Reverte
Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

DEEPFAKE EM ANGOLA: impacto, desafios e prevenção

Dra. Sandra Paula Gaspar Mainsel C. Jaime

Doutora em Ciências da Comunicação e em Mídia e Sociedade pela UAL - Universidade Autónoma de Lisboa - Portugal. Doutora em Philosophy in Business Administration e Mestra em Science in Business Administration pela FCU - Florida Christian University Estados Unidos. Graduada em Ciências da Comunicação pela UAN - Universidade Agostinho Neto - Angola. Docente do Curso de Comunicação Social na Faculdade de Ciências Sociais da UAN - Universidade Agostinho Neto – Luanda-Sul/ Angola.

ORCID: https://orcid.org/0000-0002-8632-8263

E-mail: sandramainsel@hotmail.com

RESUMO

Nos últimos anos, a tecnologia deepfake emergiu como uma inovação com potencial para criar vídeos, áudios e imagens falsificadas que se assemelham quase perfeitamente ao conteúdo real. Utilizando técnicas avançadas de inteligência artificial e aprendizagem profunda, os deepfakes representam uma ameaça significativa para as sociedades modernas. Em Angola, a chegada dessa tecnologia trouxe uma série de desafios preocupantes. O país, ainda em processo de desenvolvimento democrático e tecnológico, enfrenta riscos substanciais associados à manipulação de informações, como a influência nos processos eleitorais, a desestabilização de instituições e a violação da privacidade individual. Este artigo utiliza a metodologia de estudo de caso para examinar o impacto dos deepfakes no contexto angolano. A pesquisa focou na análise de casos específicos em que deepfakes foram utilizados para manipular a opinião pública e comprometer a integridade da informação. Através dessa abordagem, foi possível identificar os principais efeitos negativos dessa tecnologia, como a perturbação dos processos democráticos e a ampliação da desconfiança pública. As conclusões do estudo destacam que, para enfrentar os desafios associados aos deepfakes em Angola, é crucial implementar um conjunto de estratégias eficazes. Entre essas estratégias estão a criação de um regime jurídico específico, o desenvolvimento de tecnologias avançadas para detecção de deepfakes, e a promoção de campanhas de sensibilização e educação pública.

Palavras-Chave: Deepfakes; Desinformação; Angola; Manipulação de Imagem.

DEEPFAKE IN ANGOLA: impact, challenges, and prevention

ABSTRACT

In recent years, deepfake technology has emerged as an innovation with the potential to create falsified videos, audio, and images that closely resemble authentic content. Utilizing advanced artificial intelligence and deep learning techniques, deepfakes represent a significant threat to modern societies. In Angola, the arrival of this technology has introduced a series of concerning challenges. The country, still in the process of democratic and technological development, faces substantial risks associated with the manipulation of information, such as influencing electoral processes, destabilizing institutions, and violating individual privacy. This article employs a case study methodology to examine the impact of deepfakes in the Angolan context. The research focused on analyzing specific cases where deepfakes were used to manipulate public opinion and compromise the integrity of information. This approach identified the main negative effects of this technology, such as disrupting democratic processes and amplifying public distrust. The study's conclusions emphasize that addressing the challenges associated with deepfakes in Angola requires the implementation of effective strategies. Among these strategies are the establishment of specific legal frameworks, the development of advanced technologies for deepfake detection, and the promotion of public awareness and education campaigns.

Keywords: Deepfakes; Disinformation; Angola; Image Manipulation.

