Deepfakes: The Legal Implications

Trishana Ramluckan
University of KwaZulu-Natal, South Africa

RamluckanT@ukzn.ac.za

Abstract: The development of deepfakes began in 2017, when a software developer on the Reddit online platform began posting his creations in which he swapped the faces of Hollywood celebrities onto the faces of adult film artists, while in 2018, the comedic actor Jordan Peele posted a deepfake video of former U.S. President Obama insulting former U.S. President Trump and warning of the dangers of deepfake media. With the viral use of deepfakes by 2019, the U.S. House Intelligence Committee began hearings on the potential threats to U.S. security posed by deepfakes. Unfortunately, deepfakes have become even more sophisticated and difficult to detect. With easy accessibility to the applications of deepfakes, its usage has increased drastically over the last five years. Deepfakes are now designed to harass, intimidate, degrade, and threaten people and often leads to the creation and dissemination of misinformation as well as creating confusion about important state and non-state issues. A deepfake may also breach IP rights e.g., by unlawfully exploiting a specific line, trademark or label. Furthermore, deepfakes may cause more severe problems such as violation of the human rights, right of privacy, personal data protection rights apart from the copyright infringements. While just a few governments have approved AI regulations, the majority have not due to concerns around the freedom of speech. And while most online platforms such as YouTube have implemented a number of legal mechanisms to control the content posted on their platforms, it remains a time consuming and costly affair. A major challenge is that deep fakes often remain indetectable by the unaided human eye, which lead to the development by governments and private platform to develop deep-fake detecting technologies and regulations around their usage. This paper seeks to discuss the legal and ethical implications and responsibilities of the use of deepfake technologies as well as to highlight the various social and legal challenges which both regulators and the society face while considering the potential role of online content dissemination platforms and governments in addressing deep fakes.

Keywords: Deepfakes, Artificial Intelligence, Regulations, Ethics, Detection

1. Introduction

With reference to Brandon (2018) deepfakes are a form of synthesised media which are digitally altered (Witness Lab Media, 2020). The purpose for which is for example to replace an individual's "likeness" with that of another. Deepfakes have the capability to manipulate the human characteristics through deep generative methods. Deepfakes are not a new technology, although it is becoming more difficult to spot with the human senses as they utilise and apply powerful techniques from machine learning and artificial intelligence in order to manipulate or create visual and audio content with the motive to easily deceive. The key machine learning techniques that are utilized in deepfake creation are built upon deep learning and involve the training of generative neural network architectures including autoencoders or generative adversarial networks (GANs).

While deepfake technology creates new possibilities in filmmaking, which may include affordable video production and the generated but interactive videos depicting late celebrities, they have also become infamous for their potential use in creating child abuse material, pornographic videos, revenge porn, fake news, hoaxes, bullying, and financial fraud and have the potential to disinform the public and promote hate speech which ultimately undermines the core functions and norms of democratic systems. This results in hindering the public's ability to participate in decisions that may affect them and/or in determining collective agendas as well as promoting political will through any informed decision-making mechanism i.e., skewed decision making based on misleading information. This caused both industry and government to detect and limit their use of deepfake technology. With deepfake technology being easily available to the public, it has also been a leading cause of disruptions in the entertainment and media industries. Deepfakes, even with its benefits are increasingly being used in the political arena- this includes the dissemination of misinformation about political candidates and the release of fake statements from world leaders. A prominent example occurred in 2018, with a viral video depicting a deepfake-generated former President of the US Obama making a statement which was not actually real. The deepfake video, in fact, intended to demonstrate the capabilities of deepfake technology in manufacturing images and voices. If left unregulated, the evolution of this technology, does have the potential to cause mayhem by spreading disinformation. While some may argue that deepfake technology is comparable to the Enigma Machine (Hern, 2014) used in World War II by the German forces, the deceptive use of the Machine would need to be evidenced for it to be considered as fraud.

