political scene.

Indian lawmakers and regulatory bodies have realized the dangers involved in the misuse of deepfakes but still do not have specific, comprehensive legal frameworks tailored to combat these issues. Instead, various provisions under existing laws are being applied to deal with the deepfake issue. The Information Technology Act, 2000, combined with the Indian Penal Code and Copyright Act, provides some legal grounds against deepfakes in categories such as cyber harassment, defamation, and intellectual property infringement. However, these measures are limited because they were not made with AI-driven, highly sophisticated digital manipulations in mind.

Indian practice regarding the regulation of deepfakes continues evolving, with demands for targeted legislation becoming more vocal. Given the growing threat, there is an increasingly urgent need for new specialized, updated legal tools to protect the integrity of political discourse and personal reputations in India.

1.12. Laws present in India

1.12.1. Information and Technology Act[8]: Section 43A of the Information Technology Act mandates compensation for any negligence in implementing adequate security measures, leading to wrongful loss or gain.

Section 66E addresses privacy violations, making it a punishable offense to capture or distribute images of private areas without consent, with penalties of up to three years in prison or a fine up to two lakh rupees.

Sections 66D and 66F further target online crimes, specifically impersonation-based fraud and acts of cyber terrorism, which involve exploiting weaknesses in digital systems to disrupt or damage critical infrastructure.

Section 67 prohibits sharing obscene material online, with fines and imprisonment of up to five years for repeated offenses.

1.12.2. List of IT rules, 2021 in collaborations with the ministry of electronics and information technology ("MeitY"): The Government of India aims to ensure that the internet in India remains open, secure, reliable, and accountable to all digital citizens. To support this, the Ministry of Electronics and Information Technology (MeitY) frequently engages with various stakeholders through consultations like the Digital India Dialogues (DID), focusing on the challenges of misinformation and deepfakes. Upholding a zero-tolerance approach towards unlawful content, MeitY released an advisory on December 26,

2023, directing all intermediaries to fully align their terms of use with Rule 3(1)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021). Key provisions of this advisory include:

- Ensuring users on social media platforms refrain from posting prohibited content as per Rule 3(1)(b).
- Communicating prohibited content guidelines at initial registration and regularly upon each login.
- Informing users of potential legal consequences under the IPC, IT Act, and other laws for violating Rule 3(1)(b).
- Requiring intermediaries to report legal violations to law enforcement agencies.
- Directing intermediaries to identify and remove misinformation, including deepfakes.
- Enabling users and victims to report Rule 3 violations through accessible in-app options.
- Requiring intermediaries to comply with Grievance Appellate Committee orders and publish compliance reports.
- Banning advertisements for illegal loans and betting apps.
- Warning intermediaries that non-compliance may result in losing liability exemptions under section 79(1) of the IT Act.

To ensure safe internet practices, MeitY actively monitors intermediary compliance with these directives. As part of public consultations, MeitY also reviews the need for new or revised legislation to reinforce an open, safe, and trustworthy internet.

The IT Rules, 2021, which took effect on February 25, 2021, and have since been updated in October 2022 and April 2023, place specific obligations on intermediaries. These include:

- Prohibiting eleven types of content under Rule 3(1)(b).
- Mandating platforms to restrict their terms of use against prohibited content, including misinformation and deepfakes.
- Ensuring that flagged content is removed or access-disabled within 36 hours upon receiving court or government orders.
- Complying with identity verification requests from law enforcement within 72 hours as per Rule 3(1)(j).
- Ensuring complaints about prohibited content are resolved within 72 hours, with specific content, such as nudity or deepfakes, removed within 24 hours under Rule 3(2).
- Enabling significant social media intermediaries to identify the first originator of flagged content related to national security or serious criminal matters under Rule 4(2).

Additionally, the government has set up Grievance Appellate Committees on the IT Rules platform to allow users to appeal intermediary decisions regarding legal violations. The Ministry of Home Affairs also operates the National Cyber Crime Reporting Portal and a toll- free helpline (1930) to assist citizens in reporting cybercrimes.\

1.12.3. Bharatiya Nyaya Sanhita, 2023[9]: It introduces several provisions applicable to deepfake-related cybercrimes, including criminal defamation, incitement against public order, virtual forgery, and the sale of obscene material under sections like 354, 195(1), 145, 316(1), and 292-293.

