IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

DEEPFAKE THREATS: LEGAL CHALLENGES INCOMBATING AI-GENERATED MISINFORMATION

Ms. Sunidhi Gupta, Mr. Gokul Jain, Dr. Sudeepta Banerjee

Students, Assistant Professor

School of Business, MIT World Peace University, Pune

ABSTRACT: The rise of deep fake technology looms large over our societal landscape, casting shadows on politics, business, and the legal system. This research paper delves into the core of this digital menace, unraveling its intricacies and exposing the multifaceted threats it poses. From political manipulation to corporate sabotage, the tentacles of deepfakes reach far and wide. The paper navigates the treacherous waters of detection methods, exploring how we can unmask these deceptive digital creations. However, as society grapples with the impacts of deepfakes, the legal frameworks and regulations seem like feeble barricades against a looming storm. The paper critically examines existing legal structures, questioning their efficacy in the face of this evolving threat. Moreover, it confronts the imperative question on everyone's mind: What more can be done? In a world where technology advances at a breakneck pace, the paper doesn't shy away from pondering the synergy of legal and technological advancements needed to fortify our collective defense. It's a call to action, a stark acknowledgment of the urgent need to bolster our defenses against the escalating risks that deepfake technology thrusts upon us. The paper doesn't merely dissect the issue; it pushes the envelope, advocating for a proactive and adaptive approach to safeguarding the very fabric of our interconnected society. From political manipulation to corporate sabotage, the tentacles of deepfakes reach far and wide, leaving us navigating treacherous waters. The paper digs into detection methods, exploring how we can unveil these deceptive digital creations. Yet, as society grapples with the impacts of deepfakes, our legal frameworks appear feeble against the storm that's brewing. The paper takes a critical look at existing legal structures, questioning their effectiveness in the face of this evolving threat. It doesn't stop there; it stares down the pressing question on everyone's mind: What more can be done? In a world where technology races ahead, the paper doesn't shy away from pondering the synergy of legal and technological advancements needed to fortify our collective defense. This is a call to action, an urgent acknowledgment of the need to bolster our defenses against the escalating risks that deepfake technology thrusts upon us. It's not just an analysis; it's a push for a proactive and adaptive approach to safeguarding our society. The paper urges us not to dissect the issue merely but to push the envelope, advocating for a collective effort to preserve the very essence of our interconnected existence. The time for action is now, and this paper is a stark reminder of the imperative need to act.

KEYWORDS

Artificial Intelligence, Deep Learning, Deepfake, AI, AI Threats, Deepfake Threats, Legislation, Combating deepfake, synthetic media, misinformation, privacy law, defamation law, technological solutions, regulation and learnings, detection tools, authentication mechanism, media literacy and industry self-regulation.

INTRODUCTION

Deepfake technology has emerged as a formidable and pervasive threat across various sectors of society, including politics, business, and the legal system. As the manipulation of digital content becomes increasingly sophisticated, the potential for malicious use of deepfakes raises concerns about the integrity of information and its impact on individuals and institutions. This research paper delves into the nature of deepfakes, exploring their inherent risks, the methods employed for detection, societal consequences, and the existing legal frameworks designed to address these challenges. Keywords such as Artificial Intelligence (AI), Deep Learning, Deepfake, AI Threats, Legislation, and others highlight the multifaceted dimensions of this issue. Additionally, the paper navigates the intricate landscape of combating deepfake threats, examining technological solutions, regulatory frameworks, detection tools, authentication mechanisms, and the crucial role of media literacy and industry self-regulation. The central focus is

[derstanding the current state of affairs surrounding deepfake technology and addressing the imperative questionof what legal and technological advancements can be pursued collectively to enhance our ability to mitigate the escalating risks associated with this transformative and potentially harmful technology.

In the ever-evolving digital realm, the ominous rise of deepfake technology has become an omnipresent threat, infiltrating realms as diverse as politics, business, and our legal systems. This research paper is our compass through the murky waters of deepfakes, uncovering their risks, the elusive methods of detection, and the far-reaching consequences they unleash on our information landscape.

As technology becomes more adept at manipulating digital content, the looming specter of malicious deepfake use casts shadows on the integrity of information, raising legitimate concerns for individuals and institutions alike. This paper peels back the layers, spotlighting keywords like Artificial Intelligence (AI), Deep Learning, Deepfake, and Legislation to illuminate the intricate dimensions of this issue.

Our journey doesn't stop at mere exploration; we plunge into the trenches of combating deepfake threats. The paper dissects technological solutions, regulatory frameworks, detection tools, and authentication mechanisms. Yet, it alsosheds light on the unsung heroes in this battle: media literacy and industry self-regulation.