2. Deepfake Types and Challenges Posed

Deepfake technology has progressed at an alarming rate in the past decade and appear in three very general categories which includes:

2.1 Face Swapping

Face swapping involves or pertains to the replacing one's person's face with that of another in either a photo or video content.

2.2 Lip Syncing

Lip syncing pertains to the making of another person appear to say something they are not in audio or video content.

2.3 Puppet Technique

The Puppet technique refers to the fake movements of an individual in an unnatural manner.

While deepfake technology has many benefits, it does affect public figures more negatively than any other sector. (Ask the divorcee!!) The nonconsensual deepfakes that may depict celebrities in compromising situations are problematic, but it remains an important example of what this technology can produce. With reference to Bass and Penning (2023) deepfakes of celebrities have been used widely in advertising campaigns but are also now depicting political figures which may affect them with a possible loss of an election.

Used maliciously, deepfakes can inflict serious harm not only to individuals, but also within the social and democratic systems. This technology can and has been misused to commit fraud, extortion, bullying and intimidation, and has gone as far as to creating false evidence- manipulating both public debates as well as destabilising political processes. With further reference to Bass and Penning (2023), it should be considered that previously the majority of deepfakes have been pornographic videos which were produced without the consent of the women in which they are falsely depicted. This also purports gender discrimination related to the use of the technology, as this negatively affects women and demonstrates a gender disproportionality. Those who are most vulnerable to malicious deepfakes are the individual victims of fraud, blackmail, disinformation, and non-consensual pornography. Victims of disinformation spread using deepfake technology which includes the general public, businesses, and most predominantly public figures (politicians and celebrities).

While manipulated media is not a new concept, deepfakes have become more difficult to detect than previous techniques and does cause a measure of distrust in media outlets (traditional and new) (Boucher, 2021). Furthermore, various features of the current technical, social and legal context may enhance the risks associated with the technology e.g., the widespread use of social media and private messaging applications permits users with a method of rapid dissemination and altering of content with little to no monitoring. Regarding the social context deepfakes are appear aligned with an increasing notion of mistrust and polarisation while the legal status of deepfakes continue to vary dependent upon jurisdictions and is further complicated by potentially malicious users who may evade and thwart detection and enforcement efforts. With further reference to Boucher (2021) deepfakes, while not the only source of these social, technological and legal concerns, have developed a symbiotic relationship with other malevolent role players within this context, while still benefitting and prospering in this environment making significant contributions to its maintenance and development.

According to Waldemarsson (2020), deepfakes have the ability to become weaponized by harmful actors which include how deepfakes may manipulate elections e.g., hypothetically speaking- on the eve of an election, a video could surface showing a candidate engaging in some sort of misconduct, thereby potentially affecting the outcome of the election.

Deepfake content also has the ability to deepen social division e.g., Russia, a country that has developed a reputation for disseminating propaganda with an ultimate objective to divide the U.S. public (Posard et al., 2020). However, it must be noted that the U.S.- politically motivated by partisan debate, uses a variety of propaganda tactics to smear, and defame the opposition parties.

3. Deepfakes and Disinformation

Deepfakes, through technology, has been the cause of multiple disinformation instances which may vary. There still remains numerous deepfake implications which include the Political, Financial and Reputational. The examples below represent the various instances on how deepfakes may be responsible in the spreading of disinformation in the various categories.

3.1 The Political Damage of Deepfakes

The race for the Republican Party presidential nomination has experienced numerous deep fake attempts- the main purpose to which is to discredit potential candidates. Earlier in 2023, the Florida Governor Ron DeSantis' presidential campaign "War Room" appeared to release a video which depicted realistic deepfake photos of the former President Donald Trump hugging and even kissing the nose of Dr. Fauci, who is the former director of the National Institute of

Allergy and Infectious Disease. While the DeSantis Campaign admitted to the deep fake video, it did create a mild knock-on effect relating to the creation of uncertainty. Uncertainty with reference to Vaccari and Chadwick (2020) remains a cognitive impact to promote disinformation. This has led to the US Congress as well as the federal government attempting to regulate the use of artificial intelligence-generated media and in August 2023, the Federal Election Commission opened public commentary proposing a rule that all AI productions should fall under the regulations of fraudulent misrepresentation of campaign authority (McKenzie, 2023).