1.12.4. The Indian copyright act (1957)[10]: Section 51, penalizes the unauthorized creation and distribution of infringing copies, supporting action against deepfakes involving unapproved use of copyrighted material.

1.12.5. Representation of the People Act (1951)[11]: Sections 123 and 125 of the Representation of the People Act (1951), may apply, though current laws are limited in addressing the nuances of deepfake technology. The rapid pace of digital advances, the global nature of the internet, and complex intent-driven issues highlight the need for more comprehensive legislation against deepfake misuse.

1.13. Role of the election commission of India and other agencies

The ECI has now emerged as a vital agency that can be used to challenge the deepfake threats. It is a scenario that appears particularly pertinent now as deepfakes pose an existential threat to the very fabric of the democratic process. Deepfakes include AI-generated manipulations of video and audio content that may well create highly convincing false narratives or impersonations, likely to mislead voters. In this regard, the ECI has taken a multi-pronged approach. First, it collaborates with social media platforms and technology companies to identify and remove deepfake content rapidly. Through this collaboration, misleading media can be taken down even faster, especially during an election period when the impact of misinformation can be amplified. To better strengthen these efforts, the ECI works closely with MeitY and law enforcement agencies to enhance regulatory frameworks. Such a partnership will make social media service providers more accountable in their algorithm to detect and eliminate AI-generated falsehoods.

Besides these regulatory measures, the ECI has upped its ante on voter education. The Commission undertakes public awareness campaigns through which citizens are made aware of the dangers of deepfakes and the need to verify the information before accepting it as authentic. In this regard, the ECI encourages critical digital literacy among voters in order to be able to distinguish between real and manipulated information, thus limiting the influence of deepfakes on public opinion. In addition to the direct grievances of the people, the ECI has also provided grievance redressal mechanisms under which the public can complaint against misleading contents including deepfakes. Such complaints may be filed online through ECI's portal, streamlining the reporting process and making quick response action possible. These initiatives are in the greater pursuit of electoral transparency and ensuring the voting process is free and fair, all in the wake of ever-changing AI technology.

Together, these approaches to regulation and education with grievance redressal have been well-suited to ensure that all regulatory and law enforcement apparatuses work towards protecting this precious electoral process from the attack by deepfakes. Altogether, it represents the robust commitment of the ECI to protecting democratic ideals and limiting the impact that technology-facilitated distortions of facts might otherwise undermine India's electoral processes and outcomes[12].

1.14. Technological countermeasures and detection

The deepfake technology continues to develop, and a detection technique would need an update at regular intervals just to be one step ahead of the development that's going on. As of current times, the best method to recognize deepfakes would actually be a mix of a number of detecting techniques coupled

with exercising caution when approaching apparently over-polished content, and a few of the common techniques applied to recognize deepfakes include:

Visual Artifacts: Deepfakes often have visible visual artifacts such as unnatural facial movements or blinking. Such artifacts may be due to deficient train data or the very nature of deep learning algorithms that usually have a compromise between realism and efficiency of processing. Some examples include inconsistent facial expressions, not in sync eye blinking, and discrepancies or omissions of details in the background.

- **Audio-visual mismatches:** Audio-visual mismatch may exist in some few deepfakes; there is thus evidence of tampering. Lip movements of the actor may not be consistent with the audio, or conversely, background noises can be seen in the audio but missing in the video. These will be potential indicators of tampering.
- **Deep learning-based detection:** These algorithms, including deep neural networks, are trained on enormous datasets, comprising authentic and manipulated images, videos, and audio. They detect deepfakes and learn underlying patterns and artifacts of fake content. When sufficiently trained, the algorithm then rates new media to raise awareness and flag it for human experts to investigate further.
- **Forensics-based detection:** These methods look into various aspects of an image or video, such as geometric relationships between facial features, to check if content has been manipulated. They can be effective in detecting deepfakes, but certainly not foolproof. Just as the creators of deepfakes advance their methods toward creating increasingly realistic forgeries, so too must forensic techniques adapt. Further forensic analysis might include analyzing audio and video data patterns and inconsistencies in lighting and shading.
- **Multi-model ensemble:** This tends to increase the reliability of results as compared to individual models because it integrates various detection methods' different outputs such as geometric facial features evaluation and observation of lighting inconsistencies.