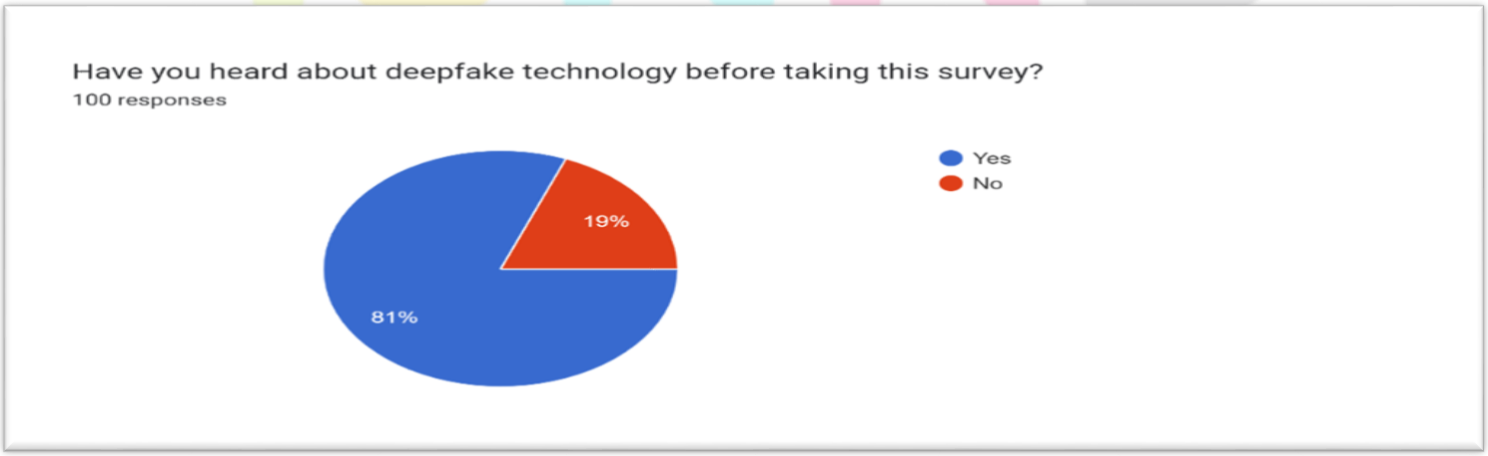
The paper acts as both detective and strategist, deciphering the current state of affairs surrounding deepfake technology. It poses a crucial question, hanging in the air like a call to arms: What legal and technological advancements can we collectively pursue to bolster our defenses against the rising tide of deepfake risks?

WHAT ARE DEEPFAKES?

Deepfakes are synthetic videos created or altered using advanced deep-learning techniques. The term "deepfake" comes from the combination of "deep learning" and "fake." Deep learning algorithms, particularly those used in generative models, manipulate or generate content to make it appear genuine.

These videos are a product of artificial intelligence applications that merge, combine, replace, and superimpose images and video clips. This technology can produce hyper-realistic videos with face swaps, leaving minimal traces of manipulation. Recent technological advancements have made it increasingly easy to create deepfakes that can be humorous, pornographic, or even politically motivated (Chawla, 2019; Maras & Alexandrou, 2018).

Deepfake technology uses AI to seamlessly merge and alter videos. The process involves training neural networks, such as autoencoders and Generative Adversarial Networks (GANs)



The visual representation illustrates the information gathered through a survey conducted by the author.

Autoencoder (WP)

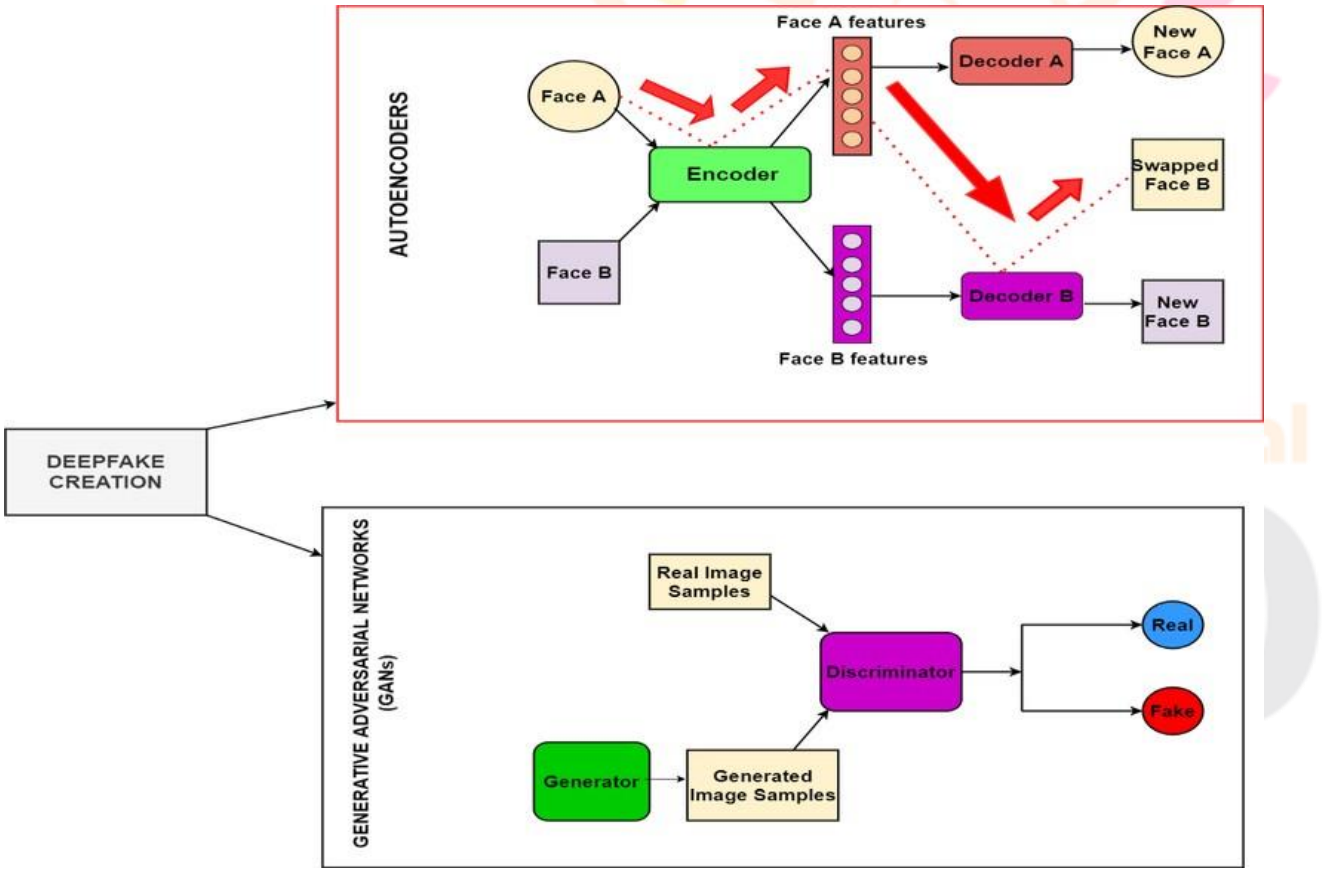
Autoencoders are a type of neural network designed for unsupervised learning. They consist of an encoder and a decoder, working together to learn a compressed representation of input data. The encoder compresses the data into a lower-dimensional representation, and the decoder reconstructs the input from this representation. In the context of deepfakes, autoencoders play a role in learning and generating realistic facial features and expressions.