Another example of disinformation spread through deepfakes occurred in March of 2022. A deepfake video began circulating on social media- the 'video' was approximately a minute in length and depicted President Zelenskyy of Ukraine appearing to advise his soldiers to lay down their arms and surrender during the Russian invasion of Ukraine. The Russian Social Media had promoted the video, (WHO DID YOU BELIEVE ABOUT THIS AND WHY – THIS IS A FUNDAMENTAL POINT/REASON ABOUT ALL DECEPTION. WHY DO YOU BELIEVE IT WAS THE RUSSIAN EXPLANATION AND NOT THE TRUTH OF THE VIDEO? THIS IS FUNDAMENTAL. but it had been later debunked with Facebook and YouTube (YOU BELIEVE THEM?) having it removed from their platforms. However, Twitter allowed the video to continue on its platform- but had informed the public that the video was possibly fake and would only remove it once it had been confirmed as a deepfake. It was later revealed that hackers had inserted the disinformation into a live scrolling-text news crawl on TV station Ukraine 24. The deepfake video had appeared briefly on the website of the broadcaster with further claims that President Zelenskyy had fled the Ukrainian capital. While it remained unclear as to the creator of the deepfake video, the only recourse was for President Zelenskyy to respond with his own video, stating, "We don't plan to lay down any arms. Until our victory." I CAN SEE THE SIDE YOU ARE ON. THAT DETERMINES YOUR BELIEF? YES OR NO? THIS IS WHAT LEADS TO DECEPTIVE TECHNIQUES BEING SO POWERFUL. IF A DEEP FAKE WAS TOTALLY REALISTIC THEN TELL THE VIEWERS IT IS A B=DEEP FAKEMAND PROPAGANDA. IF THAT IS WHAT THEY WANT TO BELIEVE, THEY WILL.

Political disinformation remains the biggest risk of deepfakes and a well-timed and executed deepfake during an election campaign would result in enormous damage on various levels.

3.2 Damage of Deepfakes in Finance

Deepfakes can also result in huge financial losses as was the case in 2019, where the CEO of a UK-based energy firm under the impression that he was on the phone with his boss (the chief executive of firm's the German parent company) merely followed the 'boss's' directive in transferring €220,000 (approx. $243,000) to the bank account of a Hungarian supplier. The voice was in fact that of a criminal, using AI voice modification technology to emulate the CEO's actual voice. This was one of the first cases in which AI-synthesized audio was used for the recreation of an actual voice.

3.3 The Reputational Damage of Deepfakes

Deepfakes have become known to cause irreparable reputational damage. Early in 2021, international news had exposed an incident involving the use of alleged deepfakes as a cyberbullying scheme. It involved a mother who allegedly modified images and videos of her daughter's cheer team members. The deepfake images portrayed the teammates consuming alcohol, vaping, and posing nude, all dismissible conduct from the cheerleading team. The mother had also allegedly encouraged suicide and while this had been deemed as a case of cyberbullying, the charges were later dropped.

With reference to Lock (2023), AI deepfakes create a significant reputational risk. And unfortunately, many celebrities have become the victim of many fake narratives, inflammatory statements, and/or explicit content that they would never normally have consented to. The concern is the rapid rate that AI-generated content can spread especially on social media platforms. Reputational risks spiral far beyond the immediate embarrassment of a falsely portrayed action or event. Deepfakes can erode public trust (both generally, and in terms of personal brand) and, in the hands of malevolent actors, can fuel misinformation and deception campaigns (*ibid*).

