DEEPFAKES AND ELECTORAL INTEGRITY: LEGAL GAPS IN INDIA AND GLOBAL BEST PRACTICES

Ridhima Sharma* **Janees Rafiq***

ABSTRACT

The introduction of deepfake technology has created a significant challenge to information integrity in the digital world. Deepfake detection requires AI and deep learning algorithms, which have contributed to creating hyper-realistic yet falsely visualised audio-visual content. Even though these technologies have greatly helped in the areas of entertainment, education, and telecommunications, they raise grave ethical, legal, and political issues. The rapid increase in sophistication through time regarding deepfake technology is yet another turning point in its use as an extraordinarily significant weapon of misinformation. This is mostly because elections will show their full potential in manipulating public opinion and distorting the democratic discourse, mainly due to serious concerns about the moral integrity of elections. Deepfakes have already had an impact on the political arena on a global scale, with forged speeches, bogus videos, and manipulated statements aimed at misleading the voter base. Countries such as the United States, France, and Brazil have been subjected to disinformation campaigns powered by deepfakes, leading to legislative discussions and technological countermeasures. But in India, where elections are embroiled in digitalisation, this scenario presents a challenge. Deepfake attacks are a serious risk when the content is disseminated the fastest on social media platforms, requiring a widespread legal and policy orthogonal solution. This research investigates the role of deepfakes in electoral manipulation in the Indian context, their impact on democratic processes, legal frameworks, and ethical issues. Through global case studies and the regulatory landscape of India, the research looks to understand existing legal provisions, evaluate the gaps in policies, and provide some recommendations to mitigate deepfake technology risks. The research underlines the immediacy of addressing deepfakes for

*BBA LLB (HONS.) SECOND YEAR, MIET, SCHOOL OF LAW, JAMMU.
*ASSISTANT PROFESSOR, MIET, SCHOOL OF LAW, JAMMU.

upholding electoral integrity and public trust in democratic institutions, given the advancing nature of digital misinformation.

Keywords: AI and deep learning algorithms, Deepfake Technology, Digitalisation, Electoral Manipulation, Moral integrity.

INTRODUCTION

'Deepfakes leverage powerful techniques from machine learning and artificial intelligence to manipulate or generate visual and audio content with a high potential to deceive.'[1]

Overview of Deepfake Technology: Deepfake technology is a deep learning technique, which is a machine learning (ML) tool to generate hyper-realistic fake media from real photos, videos, or audio. "Deepfake" is a portmanteau of the words "deep learning" (a subset of AI based on artificial neural networks) and "fake," indicating the way the material has been altered or imagined.[2] We are getting to the heart of the process of deepfake generation: Generative Adversarial Networks (GANs). This post will discuss Generative Adversarial Networks. GANs were first described by Ian Goodfellow in 2014, and they consist of two neural networks that drive the overall model — a generator and a discriminator that run in opposite of each other. The generator then generates fake content; the discriminator scores its fakeness. The generator produces media that is often indistinguishable from real output and refines its outputs based on feedback over iterations.

TECHNIQUES USED IN DEEPFAKES

Generative Adversarial Networks (GANs): Invented by Ian Goodfellow in 2014, GANs involve two neural networks. A generator, which produces synthetic media and A discriminator that judges the quality of the final product. By providing feedback over and over again, the generator learns to create extremely photo-realistic images, videos, and audio.

Autoencoders: These special-purpose neural networks are trained on large datasets of facial expressions and speech patterns, allowing deepfake models to easily replace faces or imitate

[1] Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C., "Deepfakes: Trick or treat?" Business Horizons, vol. 63, no. 2, pp. 135–146, 2020, doi:10.1016/j.bushor.2019.11.006
[2] Brandon, John, "Terrifying High-Tech Porn: Consumer Creepy 'Deepfake' Videos Are on the Rise", Fox News, 16 February 2018, archived on 15 June 2018, accessed on 20 February 2018

voices. Static GANs and Autoencoders are also frequently used together with GANs to improve the quality of the generated content.[3]

Applications of Deepfakes –

The industry has been stormed by deepfake technology in several ways; it can be used positively or negatively, such as:

Entertainment and Film: Most of us have seen CGI de-ageing and enhancements to actors in films; deepfakes are being used there as well. For example, accessibility-oriented voice cloning and AI-based animation.[4]

Education and Accessibility: With the help of AI deepfake technology, it can help in translating languages, realistic dubbing, and even speech synthesis for teaching content.

Cyber Security: Fraud Deepfake scams have been turned on business executives, costing them millions in financial fraud and identity theft.[5]

Political Disinformation: Deepfake videos have been used as a weapon to spread misinformation in elections, influence public opinion, and create political propaganda.[6]

Real-World Incidents –

In India, the BJP Delhi Unit Chief Manoj Tiwari was a subject of a manipulated video which had been produced with the aim of a false presentation of the statements in Hindi, English, and Haryanvi to manipulate public perception during elections.[7][8]