GAN: (WP)

Deepfake creation also requires the use of Generative Adversarial Networks (GANs). GANs are made up of a generator and a discriminator. The generator creates

new data instances that resemble a given dataset, while the discriminator evaluates these generated samples, trying to distinguish them from real data. The adversarial training process involves a continual interaction between the generator and discriminator, pushing the generator to create increasingly realistic content.

Deepfakes have raised concerns due to their potential for misuse. They can be used to create misleading content, manipulate public opinion, or compromise the privacy of individuals. Researchers are actively working on developing techniques to detect and authenticate media content to address the challenges posed by the proliferationof deepfake technology (Day, 2018; Fletcher, 2018).



THE POSSIBLE THREAT OF DEEPFAKE

In the realm of deepfake technology, threats loom large, casting shadows over the authenticity of digital content. As these synthetic media creations grow more sophisticated, the potential risks to individuals, businesses, and societal trust become increasingly pronounced. In this exploration, we'll dive into the murky waters of threats to deepfake, dissecting the challenges posed to privacy, security, and the very fabric of truth in our digital landscape. From the misrepresentation of public figures to the manipulation of crucial information, the dangers associated with deepfake technology demand a closer look to comprehend and confront their evolving nature.

Threats to politics

Deepfakes pose a significant threat to politics by making it possible to create convincing fake videos featuring political figures. This concern emerges because modified films may be used to distribute misleading information, influence elections, and ruin political leaders' reputations. Consider the following scenario: a deepfake video is generated to make it look as if a politician is talking or doing something they never said or did. This might cause public uncertainty and even influence election results. The false information spread through deepfake videos can be designed to manipulate public opinion, sow discord, or damage the trust people have in political figures. Political leaders and their statements hold immense influence, and deepfakes can be exploited to create fabricated content that misrepresents their views or actions. This kind of misinformation can have serious consequences, affecting public trust in the political process and even causing instability in political landscapes. The threat to politics from deepfakes underscores the importance of ensuring the authenticity of media content, especially when it involves public figures. It raises concerns about the potential misuse of technology to manipulate public perception, influence democratic processes, and compromise the integrity of political discourse. As a result, there is a growing need for vigilance, awareness, and measures to address the challenges posed by deepfake technology in the realm of politics.

CASE: A notable example was the circulation of an altered video of an American politician, Nancy Pelosi on social media. In the video, she appeared intoxicated while mispronouncing her words [18]. The American President Donald
J. Trump shared the video on his “Twitter” account to alter public perception of his opponent, Nancy Pelosi. Consequently, the video has been viewed and shared over 2.5 million times on Facebook [19]. Despite bipartisan calls for the video to be taken down, a Facebook spokesperson confirmed that the videos will not be removed because the platform does not have policies that dictate the removal of false information [20]. Therefore, this has prompted world governments to look for ways to regulate the use of DT [Shadrack Awah Buo, 2020].

Threats to the Judicial System

Deepfakes pose a serious threat to the judicial system by undermining the reliability of video evidence in legal proceedings. In simpler terms, deepfake technology can create fake videos that look incredibly real, making it difficult for judges and juries to trust what they see. Imagine a scenario where someone uses deepfake technology to make a video that shows a person committing a crime. The video could be so convincing that it looks like undeniable proof of guilt. In a courtroom, this could lead to false accusations, unjust convictions, or even the release of a guilty person. On the flip side, deepfakes could also be used to create fake alibis or evidence that makes someone innocent appear guilty. This could result in wrongful convictions or legal chaos.

CASE: in a UK child custody case, a deepfake audio file was presented as evidence to the court by the mother [8]. The mother had used DT and tutorials online to create a plausible audio file that sounded like a recording of the father threatening her, to support her claim that he was too violent to be allowed access to their children. However, after the file was forensically examined, it was proven to be fake and dismissed by the courts. [Shadrack Awah Buo,2020].

Threats to Face Swapping

Imagine a world where anyone can convincingly swap faces in videos, making it look like someone said or did things they never actually did. That's the unsettling reality of deepfake technology. It's not just a cool tech trick; it's a serious threat. One major worry is privacy. Deepfakes can put anyone's face into compromising situations in videos, potentially causing personal and professional damage. Imagine the chaos if your face is seamlessly inserted into a compromising video that you never participated in. Then there's the misinformation angle. Deepfakes can be used to create fake videos of public figures saying or doing things they never did. This can lead to widespread confusion and damage the trust we place in visual media. To tackle this, we need smarter technology that can detect these fakes. But it's not just about tech – people need to know about deep fakes and understand the risks. Legal systems also need to catch up, with laws specifically addressing the creation and spread of harmful deepfakes. Ultimately, it's a big challenge that requires a mix of technology, awareness, and legal action to keep our digital world from being manipulated in harmful ways.