4. The Role and Challenges of Law in AI

The regulation of political deepfakes presents a significant challenge. Regarding the legal implications of deepfake usage for malicious purposes, as in most jurisdictions, any piece of legislation seeking to ban deepfake usage of political officials or candidates requires a complete reworking in order to align to the protection of freedom of expression within the jurisdiction. The complexity would arise whereby, for example, satirical deepfakes would have to be allowed and there would need to be a clear distinction between deepfakes for artistic purposes and those used for malicious purposes. For the prosecution of perpetrators using deepfakes for malicious purposes, reasonable evidence together with intent would be required and proved. These requirements pose a significant challenge for lawmakers. While reasonable evidence is difficult to obtain demonstrating intent art and satire can also be subjective, and more often than not become the means for unintended purposes (Farish, 2022).

Legal recourse becomes extremely difficult in any jurisdiction. Section 4.1.1 provides an overview of international legislation on AI deepfake technology usage, while Section 4.1.2 provides the South African response to the use of deepfake technology usage.

4.1 International Legislation

4.1.1 The United States

Currently, in the US, there is no federal legislation in existence in addressing the potential threats of deepfake technology. However, at the end of 2019, Congress had approved the National Defense Authorization Act (NDAA). Section 5709 of the NDAA now premises for the Director of National of Intelligence to report on the use of deepfakes by international governments, its ability to spread misinformation, and its potential impact on national security. The main criticism of the ACT is that while it premises for the regulation of threats of deepfakes emanating from sources outside the nation, it does not address the issues that deepfakes may cause within the US.

Only a minority of US states have passed pieces of legislation regarding emerging deepfake technology. Texas approved the S.B. 751 and California passed AB730 in 2019. Both these laws ban the use of deepfakes which may be used to influence upcoming elections. California's legislation AB602, Georgia's S.B. 337 as well as Virginia's SB 1736 were also approved for the prohibition of the creation and dissemination of non-consensual deepfake pornography in 2019, while in 2020 New York law S6829A introduced the rights for legal action against the unlawful publication of deepfakes. In more recent days, a number of bills to regulate artificial intelligence (AI) have been proposed and enacted in several states in the duration of 2022. While the US legislative developments in AI have progressed, in most states there still seems to be a distinct lack of applicable legislation regarding AI in general being introduced and/or enacted.

4.1.2 China

In China the government has recently enacted strict regulations, which have become known as Deep Synthesis Provisions. These Provisions prohibit the creation of deepfakes 'without the consent of the user and require confirmation that the content was generated using AI'. Although China, has often been criticised for the human rights regarding personal freedoms, it is currently one just one of a few countries which appears to impose a strict ban regarding the use of certain deepfakes. However, there are a few other countries offering some legal protection against the malicious and unlawful use of deepfake technology, including Germany where the general right of responsibility is enshrined under Section 22 of the German Basic Law. While this Law grants individuals the right to their own image, it does not explicitly address the deepfake technology platform, this law implies that deepfakes of individuals used without their consent is ultimately deemed illegal.

China's deepfake synthesis technology regulation became effective in January 2023. This new regulation is deemed to have two key purposes which include:

- Strengthening online censorship and;
- Keeping up with rapid advancement of new technologies.

With the ubiquitous nature of the Internet, it remains important to note that more is required, than just legislation to effectively control its usage. Furthermore, for the purpose of legitimacy of any regulation, a proper framework on cyberspace needs to be developed and implemented. China's deepfake synthesis regulatory system remains important as Technology Regulation (DSTR) primarily regulates two entities which includes Deep Synthesis Service Providers, which are companies that offer deep fake services or more so, provide users with technical support; as well as the Deep Synthesis Service users, which encompasses both organizations and people deep synthesis service to create, duplicate, publish or transfer information (Nnamdi et al., 2023).