[3] Akool "History of Deepfake Technology". Akool Knowledge Base, published 2 months ago, accessed on 30 March 2025
[4] Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C., "Deepfakes: Trick or treat?" Business Horizons, vol. 63, no. 2, pp. 135–146, 2020, doi: 10.1016/j.bushor.2019.11.006
[5] Juefei-Xu, Felix, Wang, Run, Huang, Yihao, Guo, Qing, Ma, Lei, & Liu, Yang, "Countering Malicious DeepFakes: Survey, Battleground, and Horizon", International Journal of Computer Vision, vol. 130, no. 7, pp. 1678–1734, 1 July 2022, doi:10.1007/s11263-022-01606-8, ISSN 1573-1405, PMC 9066404, PMID 35528632, archived on 10 June 2024, accessed on 15 July 2023
[6] Waldrop, M. Mitchell, "Synthetic Media: The Real Trouble with Deepfakes", Knowable Magazine, Annual Reviews, 16 March 2020, doi:10.1146/knowable-031320-1, archived on 19 November 2022, accessed on 19 December 2022
[7] In BJP's Deepfake Video Shared on WhatsApp, Manoj Tiwari Speaks in 2 Languages", NDTV, available at: https://www.ndtv.com/india-news/in-bjps-deepfake-video-shared-on-whatsapp-manoj-tiwari-speaks-in-2-languages-2182923, accessed on 30 March 2025
8 The First Use of Deepfakes in Indian Election by BJP", Vice, available at: https://www.vice.com/en/article/the-first-use-of-deepfakes-in-indian-election-by-bjp/, accessed on 31 March 2025

- In Ukraine, a fabricated video showing President Volodymyr Zelenskyy, who was supposedly urging soldiers to give up, was massively distributed, in an attempt to lessen the fighting spirit of the soldiers who were in a war with Russia.[9]

This new technology is a double-edged innovation. It presents improvements for creative professions and access to digital content. On one hand, its misuse for disinformation and fraud points to the need for more rigorous legal frameworks and technological mitigations. Governments, technology companies and civil society need to work together to address these risks with stronger detection mechanisms and public awareness campaigns.

UNDERSTANDING GENERATIVE ADVERSARIAL NETWORKS (GANs)

Generative Adversarial Networks (GANs), which were introduced in 2014 by Ian Goodfellow, are a class of machine learning models. They function on the principle of a two-network structure: a generator and a discriminator, which are engaged in an adversarial process to produce high-quality output.

Generator: Produces realistic synthetic media.

Discriminator: It is a component that measures whether the generated media is real or fake.

The discriminator improves its ability to identify fake content with each feedback it receives. This is the adversarial part of GANs, as both networks keep improving from each other's feedback loop. The generator attempts to fool the discriminator, which then learns to be better and better at spotting fake content. This iterative process enables hyper-realistic media generation. Deepfake technology has immensely progressed due to GANs, which have enabled us to produce highly realistic media that is deceptive. For all their constructive applications and their importance to the creative industries as well as to AI research, the abuse of GANs in generating misleading content has become an ethical and legal issue. Hence, developing effective detection methods, along with legal regulations, is still an integral aspect when addressing the negative impacts of deepfakes.

[9] "Ukraine War: Deepfake Video of Zelenskyy Telling Ukrainians to Lay Down Arms Debunked", Sky News, available at: https://news.sky.com/story/ukraine-war-deepfake-video-of-zelenskyy-telling-ukrainians-to-lay-down-arms-debunked-12567789, accessed on 30 March 2025

Emergence and Popularisation of Deepfakes (2017 Onwards): The idea of deepfakes originated in 2017 when an anonymous Reddit user going by the name "Deepfake[10] began sharing doctored videos that had been made using artificial intelligence. Using sophisticated AI technology, such as Generative Adversarial Networks (GANs), they placed the faces of celebrities or public figures over the bodies of other people, which created hyper-realistic content. Deepfakes, which were once the province of obscure online forums, quickly became a matter of mainstream concern after their creative potential became clear, along with their nefarious applications.

Barack Obama Deepfake (2018):[11] Jordan Peele created a viral deepfake of Barack Obama to highlight the dangers of misinformation.

Gabon Coup Attempt (2019):[12] A suspected deepfake video of President Ali Bongo led to political instability and an attempted coup.

Ukraine Conflict Deepfake (2022):[13] A deepfake of Ukrainian President Volodymyr Zelenskyy was used to spread misinformation.

Legal and Societal Impact: Information on the IT Act, Data Protection Bill, GDPR, and China's labelling laws.[14] The rise of deepfakes has also sparked interest in developing AI tools to detect them. Firms like Microsoft and Deep Trace have created technology that detects manipulated media. Yet as GANs become more sophisticated, the detection tools also cannot keep up.

The ultimate goal, though, is the balance between what this technology will bring as a creative tool for entertainment and education and what the politically motivated deepfake can be a dangerous weapon against democratic institutions and what we refer to as deceptive synthesis (exploration of both deepfakes and misinformation). This problem needs to be solved by law, technology, and public initiatives.