Using a mix of these approaches, detection can be enhanced more effectively against deepfakes; yet with advancements made in deepfakes every day, improvement of their detection methods never ceases.

1.15. Role of news media in identifying and debunking deepfakes

Deepfake technology is a challenge to media, politics, and public trust in India. During elections, deepfakes can manipulate political narratives by spreading disinformation or false portrayals of candidates, which undermines democratic processes and can sway public opinion based on fabricated evidence. As detection continues to evolve, the onus is great on the government and stakeholders of India to ensure that deepfake detection improves by investing in research and development. The media outlets, with the aid of detection technologies, find and shed light on the manipulated content, even though the fight is tough. Social media too, which are the main highways for instant information dissemination, need to dedicate enough resources toward flagging or debunking deepfakes. Educating the public about deep fake recognition and reinforcing fake news detection is another very important strategy to mitigate the effects of this technology.

Detectors must be accompanied by the active role of the media in detection and public education in order to counter the challenges presented by deepfakes. It starts with investing in advanced technologies of deepfake detection. Media organizations can partner with technology companies and academic institutions to adopt AI-based tools that can rapidly identify the manipulated content. Leverage these detection systems to expose made-up media as quickly as possible so that the misinformation cannot gain any traction.

Media houses should also be proactive in fact-checking and collaborate with misinformation combat alliances to enhance the verification processes so they can provide their audiences with the right information and bust these false narratives quickly.

Public awareness campaigns are also critical. The awareness campaigns are meant to enlighten audiences on recognizing deepfakes, understanding the risks of such realities, and media literacy to enable people to learn to distinguish between authentic information and manipulated content.

Lastly, clear regulatory guidelines that favor responsible media practices can standardize responses to deepfake challenges and thus lead to overall public trust in media[13].

1.16. Public awareness campaigns and educational efforts

Public awareness programs and education are very crucial as they will help deal with the emergence of deepfakes in the Indian political setup. The first area includes public education programs to advise citizens about the presence of deepfakes and risks associated with them. Programs can be held under traditional media, social networking sites, and community awareness programs to educate the person on how to detect deepfake content. These campaigns can use past examples of deepfake cases to illustrate the direct influence such events have on the perception of public and electoral processes integrity.

In addition, educational programs should target the public, building media literacy. Through workshops and school-based programs, people can be prepared with basic digital literacy so that citizens can critically look at information and verify the authenticity of the information provided. Engagement of technology experts and media houses in these educative efforts ensures that the citizenry is updated and receives tools to detect deepfakes.

The cooperation between government authorities, NGOs, and schools will lead to more general public awareness campaigns concerning opportunities and dangers presented by deepfakes. A multi-level approach from the various sectors can be built upon to build a community that is strong and resistant to false information while having confidence in trusted information sources[14].

1.17. Influence of social media platforms in spreading or countering deepfakes

Thus, online platforms function in two outstanding roles simultaneously: proliferation as well as mitigation towards deepfakes within Indian political spheres. On one hand, there is evidence of rapidity in their deepfakes propagations for purposes of influencing voter perceptions through disinformation campaigns. During political events, manipulated media can be published widely and rapidly on websites such as WhatsApp,

Facebook, and Twitter, a challenge to users in knowing what content is authentic from what is fabricated. To this extent, even reports have surfaced that political parties are now using deepfakes in media to create an avenue for reaching wider audiences than ever before as they attempt to influence opinions and further discredit opponents with the same technology.

However, social media also plays a central role in fighting deepfakes. This would include developing an AI-driven algorithm to be possibly used for the detection of a manipulated content, partnering up with independent fact-checking organizations, and holding several educational campaigns that should be focused on the user's awareness about any form of manipulation being done online. Moreover, these platforms are always subjected to pressure by governments and civil society to become more stringent in policies adopted and speed up the deletion processes of misleading content during special periods like elections.