Threats to Business

Deepfakes pose a serious threat to businesses as they can be used to create deceptive videos that may harm a company's reputation or financial stability. Malicious actors could create deepfake videos featuring company executives announcing false information. For example, a fake video could make it seem like a CEO is declaring bankruptcy or revealing sensitive business strategies. Such misinformation can lead to panic among investors, affecting stock prices and causing financial losses. Deepfakes can be used for market manipulation. By creating fake videos that portray events impacting the business, individuals with ill intentions could manipulate stock prices. This poses a direct threat to the financial well-being of the company and its shareholders.

Deepfake videos can tarnish the reputation of businesses by depicting key figures engaging in inappropriate or unethical behavior. Even if the content is entirely fabricated, the public and stakeholders may react negatively, resulting in loss of trust and credibility. Competitive Disruption: Competing businesses could use deepfakes to disrupt their rivals. By creating fake videos suggesting internal conflicts, financial troubles, or other damaging scenarios, they may aim to gain a competitive advantage. This can lead to a loss of customers, partners, and marketshare.

In one instance, scammers defrauded a UK (United Kingdom) based firm by impersonating the Chief Executive Officer (CEO) [26]. He convinced employees from the finance department to transfer $220,000 to an account controlled by the scammers [26]. Symantec, a cybersecurity company, revealed that deepfakes and social engineering was used to defraud three CFOs (Chief Financial Officer) of undisclosed substantial funds [29]. In addition to these findings, Forrester Research [29] predicted a monetary loss of $250 million by the end of 2020 from deepfake frauds. With the continuous advancement of DT, businesses are likely to continue suffering considerable financial losses from deepfake scams. [Shadrack Awah Buo, 2020].

DETECTION TOOLS AND METHODS

In the ongoing battle against deepfake technology, the quest for effective detection tools and methods has become paramount. As artificial intelligence evolves, so do the intricacies of creating and identifying synthetic media. This research paper navigates the landscape of detection strategies, aiming to shed light on the arsenal available to discern real from manipulated content. From machine learning algorithms to emerging technological innovations, understanding how to unmask deepfakes is crucial for maintaining trust in our digital information ecosystem. This exploration delves into the methods employed to detect the subtle nuances of artificial manipulation, presenting a comprehensive overview of the current state of detection and the challenges that lie ahead.

Detecting deepfakes is a challenging task due to the increasing sophistication of the technology. Researchers and developers employ a variety of methods to identify synthetic media and distinguish it from authentic content. Here are some common methods used to detect deep fakes:

Blinking Patterns

Blinking patterns refer to the natural rhythm and frequency of a person's eye blinks. Deepfake algorithms may struggle to accurately replicate natural blinking patterns. Inconsistencies, such as abnormal or irregular blinking rates, can be indicative of facial manipulation. Analyzing the timing, duration, and regularity of blinks in a video helps in identifying potential deepfake content.

Facial Analysis

Facial analysis involves examining facial features, expressions, and movements to determine authenticity. Facial analysis for deepfake detection comprises analyzing facial expressions, eye movements, lip synchronization, and overall facial dynamics. Algorithms can compare the facial characteristics in a video to those in a reference dataset to detect any abnormalities or inconsistencies that could suggest tampering.

Reverse Engineering

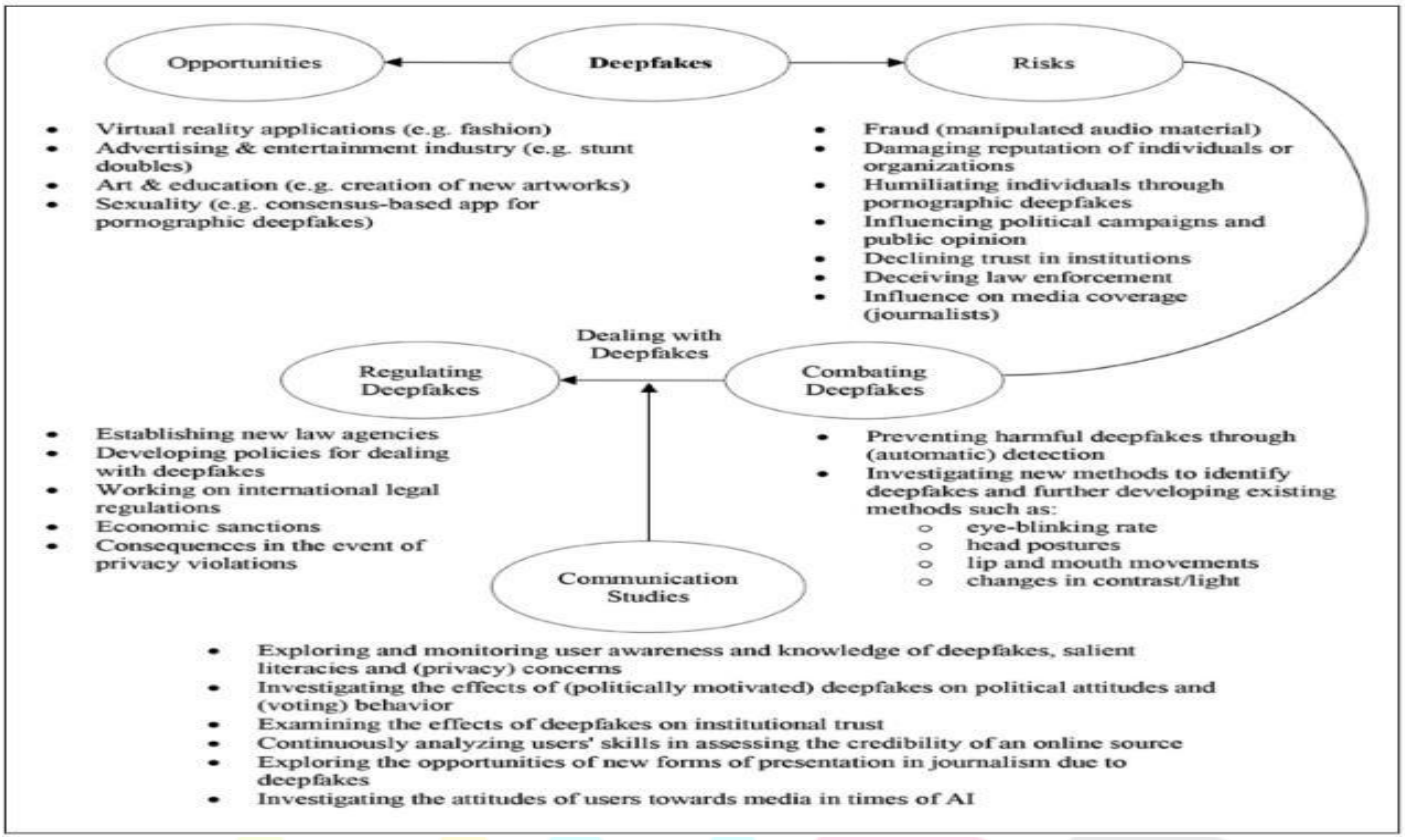
Reverse engineering involves analyzing a technology or system to understand its internal mechanisms, design, and functionality. Researchers may reverse engineer deepfake models to gain insights into their