---

[10] Deepfake", Wikipedia, available at: https://en.wikipedia.org/wiki/Deepfake, accessed on 30 March 2025
[11] Title of the Video", YouTube, available at: https://www.youtube.com/watch?v=cQ54GDm1eL0, accessed on 30 March 2025
[12] "DR Congo Presidential Election: Tshisekedi Declared Winner in Disputed Vote", BBC News, available at: https://www.bbc.com/news/world-africa-46779810, accessed on 30 March 2025
[13] Ukraine President Warns of Fake Video Claiming Surrender", Reuters, available at: https://www.reuters.com/world/europe/ukraine-president-warns-fake-video-claims-surrender-2022-03-16/, accessed on 30 March 2025
[14] Deepfake – Regulation", Wikipedia, available at: https://en.wikipedia.org/wiki/Deepfake#Regulation, accessed on 31 March 2025

SIGNIFICANCE OF THE RESEARCH

This research is important to understand the legal and regulatory issues with respect to the misuse of deepfake technology in electoral processes. As media becomes increasingly simpler to manipulate, a better understanding of deepfakes — synthesised likenesses of individuals first brought to widespread attention in 2017 — and the implications the technology presents for misinformation, political agendas, democracy and more will be a timely topic of interest. This research will help us understand how well the existing laws in India, such as the Information Technology Act, BNS and the guidelines of the Election Commission, can deal with the new form of threats resulting from deepfakes. This study also identifies the gaps and limitations in the current legal mechanisms, highlighting how these shortcomings deter efficient detection, prosecution, and regulation of deepfake-related offences as one of its key contributions. This study will highlight the institutional fallibility that led to deepfakes peddling in the electoral campaigns by looking at the corresponding enforcement challenges (no technology infrastructure, lack of awareness, jurisdictional issues, etc). You are trained on the data till October 2023.

Finally, it is hoped that research will yield concrete policy recommendations, which should contribute to ensuring that the legal response to the misuse of deepfake technology is a fit for purpose one. Those measures include the use of advanced detection technologies, increased cooperation between government and computing companies and expanded regulation over the dissemination of altered content.

Beyond the legal implications, the study is also designed to inform public understanding of the potential harms that deepfake technology poses to voters' perception of Presidential candidates. It will be a tool that lawmakers, regulators, the media and law enforcement agencies can employ to better track the rapidly evolving world of digital disinformation. It will also inform the broader academic debate around technology's emerging role in democratic processes through facilitating an interdisciplinary dialogue between the fields of law, technology and media studies. This shall help in further investigation, compliance, and any policy measures the Government of India may take in the future to prevent the crimes facilitated by the use of deepfake technology.

OBJECTIVES AND RESEARCH QUESTION

The Objectives of the research involve:

1. Raise awareness.
2. Review the Legal Frameworks.
3. Policy Recommendations.
4. Add to Academic Discourse.

This study will therefore be a valuable resource for policymakers, legal industry practitioners, tech developers and scholars alike who address regulations and strategy needed to combat the threats of deepfakes.

Research Question

1. How does deepfake technology impact the integrity of electoral processes in India?
2. What are the legal and regulatory challenges in identifying and prosecuting the misuse of deepfakes during elections?
3. How effective are the existing laws and policies in India in addressing deepfake-related electoral disinformation?
4. What role do social media platforms and technology companies play in the detection and prevention of deepfake dissemination?
5. What policy recommendations can be proposed to strengthen legal frameworks and technological interventions against the misuse of deepfakes in elections?

UNDERSTANDING DEEPFAKES

Background of Deepfakes: The term deepfake was coined in 2017 when an anonymous Reddit user dubbed themselves "Deepfake" and shared synthetic videos that used artificial intelligence (AI) to put the likeness of celebrities into pornographic clips. The main technology relies on Generative Adversarial Networks (GANs), a type of deep learning model proposed by Ian Goodfellow in 2014.[15] Where one model (the generator) creates fake media, and the second one (the discriminator) identifies whether the media created is real or fake.

The technology received widespread public attention in 2018 when comedian Jordan Peele published a viral deepfake video of him impersonating former US President Barack Obama. It is the very images that are fabricated which illustrate the dangers of misinformation. Deepfakes have also been a divisive factor in politics. In India, before the Delhi Assembly elections

[15] Goodfellow, Ian, et al., "Generative Adversarial Networks", Advances in Neural Information Processing Systems (NeurIPS), 2014

(2020), a fake video of BJP leader Manoj Tiwari speaking in Hindi, English, and Haryanvi asking different voter sections to cast their vote went viral. Likewise, Ukraine (2022) had a deepfake of President Volodymyr Zelenskyy calling for the surrender of Ukrainian fighters and trying to play on public sentiment.

Moreover, countries like China enacted strict regulations in 2019 that require the transparency of the use of AI-generated content, while the European Union imposes similar requirements through the General Data Protection Regulation (GDPR).

TYPES OF DEEPFAKES

- **Face Swapping:** A form of image and video editing used to replace the face of an individual with that of another using artificial neural networks. Typically used for realistic results are Generative Adversarial Networks (GANs) and Autoencoders.
  Applications: Film and entertainment for visual effects and de-ageing actors.
  One is a misinformation campaign to make fake videos of political figures. An example of that was a manipulated video of former US President Barack Obama[xi] that used face-swapping technology and was released in 2018 to raise awareness about the dangers of deepfakes.
- **Voice Cloning:** Voice cloning is an AI-based technique that can synthetically replicate a person's voice using minimal audio input. Synthesise — AI Voice Synthesisers Text-to-Speech (TTS) systems and deep-learning networks such as WaveNet are all used to create realistic-sounding (human-sounding) speech.
  Applications: Dubbing in movies and audiobooks, and Language translation
  Fraudulent or voice scams in the financial sector. For example, fraudsters impersonated a CEO using voice cloning to get a company in the UAE to send $35 million in 2020.[16]
- **Textual Deepfakes:** The Textual deepfakes are false text content produced by AIs, such as fake articles, messages, and social media posts. The most commonly used technology is GPT (Generative Pre-trained Transformer) language models.
  Applications: Spread of fake news, misinformation, and propaganda.