4.1.3 The United Kingdom

The United Kingdom (U.K.) has established some deep fake legislations. However, the main criticism of the UK legislation remains its main focus on cases/instances of revenge porn. The Online Safety Bill 2023 (Chapter 50) remains the primary deep fake legislation in the UK. Prior to which, prosecutors in deep fake cases, were required to prove that the malicious actor had the intent to cause distress to malicious actors- an extremely difficult task. While a successful proof of intent may incur a two-year prison sentence of the perpetrator, a failure to prove intent with proof of creation ofmisleading deepfake may only incur a six-month prison term for the malicious actor. The Online Safety Bill further stipulates the main responsibilities of deep fake service providers. It assigns them with the responsibility of user-identification verification to ensure that malicious deep fakesare traced to their creators. The main concern to the UK legislation is that it appears to premise more towards revenge pornography. Section 13 (4) of the Bill, requires that contents harmful to adults be: (1)

taken down; (2) users' access to such content be restricted; and (3) "limited" recommendation and promotion of such content.

The United Kingdom emphasises the protection of individuals through amendments to the country's Online Safety Bill- including specific bans on deepfakes utilised for nonconsensual pornography. This has ultimately created challenges regarding First Amendment rights.

4.1.4 *The European Union*

The European Union Artificial Intelligence Act (EU AI Act) can be described as the first global initiative towards the regulation of AI. The Act endeavours to turn Europe into a global hub for trustworthy AI through harmonized rules regulating the development, marketing, and use of AI within the EU. The Act endeavours to ensure that AI systems in the EU provide a safe and respectful environment encompassing all fundamental rights and morals. The key objectives of the Act are to:

- Foster investment and innovation in AI,
- Enhance governance and enforcement; and
- To encourage a single EU market for AI.

The act seeks adoption in early 2024 prior to the June 2024 European Parliament elections. A grace or transition period of 18 months will be granted prior to the regulation becoming completely enforced. The AI Act has incorporated many other regulations in the EU regulating the different elements of the digital economy including the General Data Protection Regulation, the Digital Services Act, and the Digital Markets Act. Simply stated, the AI Act will not address data protection, online platforms or content moderation (Hoffmann, 2023).

4.2 South Africa's Response to Deepfake Legislation

The South African Cybercrimes Act represents the nations attempt to develop a comprehensive legislative response to cybercrime. This Act, however, was not the first South African piece of legislation which sought to address the problem of cybercrime.

In 2002, the Electronic Communication and Transactions Act (ECTA) was enacted to "provide for the facilitation of electronic communication and transactions" as well as to provide for the creation of a national e-strategy for the nation. The focus of ECTA is for the protection of "data" (electronic communication) as well as data messages" . The Film and Publications Board Act also addresses the penalties of the distribution of child pornography however failing in premising for the distinction between real pornographic images and deepfake images (Mabunda, 2021).

In South Africa, the concept of the 'right to identity' remains key to the development of deepfake regulations. The right to identity endeavours to protect the individuals in terms of their characteristics which includes an individual's likeness, image, voice, and other distinctive personality traits. The right to identity is legally recognised in South Africa, while the use of deepfakes may appear to infringe upon this right. Its important to acknowledge that deepfakes are created with deep learning software enabling end users to develop deceptive videos, audio as well as photographs of events and people that are indistinct from reality. In South African law this is contradictory to an individual's right to control the use of their characteristics. While it appears that South African law has failed to prohibit the creation and publication of deepfakes, the "right to identity" remains a fundamental liberty and liability for the publication of deepfakes may be established using principles in other fields of law, including the law of delict and criminal law. Detection of deepfakes is becoming difficult and their dissemination over the internet continues to evolve, which necessitates a new perspective on how to provide relevant recourse for victims of deepfakes whose right to identity has been violated. It also establishes the need for liability of people who may be tagged and party to deepfakes posted on social media platforms (Mashinini, 2020).

5. Discussion

Deepfakes have become even more prolific in the digital age, with the damage that they can and have caused. Deepfakes have an impact on society, on the citizenry, education, social welfare, politics, media, business, and everyday life in general. The simplicity in using deepfake technology has provided a means for end-users including apps FakeApp, which is a face-swapping app and Zao, a Chinese mobile app which uses movie clips, and Apple's text-to-speech (TTS) editing system to flourish and create chaos (Kietzmann, 2019).