architecture, parameters, and generation processes. By understanding how deepfakes are created, developers can design more effective detection algorithms. Reverse engineering also aids in recognizing patterns, artifacts, or unique identifiers associatedwith deepfake generation.

Artifact Analysis

Artifact analysis involves examining anomalies, distortions, or unintended elements introduced during the generation of synthetic content. Deepfake generation frequently creates artifacts like strange skin textures, irregular lighting, or errors. Artifact analysis algorithms seek to detect these anomalies in both visual and auditory material. Visual abnormalities around face borders, for example, or audio artifacts in modified speech, can be indicators of deepfakemanipulation.

Figure 1. Model of dealing with deepfakes



IMPACT OF DEEPFAKE ON SOCIETY

"This is developing more rapidly than I thought. Soon, it's going to get to the point where there is no way that we can detect [deepfakes] anymore, so we must look at other types of solutions. "

Hao Li

Deepfake Pioneer & Associate Professor

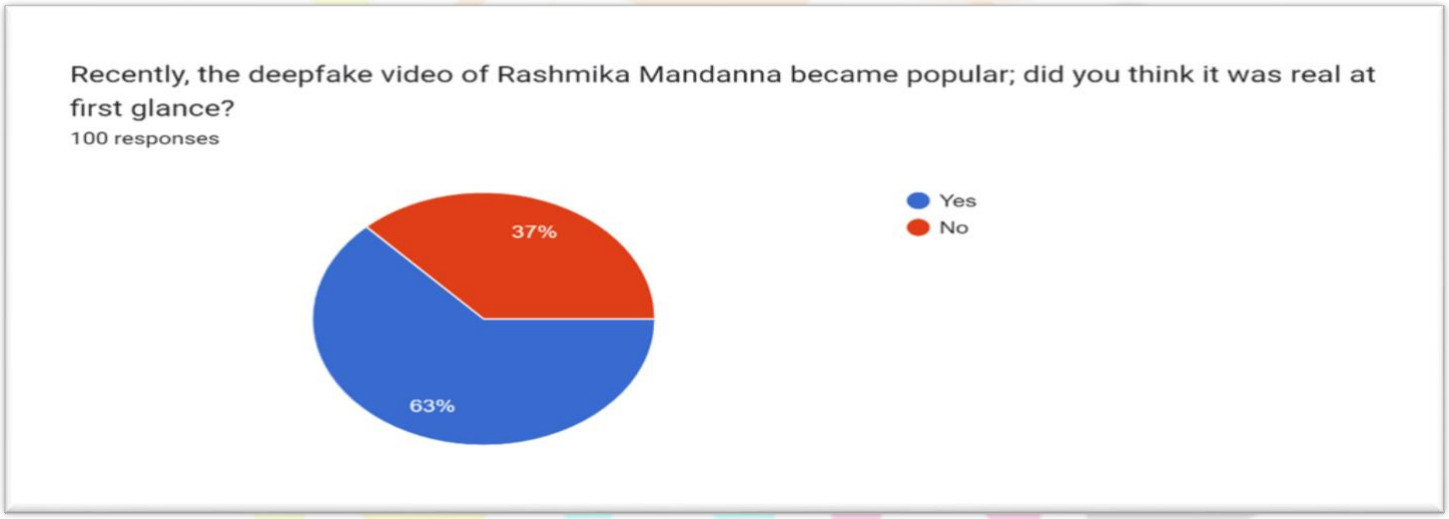
Deepfake technology's widespread usage, particularly in the generation of sexual content without authorization, has substantial psychological and emotional consequences for people and society. Victims face a harrowing invasion of their privacy and autonomy, as well as great emotional upheaval, humiliation, and embarrassment when their private moments are abused. Anxiety and a sense of powerlessness are exacerbated by the fear of reputational harm and the deterioration of personal connections. Deepfake legal ambiguities exacerbate these emotional costs, producing an environment of dread and distrust. Beyond individual suffering, the social ramifications shape attitudes of technology, privacy, and ethical limits, stressing the urgent need for complete remedies that include technical protections, legislative reforms, and increased public awareness.