As countermeasures, most advocates call for stronger legislative and technological interventions to ensure deepfakes in no way undermine democratic processes in India[15].

1.18. Ethical dilemmas in the creation and use of deepfakes

Deepfake technology launches a highly multifaceted suite of ethical problems, especially in its creation and deployment within influential spheres like politics. Primarily, it raises serious ethical questions because it may distort reality with invented very realistic material so as to mislead audiences, distribute false information, and manipulate public opinion. In the context of Indian politics, given that social media is very significant for electoral communication, this would be a very serious disintegrator of democratic credentials through the creation of manipulated and false narratives around various political figures or events, such as statements and events alleged to have been made or to have occurred that do not, in fact, exist. Those then bring the reputation of public leaders into disrepute by having voters presented with allegedly 'made' or manufactured statements and actions attributed to such political figures.

Another serious issue is the unauthorized use of a person's likeness because it violates privacy rights and may cause both personal and professional harm. Victims of deepfake content are most likely to face unfair humiliation, threats, or extortion, raising issues about how to balance the advancement of technology with the protection of human rights. Further, these deepfakes contribute to the larger problems in society by causing mistrust in media and authentic sources of information, thus leading to waves of broad uncertainty and cynicism through the public.

This means that the challenge really is in the regulation of application, because deepfakes, as such, are not inherently unethical and have very valid applications in entertainment, satire, and educational settings. Thus, the urgent need is to develop comprehensive ethical and legal frameworks to mitigate damages but harness the benefits of this technology[16].

2. Solutions and Suggestions

2.1. Watermark the contents for authentication

As against the deepfake misinformation that one faces, watermarking such digital content is important so that the authenticity can still remain with sensitive media in matters of public figures and in government communications. Metadata-including who created it and where and when-is considered in these watermarks for content, which may defeat the deepfakes into undetected content because nothing would be visible but authentic metadata would exist for an end-user to determine his reliability. Public awareness campaigning may educate users about looking into the watermark media to mark it as a reliable document, which makes the existence of digital information even better by reliability.

2.2. The digital India deepfake bill is passed

A "Deepfake Regulation Bill" might provide an appropriately tailored legal framework to criminalize bad-faith use of AI for content manipulation. It will outline the appropriate penalties by creating and disseminating deepfakes when fraudulently, libelously, or otherwise harmfully used. An exception will be allowed for any form of satire, parody, or for educational purposes in order that the bill provides a delicate balance between free speech and unlawful use. This legislation would suppress misinformation but would also have avenues for justice to be achieved legally by the victims.

Deepfake Regulatory Authority

A Deepfake Regulatory Authority could be very vital in monitoring, verifying, and managing the ethical application of deepfake technology, particularly during election times. The authority would ensure coordination with the social media companies and the AI developers to ensure incorporation of detection tools in content before sharing. In addition, this authority would enable reports of suspected cases of misused deepfakes on the part of the citizenry for quick takedowns and remedial action. Setting standards and tracking adherence could position this body strongly at the forefront of enforcing a national standard against misuse in the deepfake field.

2.3. Deploy AI-enabled detection systems

Consequently, detection systems that have the integration of AI can establish the deepfakes and regulate their circulation. Applications such as WhatsApp, Facebook, and Twitter can attach AI-based facial recognition patterns, voice analysis patterns or movement inconstancies inside the media content. Altogether this will be embedded to these digital sites so they can tag or stop deepfakes from circulating freely. It limits the expansive circulation of such information plus builds people's trust in the media particularly during elections.

2.4. Public awareness and education launch

Educating citizens is the most important part of vigilance about deepfakes. Governments and organizations can also collaborate to run campaigns of education that make the dangers of deepfakes familiar to everyone. The above programs can educate how a manipulated media can be discovered and also teach people not to fall for any difference between real and fake news. Integrating digital literacy programs into schools and community centers could also build a digitally educated society, better placed to deal with deepfake-led misinformation.