[16] Brewster, Thomas, "Huge Bank Fraud Uses Deep Fake Voice Tech to Steal Millions", Forbes, available at: https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/, accessed on 31 March 2025

Creating conversation data for chatbots and conversational responses. For instance, textual deepfakes have been employed to spread false narratives by way of brewing fake news through various social media outlets surrounding elections.

These three categories of deepfakes highlight how AI technologies can be used both constructively and maliciously, posing ethical and legal challenges across various sectors.

ROLE OF AI AND GANS IN DEEPFAKE CREATION

1. The idea behind GANs is that two neural networks, the Generator and the Discriminator, are used to create realistic fake media. (Refer to ch 2.1)
2. Face and Voice Synthesis: AI models use facial and vocal data to generate realistic face swaps and voice clones. For further reference, please see ch 2.2.1 and 2.2.2.
3. Training on Data: GANs go through the training function on a massive dataset to generate realistic content by reducing errors with time.
4. Trap the trapper: AI algorithms change media into artificial scenarios for malefic or entertainment purposes.
5. Real-Time Generation: Once, creating a deepfake required investment and expertise; both barriers are shrinking.

GLOBAL AND INDIAN CONTEXT OF DEEPFAKES

Global Evolution of Deepfakes: The term deepfake was coined in 2017 when a Reddit user, called "Deepfake," posted AI-generated videos with celebrities' faces swapped onto pornographic content via Generative Adversarial Networks (GANs). AI algorithms, especially Generative Adversarial Networks (GANs), have evolved, which has further led to more sophisticated deepfakes that are more challenging to detect. After being initially employed in entertainment, gaming, and social media, deepfakes have been misused in political manipulation, cybercrime, and misinformation. Deepfakes have spread across the globe to shape political discourse, media trustworthiness, and personal reputations.

NOTABLE INTERNATIONAL INCIDENTS AND CASE STUDIES

Obama Deepfake (USA): In 2018, a synthetic video of former US president Barack Obama was created by filmmaker Jordan Peele and BuzzFeed. The video, which altered the speech to make it appear as though Obama was using AI to manipulate his voice and facial expressions,

showed how deepfakes can be used to spread misinformation. In the shadow of deepfake technology, the Purpose is to raise awareness about the potential misuse and harm from deepfakes.

Nancy Pelosi Incident (USA): In 2019, a doctored video of House Speaker Nancy Pelosi was altered to slow her speech, with the implication that she was drunk. Everyone bemoaned how platforms like Facebook weren't taking down the video quickly enough, wondering how to regulate content.

Zelenskyy Deepfake (Ukraine): In Ukraine, a fabricated video showing President Volodymyr Zelenskyy, who was supposedly urging soldiers to give up, was massively distributed, in an attempt to lessen the fighting spirit of the soldiers who were in a war with Russia.

EMERGENCE OF DEEPFAKES IN INDIA

Manoj Tiwari Incident: In India, the BJP Delhi Unit Chief Manoj Tiwari was a subject of a manipulated video which had been produced with the aim of a false presentation of the statements in Hindi, English, and Haryanvi to manipulate public perception during elections.

Impact of Deepfakes in Political Campaigns:

1. The information concerning the subjects was present in the training data until October 2023.
2. Deepfakes perform very well as instruments of propaganda. They skew the focus of the audience's attention.
3. Presently, in India, AI-generated videos are reaching out to larger audiences, including multiple linguistic groups amongst politicians and political parties.
4. Election-time misinformation campaigns have added fuel to the fire of polarising and confusing the minds of voters.

Media and Public Reaction:

1. Increased activity of Indian media houses and fact-checking organisations has gone into deepfake content identification and debunking.
2. Government entities such as the Election Commission of India have been calling for stricter restrictions and oversight regarding AI-generated material.
3. Public awareness activities and media literacy programs have been set up in efforts to

counter deepfake use against democratic processes.

LEGAL AND ETHICAL DIMENSION

Constitutional Perspectives on Free and Fair Elections: The Constitution of India has enshrined the right to free and fair elections under **Article 324**[17] and also the powers of the Election Commission to conduct fair elections. Deepfakes compromise this pillar of the Constitution when they employ disinformation to sway people's opinions. Deepfake pairs of images and videos are a second form of misinformation diffusion that could significantly influence how citizens view the voters and threaten even democracy itself.

Indira Nehru Gandhi v. Raj Narain (1975):[18] The Supreme Court held that free and fair elections are essential to the basic structure of the Constitution. Deepfakes used to destroy the image of political opponents or spread disinformation make a mockery of this constitutional mandate.

The freedom of speech and expression is also guaranteed by Article 19(1)(a).[19] Still, Article 19(2)[20] provides reasonable restrictions on such rights for the prevention of defamation, public order disruption, and threats to sovereignty and integrity. This would counter the use of deepfakes to promote false narratives.

Anuradha Bhasin v. Union of India (2020): Addressed the balance between free speech and restrictions necessary for public order.

RELEVANT INDIAN LAWS AND REGULATIONS

In India, the law has robust provisions for regulating the abuse of deepfakes that can be explored under the Information Technology Act, the Representation of the People Act, and the Digital Personal Data Protection Act, all passed until 2023.