With ease of access to deepfake technology, the superimposition and swapping of individuals faces into movies and television may appear appealing and humorous to some extent e.g., in 2019 a clickbait video entitled "KEANU REEVES STOPPED A ROBBERY '' included the use of a stuntman and voice actor with the actor's face being superimposed onto the actual stuntman (Bode, 2021). The video went viral across numerous social media platforms, even though it was falsified. And as entertaining as this may appear for many, it also demonstrates the ease of deepfake content creation and establishes a severe lack of accountability. This means that anyone anywhere, has the ability to create altered videos, pictures and audio which may appear realistic to the general public.

This creates the complexities relating to accountability and necessitates the development of regulations for more control over this type of technology, while still adhering to a nations basic rights including the freedom of expression (Diakopoulos and Johnson, 2019). Many politicians have also become the victims of deepfakes (Citron and Chesney, 2019). This technology has the ability of creating fake videos even inciting assassinations or even political figures like Speaker Nancy Pelosi slurring her speech (Denham, 2020). While this seems minor, it is known to cause severe reputational and economic damage. Deepfakes have also created a hotbed for fraud including activities on the dark web which uses deepfakes to blackmail, create pornographic videos, and execute identity theft (Security Firm, 2021).

Society and governments require applicable countermeasures when such activities impact personal liabilities such as non-consenting individuals, government officials, and organizations (Kietzmann et al., 2019, cited in Nour and Gelfand, 2021). Currently, there is no international convention against deep fake technology. At the United Nations Institute for Disarmament Research (UNIDIR) 2021 Innovations Dialogue on Deepfakes, Trust and International Security (Geneva 2021), explored the importance of trust for international security and stability and provided insight to the increasing deepfakes phenomenon and ways in which the technology use could undermine this trust.

6. Conclusion

Although deepfake technology has many advantages it has evolved to the extent that in many instances go undetected. With the ability to emulate humans in most ways it has that ability to portray fakes and allow these to appear as factual—spreading falsehoods and misinformation. Without the creation regulations, deepfake technology and malicious users have the potential to create irreversible damage.

The key issue remains that social media companies are permitted to provide independent decisions on content posted on their platforms, however, with reference to the latest case involving the posting of deepfake imagery of Taylor Swift, the US Government has acknowledged the responsibility of the social media companies in enforcing rules to prevent the spread of misinformation, and non-consensual, intimate imagery of existing people. While a case of libel maybe deemed plausible in this case – the question of attribution and reasonable evidence would need to be proved. Furthermore, would it be a case against the media platform hosting the images or the creator of the content itself. In this instance, it may be noted that X had removed the images from its platform with immediate effect also issuing a statement to the fact that the images were in fact fake.

Therefore, while there are other avenues in the legal denomination to prosecute the malicious use of deepfake technology, main concern remains however on the need to develop specific legislation or regulations that protect the right to one’s identity while also upholding the freedoms of speech and expression. Deepfake technology remains a powerful weapon which can blur the boundaries between fact and fiction, if left uncontrolled (Quirk, 2021). This emphasises the dire need for the development of an all-encompassing legislation or regulatory framework which must cover all aspects of deepfake technology and its usage. must be all encompassing, that is, they must cover all aspect sf deepfakes. An in depth deep fake regulation would premise for several deep fake malicious acts and the punitive consequences thereof, e.g. China’s Deep Synthesis Technology Regulation . Furthermore, it becomes more than a legal issue, but one of ethics and trust. This would lead to greater trust in the media, international and national security and sustainability, promoting a safer internet for all as well as preserving human dignity (Nnamdi et al., 2023).