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

DEEPFAKE EN ANGOLA: IMPACTO, DESAFÍOS Y PREVENCIÓN

RESUMEN

En los últimos años, la tecnología deepfake ha emergido como una innovación con el potencial de crear videos, audios e imágenes falsificadas que se asemejan casi perfectamente al contenido real. Utilizando técnicas avanzadas de inteligencia artificial y aprendizaje profundo, los deepfakes representan una amenaza significativa para las sociedades modernas. En Angola, la llegada de esta tecnología ha traído consigo una serie de desafíos preocupantes. El país, aún en proceso de desarrollo democrático y tecnológico, enfrenta riesgos sustanciales asociados con la manipulación de información, como la influencia en procesos electorales, la desestabilización de instituciones y la violación de la privacidad individual. Este artículo utiliza la metodología de estudio de caso para examinar el impacto de los deepfakes en el contexto angoleño. La investigación se centró en el análisis de casos específicos en los que se utilizaron deepfakes para manipular la opinión pública y comprometer la integridad de la información. Este enfoque permitió identificar los principales efectos negativos de esta tecnología, como la perturbación de los procesos democráticos y la ampliación de la desconfianza pública. Las conclusiones del estudio destacan que, para enfrentar los desafíos asociados con los deepfakes en Angola, es crucial implementar un conjunto de estrategias efectivas. Entre estas estrategias se incluyen la creación de un marco jurídico específico, el desarrollo de tecnologías avanzadas para la detección de deepfakes y la promoción de campañas de sensibilización y educación pública.

Palabras clave: Deepfakes; Desinformación; Angola; Manipulación de Imágenes.

INTRODUÇÃO

Os *deepfakes* são mídia falsificadas criadas através de inteligência artificial (IA) e técnicas de aprendizagem profunda *(deep learning*).

O termo "*deepfake*" surgiu em 2017 quando um utilizador do Reddit, sob o nome "*deepfakes*", começou a postar vídeos pornográficos alterados digitalmente, usando imagens de celebridades. A tecnologia utilizada baseava-se em inúmeras imagens e vídeos de celebridades para aprender a imitar as suas expressões faciais e sobrepor o rosto de uma celebridade no rosto de atrizes de filmes pornográficos (Chawki, 2024).

A preocupação principal é que existem *softwares* de código aberto[1] e aplicações que tornam esta tecnologia acessível a qualquer pessoa. Para obter um bom resultado, ou seja, um deepfake capaz de enganar os utilizadores de redes sociais, é necessário ter um grande acervo de material (Molina; Berenguel, 2022). A duração do processo de criação de conteúdos dependerá das configurações de hardware utilizadas e das Redes Adversárias

[1] Softwares de código aberto (ou *open source software)* são programas cujo código-fonte é disponibilizado publicamente. Isso significa que qualquer pessoa pode visualizar, modificar e distribuir o código do software.

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

Generativas (GANs)[2]. Estas redes podem ter limitações tanto na implementação quanto na aplicação; por exemplo, para gerar imagens em full HD é necessário mais tempo e um hardware potente, além de um grande conjunto de dados (Kaur et al., 2024). Uma vez que o processo é realizado, a geração dos dados sintéticos torna-se mais rápida e eficiente.

A maioria dos *deepfakes* são de natureza pornográfica. A tecnologia por trás dos *deepfakes* é capaz de aprender e gerar novos dados a partir de conjuntos de dados existentes, como fotos, áudio e vídeo, que são processados através das GANs (Westerlund, 2019).

Face ao referido, o objetivo geral deste artigo passa por fornecer uma visão abrangente sobre os *deepfakes* em Angola, destacando os seus impactos, desafios e estratégias de prevenção, com o intuito de informar, analisar, identificar problemas e propor soluções eficazes para enfrentar essa crescente ameaça à integridade da informação e à segurança pública.

Quanto aos objetivos específicos definiu-se:

- Discutir como os *deepfakes* afetam a política, a mídia, a segurança pessoal e a privacidade dos cidadãos angolanos;

- Elencar os principais obstáculos que Angola enfrenta na identificação e combate aos *deepfakes*, incluindo limitações tecnológicas, legais e de conscientização pública;

- Sensibilizar o público e os profissionais sobre a existência e os perigos dos *deepfakes*, incentivando uma abordagem crítica e informada em relação ao consumo de mídia.

A investigação sobre *deepfakes* em Angola reveste-se de grande importância para compreender a extensão e as implicações desta tecnologia emergente no contexto local. Os *deepfakes,* enquanto avanço significativo em IA e manipulação digital, apresentam desafios únicos que necessitam de uma abordagem cuidadosa para proteger a integridade da informação e garantir a segurança pública.