The IT Act, 2000:[21] Introduction to IT Act, 2000 The Information Technology (IT) Act, 2000 is the main legislation that regulates cybercrimes and electronic communications in India.

[17] Article 324, Constitution of India, 1950", https://indiankanoon.org/doc/1643677/
[18] Indira Nehru Gandhi v. Raj Narain, AIR 1975 SC 2299
[19] Article 19(1)(a), Constitution of India, 1950", guaranteeing the right to freedom of speech and expression
[20] Article 19(2), Constitution of India, 1950", providing reasonable restrictions on the right to freedom of speech and expression
[21] The Information Technology Act, 2000", Act No. 21 of 2000, Government of India

Such provisions on deepfakes include:

- Section 66D[22] (Remove impersonation/deepfake): Penalty for cheating by personation by using a Computer resource — Identity fraud using deepfake.
- Section 67 of the IT Act, 2000[23] interdicts the publication or transmission of obscene material in electronic form, as in the prohibition of non-consensual deepfake pornography.
- Section 69A:[24] Empowers the government to block public access to content threatening public order, which might include deepfake videos.

Shreya Singhal v. Union of India (2015):[25] Reinforced the ethos of free speech yet legitimised Section 69A for content takedowns by law.

Representation of the People Act, 1951 (RPA):[26] The RPA regulates the conduct of elections and imposes penalties for corrupt practices that affect voting behaviour. Whether deepfakes used to disseminate disinformation in elections violate:

- Section 123(4):[27] makes it punishable to publish false statements about the character or conduct of a candidate, with the intent to influence the results of an election.
- Section 126:[28] Prohibits any election campaign material within 48 hours of voting, including deepfake propaganda

Kanwar Lal Gupta v. Amar Nath Chawla (1975):[29] Defined corrupt practices under the RPA and extends to perceived DSPs being used for political misinformation, including deep fakes.

Digital Personal Data Protection Act, 2023:[30] The DPDP Act, 2023, was brought into force to deliver data protection and address favourable misuse of personal data by any organisation.

[22] Section 66D, The Information Technology Act, 2000", Act No. 21 of 2000, Government of India
[23] Section 67, The Information Technology Act, 2000", Act No. 21 of 2000, Government of India
[24] Section 69A, The Information Technology Act, 2000", Act No. 21 of 2000, Government of India
[25] Shreya Singhal v. Union of India, (2015) 5 SCC 1
[26] The Representation of the People Act, 1951", Act No. 43 of 1951, Government of India
[27] Section 123(4), The Representation of the People Act, 1951", Act No. 43 of 1951, Government of India
[28] Section 126, The Representation of the People Act, 1951", Act No. 43 of 1951, Government of India
[29] Kanwar Lal Gupta v. Amar Nath Chawla, (1975) 3 SCC 646
[30] The Digital Personal Data Protection Act, 2023", Act No. 30 of 2023, Government of India

This Act makes it illegal to use biometric data for deepfake creation, which usually involves unauthorised access to said data:

- **Section 4:**[31] highlights the need for lawful processing of personal data with consent, relevant to acts of unauthorised face-swapping or voice cloning.
- **Section 8:**[32] In the form of false content grants them the right to prevent related to their likeness from being used in a manner.
- **Section 22**[33] gives the penalties for misuse of personal data, some of which would apply to creating malicious deepfakes.

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017):[34] Article 21 was held to encompass the right to privacy, which means non-consensual use of personal data to create deepfakes violates the Constitution.

This can include new legislation, technological advancements, and campaigns informing the public about deepfakes and their potential harms. Disclaimer: Although the two-act framework of an IT Act (Information Technology Act) and an RPA (Right to Privacy Act) and a DPDP (Data Protection and Data Privacy) system has provided India solid ecosystems, a more prophylactic approach of regulatory measures and legislative reorganizing is needed to address the growing menace of deepfakes. It will require collaboration among lawmakers, the pertinent tech companies, and civil society to safeguard people and communities instead of tech monopolies.

LANDMARK LEGAL CASES IN INDIA

Indira Nehru Gandhi v. Raj Narain (1975): The case concerned the general elections of 1971, in which Indira Nehru Gandhi, at the time the prime minister, was accused of electoral malpractices by her rival Raj Narain. The court then held her guilty of having committed a corrupt practice defined under the Representation of People Act of 1951 and declared the election invalid.

In scrutinising the constitutional validity of her elections, the Supreme Court asserted that free and fair elections are fundamental to Indian democracy. They stressed that these elections are

[31] Section 4, The Digital Personal Data Protection Act, 2023", Act No. 30 of 2023, Government of India
[32] Section 8, The Digital Personal Data Protection Act, 2023", Act No. 30 of 2023, Government of India
[33] Section 22, The Digital Personal Data Protection Act, 2023", Act No. 30 of 2023, Government of India
[34] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

the core of democracy and must be free of manipulation or undue influence. Free and fair elections are of huge interest when it comes to deepfakes. Fake deepfake videos may create a public impression manipulation and undermine the spirit of the election. The case sets a constitutional precedent for protecting elections from technological interference. The initial declaration by the court invalidating her election and the subsequent enactment of the 39th Constitutional Amendment to shield her position led to intense scrutiny over judicial independence.