Case of deep fake pornography

Actor Rashmika Mandana's manipulated video has sparked debate in India over the threats posed by deepfakes. But she is not the only victim of manipulated content created using artificial intelligence (AI) tools. There's a darker underbelly of AI-generated content that barely makes it to the headlines and often gets pushed under the carpet.

Deepfake pornography featuring celebrities, once relegated to the obscure corners of the internet, has now proliferated onto mainstream social media platforms.

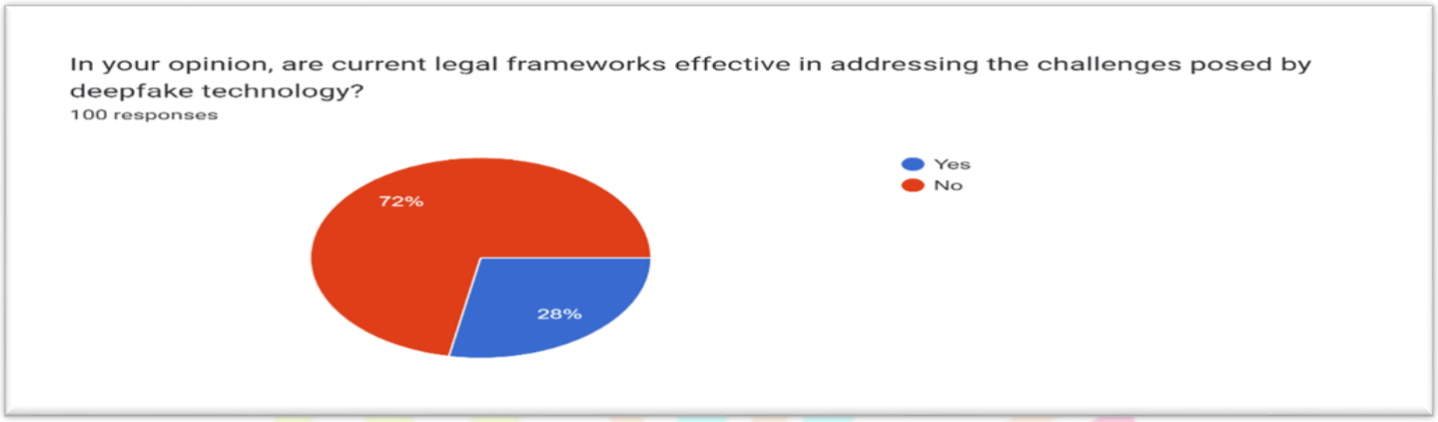
The actress took her social media platform to address and monitor the issue, sharing her concerns through an Instagram story.



The visual representation illustrates the information gathered through a survey conducted by the author.

EXISTING LEGISLATION OF DEEPFAKE

In the realm of combating deepfake shenanigans, the legal battleground is a patchwork quilt of approaches. The United States kicked off the show with its Malicious Deep Fake Prohibition Act in 2018, attempting to pin down the slippery world of synthetic media. Europe followed suit, waving the GDPR flag in May 2018, while also throwing down the gauntlet with the EU Code of Practice on Disinformation. Meanwhile, over in China, it's less about specific deepfake laws and more about putting a "label" on it. The whole scene is like a dance where everyone's got a different rhythm. This research paper takes a stroll through these legislative landscapes, exploring the challenges and nuances that each country brings to the table in the ongoing battle against the rise of deepfake mischief.



The visual representation illustrates the information gathered through a survey conducted by the author.

USA

The United States took early steps to address concerns related to artificial intelligence, notably with legislation targeting deepfake technology. In December 2018, the Malicious Deep Fake Prohibition Act of 2018 was passed by the U.S. Congress, marking the first attempt to define and regulate deepfakes. Subsequently, in June 2019, the DEEPFAKES Accountability Act was introduced. However, this act faced public opposition due to perceived vagueness in its definitions and potential conflicts with the First Amendment of the U.S. Constitution, which safeguards freedom of speech. During the same year, Congress proposed the Deepfake Report Act of 2019, which mandated the U.S. Department of Homeland Security to regularly issue evaluation reports on deepfake technology. Notably, some individual states responded promptly to concerns about the misuse of deepfakes, particularly in cases involving "pornographic videos" and "political elections." These state-level responses reflect a recognition of the need to address specific challenges posed by deep fake technology at both federal and state levels

India

In the context of the Information Technology Act (IT Act) in India, there are specific provisions that can be relevantto combat the misuse of deepfake technology.

Section 66D - Cheating by personation using a computer resource. This section deals with cases where a person cheats by posing as another person using computer resources. Deepfakes, which involve creating manipulated videos or images to impersonate someone, could fall under this provision. Section 43 - Unauthorized access: Unauthorized access to computer resources is covered under Section 43 of the IT Act. If deepfake technology involves unauthorized access to someone's personal data or computer systems, this section may be applicable. Defamation Laws: While not explicitly under the IT Act, defamation laws could be invoked if deepfake technology is used to create and spread

false information that harms someone's reputation. The victim may pursue legal action for defamation. Deepfakes can infringe upon an individual's right to privacy. Depending on the circumstances, relevant provisions related to privacy under the IT Act and other privacy laws may be applicable.