2.5. Cooperation with international regulatory organizations

Since deepfakes and misinformation are global problems, India would be best suited to collaborate with international organizations like the United Nations and the European Union in developing standard global regulations. Through bilateral and multilateral agreements, India can share detection technologies and coordinate actions to control the flow of foreign-created deepfakes. Such international collaboration would support

national efforts by addressing cross- border challenges, promoting digital integrity, and protecting the public from manipulative content from foreign sources.

2.6. IT and the guidelines of the election commission of India

The Information Technology Rules, 2021 forms a basis for a general regulation of digital content; however, it must further be extended to form strict guidelines to deal with such specific deepfake threats. For example, the ECI can issue guidelines according to which all political material, posted online, may go through some verification and confirmation of authenticity. In the light of elections, digital firms should be asked to detect those political advertisements that are the cases of deep faking during election time. It will keep malpractices out of the AI-based system during elections and build stronger confidence among citizens regarding this electoral process.

3. Conclusion

As AI advances, deepfake technology has emerged as both a powerful tool and a potential threat to the integrity of democratic societies. In the Indian context, where political dynamics and digital media use are intricate and influential, the stakes of this technology are especially high. Deepfakes enable hyper-realistic manipulation of audio, video, and images, which poses significant risks, especially in shaping public opinion during elections. This unprecedented accessibility of such technology also threatens to blur the lines between reality and fiction, meanwhile creating a public distrust of media and institutions.

Indian policymakers are slowly waking up to these threats in the form of various legislative initiatives, such as the Information Technology Act and changes in IT rules regarding misuse of synthetic media. However, the paper identifies an imperative for deepfakes: regulations that would specifically target this particular nuance. Public awareness programs and educational campaigns could be used to make people better equipped to recognize genuine information, which could in turn reduce the impact of deepfake manipulation on the political decisions they make.

The report points out that the three things the nation needs to see it through this matter would include legislative change, furthering of scientific progress with detection devices, and social consciousness building. With a sense that India is already primed for big elections, these strategies are apropos in ensuring democracy doesn't succumb to either moral or operational threats thrown its way by deepfakes. Balancing AI with responsibility will foster an efficient and resilient society resistant to the insidious digital manipulation by creating the lifeblood - keeping citizens' trust - while making sure democratic principles continue to be healthy and hearty.

4. References

1. MIT Sloan School of Management, Deepfakes Explained. MIT Sloan.
2. Singh P. Manipulating Reality: Understanding the Ethical and Legal Dimensions of Deepfakes. Lawctopus.
3. Associated Press, Deepfake of Biden's Voice Called Early Example of U.S. Election Disinformation. Voice of Am.
4. Hern A. Doctored Sunak Picture Is Just Latest in String of Political Deepfakes. The Guardian.
5. Varma R. Regulating Deepfakes: Generative AI in India, Explained. The Hindu.
6. Deepfake' Video Shown at Indian Politician's Funeral in Karnataka Sparks Controversy. BBC News.
7. Dhankhar S. AI, Deepfakes, Bad Laws, and the Big Fat Indian Election. Reuters Inst.
8. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §§ 43A, 66E, 66D, 66F, 67.
9. Bharatiya Nyaya Sanhita. 2023, No. 4, Acts of Parliament, 2023, §§ 354, 195(1), 145, 316(1), 292-293.
10. Indian Copyright Act. 1957, No. 14, Acts of Parliament, 1957, § 51.
11. Representation of the People Act. 1951, No. 43, Acts of Parliament, 1951, §§ 123, 125.
12. Aryan A. From IT Bots to AI Deepfakes: The Evolution of Election-Related Misinformation in India. The Hindu.
13. World Economic Forum. Deepfakes in India: Tackling AI-Generated Misinformation in Elections.
14. Mukhopadhyay S. Indian Election Was Awash in Deepfakes, but AI Was a Net Positive for Democracy. The Conversation.
15. Wachter S. Ethical Dilemmas in Deepfakes, 13 J. Strategic Security 56.
16. Ethical Dilemmas in Deep Fakes, Drishti IAS.