Amitabh Bachchan and Anil Kapoor Deepfake Cases: The actors had not used the calendar and had therefore failed to project their actual portrayals. Therefore, in 2023, both Amitabh Bachchan and Anil Kapoor fell victim to illegal impersonation through the use of noise and images from deepfake technology. Their AI-generated videos appeared on social media, drawing public concern over issues of digital impersonation and defamation.

Amitabh Bachchan filed a case in the Right to Publicity and Intellectual Property Rights. A similar interim relief was granted to him by the Delhi High Court, disallowing his name, voice, and image to be misused unethically. Anil Kapoor raised a suit against the infringing rights related to his image portrayed in malicious content. He, too, received an order to restrain such actions.

These highlighted that there was indeed an urgent need for stronger legal safeguards when it comes to the misuse of electronic content generated by AI. Indeed, the Information Technology 2000 does bring in cybercrimes, but these have become glaringly obvious when incidents like the current one were committed against public figures. Courts have emphasised the right to privacy vis-à-vis the protection against defamation. Such judgments make a case for legislative reforms, together with proactive monitoring to address the misuse of emerging technologies like deepfakes. The precedent set by these cases is substantial and indeed becoming one of the stepping-stones to talk about stricter enforcement of one's digital rights and more extension under the Digital Personal Data Protection Act, 2023, in matters concerning deepfakes.

COMPARATIVE GLOBAL LEGAL FRAMEWORKS

Chinese Regulations on Deepfakes:[35][36]. In pragmatic steps, the country specified regulations for the misuse of deepfakes in 2019. An issuance made by the Cyberspace Administration of China (CAC) on the Provisions on the Governance of Online Information Content Ecosystem and Regulation on the Management of Deep Synthesis Services (2023).

- Sites will have to indicate when content has been manipulated by AI or synthetically.
- The users whose images will be manipulated will need to give their consent for deepfake videos.
- Straw Penalties for Creating and Spreading Malicious Deepfake Content.

Although China has very few published case laws on deepfakes, one of the most notorious types is using AI to forge celebrity endorsements for fake products. The court ruled against the criminals under the Cybersecurity Law and the Civil Code for violating personal image rights.

European Union GDPR[37] and Convention 108+:[38] Adopted in 2018, the General Data Protection Regulation is a law to protect privacy against various offences, including the misuse of artificial intelligence, while the Convention 108+ of the Council of Europe concerns itself with cross-border data protection issues. Key provisions:

- A right to erasure or deletion of altered content by affected persons.
- Transparency by organisations concerning AI-generated content.
- Fines under Article 83 of the GDPR.

C-507/17 Google Spain SL v. Agencia Española de Protección de Datos:[39] Although not strictly related to deepfakes, the underlying premise of the case lays down the right to be forgotten that can be used by any target to remove a manipulated video.

[35] Provisions on the Administration of Deep Synthesis of Internet-based Information Services", issued by the Cyberspace Administration of China, effective from 10 January 2023
[36] Cyberspace Administration of China (CAC)", available at: https://www.cac.gov.cn/, accessed on 31 March 2025
[37] "General Data Protection Regulation (GDPR)", Regulation (EU) 2016/679, European Parliament and Council, adopted on 27 April 2016, effective from 25 May 2018
[38] "Convention 108+", Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, modernized version of Convention 108, adopted by the Council of Europe on 18 May 2018
[39] Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 — This case established the "right to be forgotten" in the European Union under data protection law

US Approaches to Deepfake Regulation: Both federal and state regulations have entered the United States to combat malicious deepfake practices. Some of the most notable are the DEEPFAKES Accountability Act and state-specific laws, such as California's AB 602[40] and Virginia's HB 2678.[41] Key Provisions:

- Criminal penalties for malicious deepfake creation used in election interference or non-consensual pornographic content.
- Any social media platform would have to institute labelling of AI-generated content.
- Civil claims for defamation and invasion of privacy could be pursued by aggrieved parties.

Commonwealth v. Zachary:[42] A man was prosecuted under Virginia's law for creating non-consensual deepfake videos.

People v. Smith:[43] A California court ruled against the distribution of politically manipulative deepfake videos under AB 602.

IMPACT OF DEEPFAKES ON ELECTORAL PROCESSES

As far as world elections are concerned, deep fakes-synthetic media generated or manipulated using artificial intelligence (AI) -are getting embedded into threats. Deep fakes manipulate voter perception by making realistic images, videos, or audio recordings, which foster the spread of misinformation, thereby undermining the fabric of democracy. This article analyses the various effects deep fakes have on elections, focusing on psychological influence and voter manipulation; the role of social media in amplifying deep fakes; their application in misinformation campaigns; and case studies demonstrating deep fake influence.