European Union

In April 2018, the European Commission released a comprehensive open letter titled "Tackling Online Disinformation: a European Approach," outlining key principles to prevent the unlawful manipulation of public opinion by information publishers. Subsequently, in May of the same year, the European Union officially enforced the General Data Protection Regulations (GDPR), which established stringent rules governing the use of deep synthesis technology. These regulations aimed to safeguard personal data, especially citizens' images vulnerable to misuse in deepfake scenarios. Building on this, in June 2018, the European Council adopted the EU Code of Practice on Disinformation, actively advocating for industry self-regulation. This initiative consciously sought to limit and control the spread of illegal content related to "deepfake" technologies, reflecting a commitment to addressing challenges posed by deceptive online content at a regional level.

China

In China, there is no specific legislation dedicated to addressing deepfake technology. Instead, the country emphasizes the standardization and restriction of the creation, release, and dissemination of deepfake content. This approach is rooted in the protection of citizens' rights concerning their portraits and reputation, along with the broader goals of safeguarding national and social security. Notably, China's legal regulations primarily focus on imposing an obligation to label deepfake content. However, a significant drawback is the absence of punitive measures for violations of this labeling obligation. While the regulations emphasize the importance of labeling, the lack of legal consequences diminishes the practical value of these provisions, leaving a gap in effective legal protection.

WHAT CAN BE DONE?

In combating the threats posed by deepfakes, a critical aspect lies in the continuous advancement of technology. This involves the development and enhancement of deepfake detection algorithms capable of identifying manipulated content, the exploration of blockchain technology for secure media verification, the creation of sophisticated media forensics tools to analyze digital content, and the implementation of public awareness campaigns to promote media literacy and critical consumption habits, ultimately mitigating the impact of deceptive synthetic media.

Numerous computer science publications have delved into the detection and implications of deepfakes, with a focus on developing techniques to identify and trace their origins. Detection methods include analyzing foreground and background in image swaps, key points detection, evaluating facial expressions, head movements, teeth and eyes reflections, mouth movements, mesoscopic image properties, and eye blinking anomalies. Some propose blockchain-based solutions for source tracing. While these technical approaches aim to regulate deepfakes by aiding identification and supporting decisions on content removal, certain weaknesses persist, such as challenges with low-quality images, difficulties when subjects don't look directly into the camera, and limitations in verifying blinking rates due to factors like mental health or dopamine activity. Some studies also face limitations in generalizability due to small dataset sizes. Despite promising strides, ongoing development is needed to address these shortcomings and enhance the overall effectiveness of deepfake detection methods.

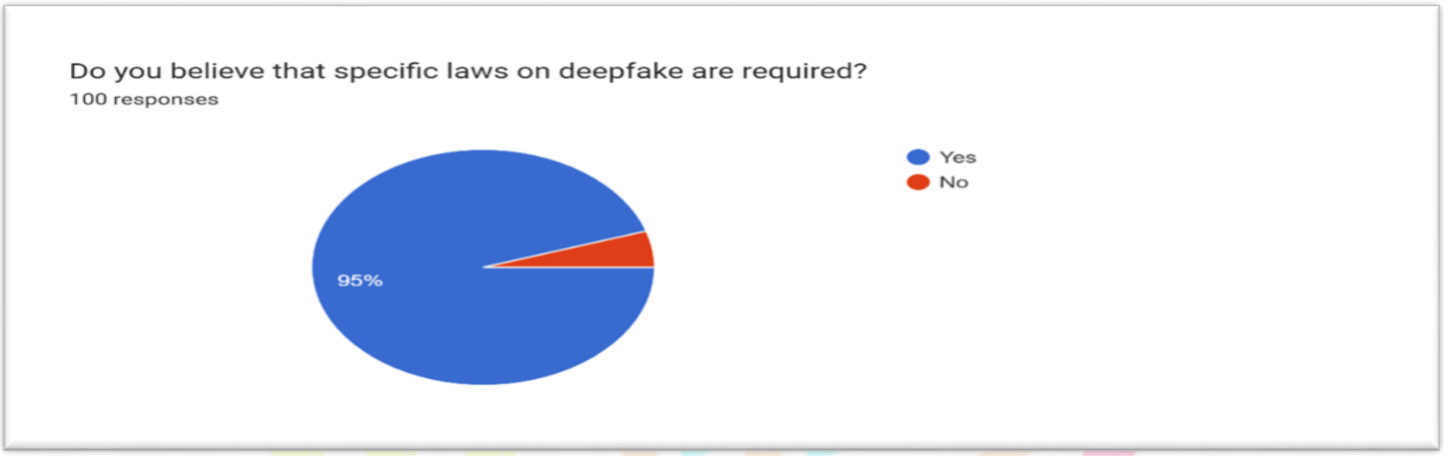
Legal Measures

To address the challenges of deepfakes, legal frameworks must evolve to encompass specific

measures. This includes criminalizing the creation and distribution of malicious deepfakes, enacting laws to protect victims and facilitate the swift removal of deceptive content, and strengthening intellectual property laws to cover unauthorized use of an individual's likeness or voice for synthetic media. These legal measures provide a foundation for holding perpetrators accountable and offering recourse for those affected by the malicious use of deepfake technology.