References

Bass, DF., and Penning,. N. (2023). The Legal Issues Surrounding Deepfakes. Honigman LLP Attorneys and Counsellor’s. https://www.honigman.com/the-matrix/the-legal-issues-surrounding-deepfakes

Bode, L (2021). Deepfaking Keanu: YouTube deepfakes, platform visual effects, and the complexity of reception. Convergence: The International Journal of Research into New Media Technologies 27 (4) 135485652110304-934. https://doi.org/10.1177/13548565211030454

Boucher, P. (2021).” What if deepfakes made us doubt everything we see and hear?” European Parliament. https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690046/EPRS_ATA(2021)690046_EN.pdf

Brandon, J (2018). "Terrifying high-tech porn: Creepy 'deepfake' videos are on the rise". Fox News. Archived from the original on 15 June 2018. Retrieved 05 October 2023

Denham, H. (2020). Another fake video of Pelosi goes viral on Facebook. The Washington Post. Retrieved from https://www.washingtonpost.com/technology/2020/08/03/nancy-pelosi-fake-videofacebook

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

Fagan, K. (2018). “A viral video that appeared to show Obama calling Trump a ‘dips—‘ shows a disturbing new trend called ‘deepfakes,'” Insider, last modified April 17, 2018, accessed April 30, 2023, https://www.businessinsider.com/obama-deepfake-video-insulting-trump-2018-4 .

Farish, K. (2022) Political Deepfakes: social media trend or genuine threat? https://www.dacbeachcroft.com/en/gb/articles/2022/september/political-deepfakes-social-media-trend-or-genuine-threat/

Hern, A. (2014) How did the Enigma machine work? The Guardian, November 14, 2014. https://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game

Hoffmann, M. (2023) The EU AI Act: A Primer. CSET. https://cset.georgetown.edu/article/the-eu-ai-act-a-primer/#:~:text=The%20AI%20Act%20is%20a,systems%20across%20EU%20member%20states

Lock, O. (2023). The legal issues surrounding deepfakes and AI content. Farrer & Co LLP. https://www.farrer.co.uk/news-and-insights/the-legal-issues-surrounding-deepfakes-and-ai-content/

Mabunda, SM. (2021). The South African Legislative Response to Cybercrime. PhD Thesis- University of the Western Cape. https://etd.uwc.ac.za/bitstream/handle/11394/8693/mabunda_m_law-2021.pdf?sequence=1&isAllowed=y

Mashinini, N. (2020). The impact of deepfakes on the right to identity: a South African perspective. SA Mercantile Law Journal.Vol.3, No 32. https://journals.co.za/doi/epdf/10.47348/SAMLJ/v32/i3a5

McKenzie, B. (2023). Is that real? Deepfakes could pose danger to free elections. https://news.virginia.edu/content/real-deepfakes-could-pose-danger-free-elections

Quirk, C.(2021). The High Stakes of Deepfakes: The Growing Necessity of Federal Legislation to Regulate This Rapidly Evolving Technology. Princeton Legal Journal. https://legaljournal.princeton.edu/the-high-stakes-of-deepfakes-the-growing-necessity-of-federal-legislation-to-regulate-this-rapidly-evolving-technology/

Nnamdi, N., Adeyemi, O., and Abegunde, B. (2023). An Appraisal of the Implications of Deep Fakes: The Need for Urgent International Legislations. Available from: https://www.researchgate.net/publication/372611418_An_Appraisal_of_the_Implications_of_Deep_Fakes_The_Need_for_Urgent_International_Legislations [accessed Nov 10 2023]

Nour., N and Gelfand, J. (2021). Deepfakes: A Digital Transformation Leads to Misinformation. Conference Proceedings Insights and Issues that Challenge and Demonstrate the Role of GL. http://www.greynet.org/images/GL2021_Nour_and_Gelfand_pp.55-65.pdf

Vaccari, C and Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. Social Media + Society. https://journals.sagepub.com/doi/pdf/10.1177/2056305120903408

Witness Org (2020). "Prepare, Don't Panic: Synthetic Media and Deepfakes". Archived from the original on 2 December 2020. Retrieved 05 October 2023