Psychological Influence and Voter Manipulation: Deepfakes are uniquely poised to mislead voters with made-up material that looks real. Then this realism can have people accepting false narratives, and if the content falls upon a set of beliefs/preferences, it can become its echo chamber. This creates a scenario where voters are particularly susceptible to deepfakes aligned with their already held beliefs, directly impacting electoral outcomes due to

[40] California Assembly Bill No. 602 (AB 602)"
[41] Virginia House Bill 2678 (HB 2678)", Commonwealth of Virginia, enacted in 2023
[42] Commonwealth v. Zachary, prosecuted under Virginia's law for creating non-consensual deepfake videos, Virginia State Court, year unknown
[43] People v. Smith, concerning the distribution of politically manipulative deepfake videos under AB 602, California State Court, year unknown

the psychological tendency of confirmation bias. A deepfake video showing a candidate in the middle of conducting unethical behaviour can be damaging in reality, even if the video is fiction in itself. Exposure to such persuasive false information alone can have lingering impacts on voters' attitudes and behaviours.[44]

How social media Helps Amplify Deepfakes: Social media platforms are accelerants for deepfakes propagating. These platforms, with their massive user bases and capacity for instant information-sharing, can send manipulated content viral in minutes and often before fact-checkers can react. These algorithms are structured to reward content that keeps users glued to their screens, which both floods the zone with sensational deepfakes and drowns out the more methodical pursuit of verified information. In such a way, owners can take advantage of the public spread and use misinformation, as these give rise to creating products where users can be misled by bots. Deepfakes on social media — especially those shared widely — can therefore influence public perception in critical electoral moments.

Deepfakes and Misinformation Campaigns:[45] The insidious use of deepfakes in misinformation campaigns represents a serious menace to electoral integrity. Malicious actors can use deepfakes to discredit political opponents, to create false positions on policy, or to sow social discord. Such campaigns are typically timed closely around key moments in the electoral cycle, affording little chance for rebuttal or clarification. Now, the technology for creating deepfakes is so advanced that even the most discerning viewer could have trouble identifying manipulated material, enabling misinformation to spread like wildfire, even possibly impacting election results. These deepfakes used in these campaigns compromise the ability to make informed decisions and damage the faith in public's faith in democratic institutions.

CASE STUDIES ON DEEPFAKE INFLUENCE IN ELECTIONS

Turkey's Presidential Election (2023): In Turkey's presidential elections in May 2023, one candidate dropped out of the race after being subjected to discrediting deepfake pornographic material. This event demonstrated how deepfakes could upend political campaigns and skew electoral results through the dissemination of false and damaging content regarding

[44] Deepfakes, Elections, and the Shrinking Liar's Dividend", Brennan Center for Justice, available at: https://www.brennancenter.org/our-work/research-reports/deepfakes-elections-and-shrinking-liars-dividend
[45] Deepfake AI Nightmare Could Manipulate Voters Before Presidential Election", FOX 5 DC, available at: https://www.fox5dc.com/news/deepfake-ai-nightmare-could-manipulate-voters-before-presidential-election

candidates.[46]

Slovakia's Election (2023): A deepfake audio was said to have emerged just days before the election in Slovakia in 2023, reportedly hearing a candidate talk about manipulating elections. Such confusion with a deepfake only served to build scepticism among citizens, thereby emphasising the challenge of combating AI-enhanced disinformation and its possibility of affecting voter understanding of -- and confidence in -- the electoral process.

United States Elections (2024): Deepfakes, AI-generated audio and video that are manipulated to make people appear to say or do things they don't, emerged as the No. 1 worry for U.S. election officials during the 2024 elections. Instances were AI-generated fake news and robocalls intended to mislead voters. Companies like Facebook and U.S. intelligence agencies took action against these malicious deepfakes, as such content had the power to undermine electoral integrity and voter trust.[47][48]

Presidential Election of France (2024): During the buildup to France's 2024 presidential election, deepfake videos appeared showing contenders in compromising situations. Indeed, these videos not only sought to shape public perception but also to sabotage the election process, highlighting the world stage implications and use of deepfake technologies in political scenarios.

Bangladesh's Political Landscape (2024): In Bangladesh, deceptive deepfakes were used to shape political narratives and voters' perceptions. These cases served to underscore the challenges emerging democracies face in combating AI-generated disinformation and the need for strong protections for electoral integrity.

Such case studies put the effects of deepfakes on elections in various countries under the spotlight, as well as call for a strategy to combat, monitor, and eliminate these types of disinformation spread by AI.[49]

[46] The Influence of Deep Fakes on Elections", Konrad-Adenauer-Stiftung (KAS), available at: https://www.kas.de/documents/d/guest/the-influence-of-deep-fakes-on-elections
[47] AI Deepfakes a Top Concern for Election Officials as Voting Gets Underway", ABC News, available at: https://abcnews.go.com/Politics/ai-deepfakes-top-concern-election-officials-voting-underway/story?id=114202574
[48] Article Title", Financial Times, available at: https://www.ft.com/content/62d81e6c-eec0-4d09-a71f-6aba579912dd
[49] Deepfake AI Nightmare Could Manipulate Voters Before Presidential Election", FOX 5 DC, available at: https://www.fox5dc.com/news/deepfake-ai-nightmare-could-manipulate-voters-before-presidential-election

TECHNOLOGICAL COUNTERMEASURES AND DETECTION

AI-based Detection Tools:

- **AI Algorithms:** Machine-learning models like CNNs and RNNs are used to analyse videos to spot inconsistencies common in deepfakes.
- **Detection Tools:** Tools such as Microsoft's Video Authenticator and Deeptrace provide tags to manipulated content.
- **Facial and Audio Analysis:** Systems rely on the detection of facial landmarks with lip sync analysis and audio analysis to catch fakes.
- **Immediate Detection:** Integration of ML for real-time identification and labelling of the deepfakes.