Various legal scholars, such as Caldera (2019), Citron and Chesney (2018, 2019), Hall (2018), and Silbey with Hartzog (2019), have explored the legal regulation of deepfakes. Existing laws, such as the right to

protect one's image and copyright regulations, offer some protection but are not fully tailored to the unique characteristics of deepfakes. The inadequacy of current laws is evident in issues related to unlawful pornography and the need for potential new agencies to address deepfake problems effectively. Military involvement in armed conflicts, covert investigations regarding foreign government threats, and the possibility of economic sanctions have also been considered (Citron & Chesney, 2018, 2019). While legal discussions often focus on the USA, Farish (2020) explores the applicability of English law, emphasizing the necessity for international regulations due to the global nature of deepfake creation and dissemination. Recommendations include organizations developing policies to combat fake news and using algorithms to prevent misinformation spread (Hall, 2018). Despite the absence of draft laws, legal perspectives propose diverse strategies, including new agencies, international regulations, and economic consequences for privacy violations, to effectively address the challenges posed by deepfakes.



The visual representation illustrates the information gathered through a survey conducted by the author.

Regulatory Approaches

Regulatory bodies play a pivotal role in overseeing and enforcing measures to counter deepfake threats. This involves mandating compliance requirements for online platforms, setting standards for deepfake detection and mitigation, fostering international cooperation to address cross-border challenges, and introducing transparency regulations that hold technology companies accountable for their efforts. By combining regulatory oversight with technological innovation and legal measures, a comprehensive approach emerges to safeguard against the harmful impacts of deepfakes and create a more secure digital landscape.

CONCLUSION

In the ever-evolving landscape of deepfake threats, this research underscores the critical need for a comprehensive and collaborative approach. The multifaceted nature of combating AI-generated misinformation demands a delicate balance between technological innovations, legal frameworks, and effective regulations. As we navigate this complex terrain, the collective effort to address deepfake risks becomes crucial for maintaining trust in digital information and protecting individuals and society at large.

The complexity of the deepfake challenge isn't one-dimensional. It's a puzzle with technological innovation, legal frameworks, and effective regulations as its pieces. Each element must complement the others to form a cohesive defense against the manipulation of digital content. This is not a solo mission but a collective effort where the synergyof technology, law, and regulation becomes our arsenal.

As we tread through this complex terrain, the need for a joint approach becomes crystal clear. Deepfake risks aren't isolated threats; they permeate the very fabric of our digital existence. A united effort isn't just an option; it's a necessity to maintain trust in the information we encounter daily.

Trust is the linchpin in this digital age. If we can't trust the authenticity of what we see and hear, the foundations of our digital society crumble. Hence, the collective endeavor to combat deepfake risks is not just

about technologicalprowess; it's about preserving the essence of trust in our interconnected world.

This research stands as a call to arms, emphasizing that the battle against deepfakes is not a solitary one. It's a collaborative effort that demands a Spartan resolve, devoid of unnecessary complexity. In simplicity, we find strength
– strength to fortify our digital landscape and protect the very core of our societal trust.

REFERENCES

Westerlund, M. 2019. **The Emergence of Deepfake Technology: A Review**. *Technology Innovation ManagementReview*, 9(11): 40-53. http://doi.org/10.22215/timreview/1282

Jones, V. A. (2020). *Artificial intelligence enabled deepfake technology: The emergence of a new threat* (Doctoraldissertation, Utica College).

Buo, S. A. (2020). The emerging threats of deepfake attacks and countermeasures. *arXiv preprint arXiv:2012.07989*.

Diakopoulos, N., & Johnson, D. (2021). Anticipating and addressing the ethical implications of deepfakes in thecontext of elections. *New Media & Society*, *23*(7), 2072-2098.

Liu, M., & Zhang, X. (2022, December). Deepfake Technology and Current Legal Status of It. In *2022 3rdInternational Conference on Artificial Intelligence and Education (IC-ICAIE 2022)* (pp. 1308-1314). Atlantis Press.

Collins, A. (2019). *Forged authenticity: governing deepfake risks* (No. REP_WORK). EPFL International RiskGovernance Center (IRGC).

Feeney, M. (2021). Deepfake Laws Risk Creating More Problems Than They Solve. *Regulatory Transparency Project*.

O'Halloran, A. (2021). *The Technical, Legal, and Ethical Landscape of Deepfake Pornography* (Doctoral dissertation, Brown University).

Godulla, A., Hoffmann, C. P., & Seibert, D. (2021). Dealing with deepfakes–an interdisciplinary examination of the state of research and implications for communication studies. *SCM Studies in Communication and Media*, *10*(1), 72-96.

R. Katarya and A. Lal, "A Study on Combating Emerging Threat of Deepfake Weaponization," *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2020,pp. 485-490, doi: 10.1109/I-SMAC49090.2020.9243588.

Zhao, H., Zhou, W., Chen, D., Wei, T., Zhang, W., & Yu, N. (2021). Multi-attentional deepfake detection. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 2185-2194).

yrone Kirchengast (2020) Deepfakes and image manipulation: criminalization and control, Information & Communications Technology Law, 29:3, 308-323, DOI: 10.1080/13600834.2020.1794615

Gieseke, A. P. (2020). " The New Weapon of Choice": Law's Current Inability to Properly Address DeepfakePornography. *Vand. L. Rev.*, *73*, 1479.

https://www.indiatoday.in/india/story/let-alone-rashmika-mandanna-internet-is-filled-with-deepfake-bollywood-porn-2459404-2023-11-07

https://www.researchgate.net/publication/350663190_Dealing_with_deepfakes_-_an_interdisciplinary_examination_of_the_state_of_research_and_implications_for_communication_studies

Dealing with deepfakes - An interdisciplinary examination of the state of research and implications for communication studies