[2] Goodfellow et al. (2014) introduziram as GANs, que consistem em duas redes neurais competindo entre si, resultando na geração de conteúdos altamente realistas. Após o treino, o modelo de IA pode gerar novas imagens, vídeos ou áudios que parecem autênticos.

Em primeiro lugar, o impacto social e político dos *deepfakes* pode ser profundo. Num país como Angola, onde a confiança nas instituições e na mídia pode ser vulnerável, a capacidade de criar vídeos falsos que imitam figuras públicas ou políticos tem o potencial de gerar desinformação e perturbar o ambiente político. Portanto, é crucial entender como esses conteúdos podem influenciar a opinião pública e desestabilizar o cenário político.

Além disso, os *deepfakes* podem afetar a segurança e a privacidade pessoal. A possibilidade de criar vídeos manipulados que comprometem a imagem de indivíduos pode levar a situações de assédio, chantagem e outros crimes (Kharvi, 2024). Compreender como esses ataques têm impacto nos cidadãos angolanos é essencial para desenvolver mecanismos de proteção e resposta adequados.

Outro ponto relevante são os desafios tecnológicos e legais enfrentados por Angola na deteção e combate aos *deepfakes.* O país pode encontrar dificuldades devido a limitações tecnológicas e lacunas na legislação. Portanto, identificar estes obstáculos e sugerir melhorias nas políticas e infraestruturas existentes é fundamental para enfrentar a disseminação de conteúdos manipulados.

Finalmente, a investigação contribui para o corpo académico existente sobre *deepfakes* e as suas consequências, oferecendo dados concretos para o contexto angolano. Ao propor soluções práticas e estratégias de prevenção, o estudo visa fornecer uma base sólida para futuras ações e políticas, abordando uma ameaça tecnológica crescente e disruptiva.

2 REVISÃO DA LITERATURA

2.1 A CONSTRUÇÃO DOS DEEPFAKES: Métodos e Tecnologias

A criação de *deepfakes* começa com a recolha de uma grande quantidade de dados visuais e/ou auditivos da pessoa-alvo, que pode incluir fotografias, vídeos e áudios disponíveis publicamente. Segundo Chesney e Citron (2019), a abundância de dados disponíveis na internet facilita a recolha de material necessário para criar *deepfakes* convincentes.

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

A criação de *deepfakes* envolve o uso de técnicas avançadas de IA para gerar imagens ou vídeos falsos que parecem reais. Através de métodos de aprendizagem de máquina, os sistemas são treinados para analisar e imitar características faciais, movimentos e expressões de uma pessoa específica. Entre as ferramentas usadas estão as GANs, que criam novas imagens a partir de dados existentes, ajustando continuamente para melhorar a semelhança com a realidade (Gupta et al., 2023).

Por exemplo, num vídeo deepfake, o rosto da pessoa-alvo pode ser sobreposto ao de outra pessoa, sincronizando os movimentos dos lábios e expressões faciais com o áudio falsificado (Kietzmann et al., 2020). Os *deepfakes* são refinados para aumentar o realismo, ajustando detalhes como iluminação, textura da pele e sincronia de áudio. Podem ser usadas técnicas de pós-produção para polir o resultado final, tornando-o ainda mais convincente (Westerlund, 2019).

Essas falsificações são cada vez mais sofisticadas e difíceis de detectar a olho nu, o que representa um desafio significativo para a verificação de factos e a proteção contra desinformação. De acordo com Paris e Donovan (2019), a capacidade dos *deepfakes* enganarem até mesmo observadores treinados sublinha a urgência de desenvolver métodos eficazes para a sua detecção e mitigação.

2.2 IMPACTOS NEGATIVOS DOS DEEPFAKES: desinformação, fraudes e violações de privacidade

Uma das maiores preocupações com os *deepfakes* é o seu potencial para disseminar desinformação. Podem ser usados vídeos manipulados para fabricar notícias falsas e desacreditar figuras públicas e políticos, sendo frequentemente tão realistas que conseguem enganar o público e influenciar a opinião pública de maneira significativa (Satariano; Mozur, 2023). Por exemplo, podem ser usados *deepfakes* para falsificar declarações de políticos, causando confusão e desconfiança entre os eleitores (Łabuz et al., 2024).