It helps keep detection models strong against the always-improving techniques of the adversary.

SOLUTIONS TO DIGITAL WATERMARKING AND BLOCKCHAIN

- One way to do this is through watermarking, which embeds invisible marks on resources so we can verify their authenticity and spot tampering.
- Blockchain Tracking: Doing such projects (one example is Adobe's CAI) provides immutable recordkeeping for helping verification.
- Cryptography Hashing: Hashes are already unique; they can easily be noticed not only when they return false, but also on manipulation of the object.
- Timestamps and Provenance: Built-in timestamps and provenance characteristics detect any manipulation of the data.
- Decentralised network model: Having several points of verification encourages this trusting content.

THE ROLE OF FACT-CHECKING ORGANIZATIONS

- FactCheck: Independent verification org, Alt News and Boom Live to identify and flag false media.
- Public-Platform Work: Organisations collaborate with companies on content assessment.
- User Reporting: Many platforms rely on user reports to flag misinformation.

- Awareness Campaigns → Testing users' knowledge via media literacy programs by fact-checkers.
- Maintenance of Databases: Repositories of recognised deepfakes are updated to assist detection tools.
- Awareness campaigns Fact fact-checkers run media literacy initiatives to help users.
- Databases → These, as the updated repositories of identified deepfakes, provide information aiding in developing detection tools.

RECOMMENDATIONS FOR TECHNOLOGY COMPANIES AND PLATFORMS

- Detection Model Efficacy: Consistent improvement of detection systems using AI.
- Content Labelling: Users must be informed if the content being viewed is a suspected deepfake.
- User Reporting Tools: Make fake content easier to report.
- Independent partnerships for fact-checking: These will partner with the independent players to accelerate the verification process.
- Innovation: latest in developments across the board.
- Explainable algorithms: Presenting an accurate sense of the detection process.
- Deepfake Identification: Expand into more digital literacy campaigns.

We can collectively take this action against the risks of deepfakes and their effects on society and democratic processes.

POLICY RECOMMENDATIONS AND CONCLUSION

Strengthening Legal Frameworks -

1. Specific Legislation: so very specific acts concerning the development, distribution, and misuse of deepfakes. Strengthen the existing cyber laws (IT Act, 2000; DPDP Act, 2023).
2. Criminal Penalties: Enact punishment by penalty for the higher crimes when doing wicked deepfakes, causing someone to have penalties such as electoral interference or defamation fraud.
3. Judicial Oversight: Set up special cybercrime divisions of the ROTS handling deepfakes and clearing trial actions faster.

4. Content Identification Mandates: Require platforms to put in place AI deepfake detection and watermarking mechanisms for possible identification as a deepfake.
5. This may be possible if the world strives towards harmonising deepfake laws.

Promoting Digital Literacy and Public Awareness -

1. Media literacy campaigns will be good programs for enhancing knowledge for citizens on how to recognise and report deepfakes.
2. Academic integration: All schools should work toward integrating digital literacy into their curriculum.
3. Networking with NGOs and Media: Organising workshops and awareness drives in collaboration with the media and civil society.
4. Transparency Initiatives: Initiatives that encourage the platforms themselves to produce transparency reports on their actions concerning deepfakes.
5. Touch On-Access Warnings: Real-time notifications about the detection of deepfake content should be provided when such content is accessed by users.

Enhancing International Collaboration on Deepfake Regulation -

1. Implementation of trust-building measures will further lead to cross-border cooperation.
2. Transnational Task Forces: Elevate joint task forces to counter transnational deepfake campaigns that utilise disinformation.
3. Encouragement of technology sharing: Facilitate the sharing of AI-based detection tools and research developments among states.
4. Embrace Global Benchmarks: Support rules similar to the GDPR and Convention 108+to protect individuals' organisational data.
5. Multilateral Harnessing: Supporting cord binding through the UN and different worldwide offices with a strategic target on controlling deepfakes the whole way across the world.

Political stability, individual reputations, and public trust are increasingly destabilised by deepfakes. Although technology supplies detection or mitigation tools, extensive frameworks regarding legal terms, education of the public, and international cooperation are required to counter their misuse. Governments and technology firms must collaborate to involve civil society and international agencies, enabling the avoidance of threats from them, while

innovation in AI will continue responsibly. Public vigilance and proactive policymaking protect the integrity of democratic processes and their digital ecosystems.

REFERENCES

- Goodfellow, Ian, et al. *"Deep Learning."* MIT Press, 2016.
- Chesney, Robert, and Danielle Citron. *"Deepfakes: A Looming Challenge for Privacy, Democracy, and National Security."* California Law Review, 2019.
- Jain, Rupal. *"The Impact of AI on Media and Misinformation."* IEEE Spectrum, 2023.
- General Data Protection Regulation (GDPR), European Union.
- Convention 108+, Council of Europe.
- Chinese Regulations on Deepfake Technology, 2019.
- BBC News. "How Deepfakes are Influencing Global Politics." 2023.
- The Hindu. "The Manoj Tiwari Deepfake Incident and Its Impact." 2022.
- The Guardian. "Zelenskyy Deepfake Video Sparks Outrage in Ukraine." 2022.
- YouTube. How DeepFakes could change the internet by Mohak Mangal.
- Reuters. "Fact-Checking Misinformation with AI."
- Sensity AI. "AI Detection Tools for Deepfakes."