Os *deepfakes* também representam uma ameaça significativa à privacidade individual. A facilidade de acesso a software de código aberto para criar *deepfakes* significa que qualquer pessoa pode criar vídeos manipulados de outros, muitas vezes com fins maliciosos. Isso inclui a criação de vídeos pornográficos não consensuais, conhecidos como

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

pornografia de vingança, onde o rosto de uma pessoa é sobreposto ao corpo de uma atriz em filmes pornográficos. Tais práticas podem levar a graves consequências emocionais e sociais para as vítimas (Gosse; Burkell, 2020; Maddocks, 2020).

Além disso, podem ser usados *deepfakes* em esquemas de fraude e extorsão. Um exemplo disso é o uso de *deepfakes* para criar áudios ou vídeos falsos de gestores de empresas, enganando funcionários de modo que transfiram grandes somas de dinheiro para contas fraudulentas. Este tipo de crime, conhecido como "fraude de CEO"[3], está em ascensão e representa um grande risco financeiro para as empresas (Juan, 2023; Rancourt-Raymond; Smaili, 2023).

A capacidade de recorrer a *deepfakes* para criar vídeos falsos altamente realistas também pode ser utilizada para desestabilizar sociedades. Por exemplo, vídeos *deepfake* podem ser usados para incitar violência ou promover discursos de ódio, exacerbando tensões sociais e étnicas. A difusão de tais vídeos pode levar a protestos violentos e a uma quebra na ordem social (Pawelec, 2022; Pfefferkorn, 2021).

Noonan (2024) elenca as consequências de alguns *deepfakes* que surgiram nos últimos anos. Num caso ocorrido no Gabão em 2018, o Presidente Ali Bongo, que não aparecia aos olhos do público há muito tempo e que alguns pensavam estar morto, publicou um vídeo de um discurso. Os opositores políticos apelidaram o vídeo de *deepfake*, desencadeando uma tentativa de golpe de Estado por parte dos militares. Outro caso é contado por X Gonzáles, uma forte defensora de leis mais rígidas sobre armas nos EUA. Gonzáles é uma sobrevivente do massacre na escola de Parkland e ganhou reconhecimento internacional pelo seu discurso emocionado num serviço memorial após o evento. Os opositores de mais legislação sobre armas difamaram Gonzáles num vídeo que a mostrava a rasgar a Constituição americana. No vídeo original, ela rasga um alvo. Outro exemplo é um vídeo produzido sobre a democrata norte-americana Nancy Pelosi que demonstra a capacidade de troca de vozes. Os apoiantes de Trump, portanto concorrentes da Presidente

[3] Em janeiro de 2024, a empresa Arup foi vítima de uma fraude com recurso a tecnologia de IA, através da criação de um *deepfake* do diretor financeiro da empresa, que levou um dos trabalhadores do seu escritório em Hong Kong a transferir 25 milhões de dólares para diversas contas pertencentes a um grupo de criminosos cibernéticos (Silva, R., 2024).

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

da Câmara dos Representantes, editaram um vídeo para a fazer parecer bêbeda e algo confusa. O falso foi clicado milhões de vezes, apesar de Nancy Pelosi não beber álcool.

No entanto, apesar das suas aplicações negativas, os *deepfakes* também têm diversas aplicações positivas amplamente reconhecidas em diferentes áreas da vida social.

2.3 O uso positivo de Deepfakes

Embora os *deepfakes* sejam frequentemente associados a preocupações de segurança e privacidade, eles também oferecem várias aplicações positivas em diversas áreas. Por exemplo, podem ser usados para criar materiais educativos mais envolventes e interativos. Uma aplicação construtiva é a utilização de vídeos educativos que apresentam figuras históricas ou cientistas renomados que "falam" diretamente aos alunos. Essa abordagem torna a aprendizagem mais dinâmica e atraente, ajudando a captar a atenção dos estudantes e a melhorar a retenção do conhecimento (Roe; Perkins, 2024).

No setor de entretenimento, os *deepfakes* têm sido utilizados para revitalizar produções cinematográficas e televisivas. A tecnologia permite recriar atores falecidos para papéis póstumos ou rejuvenescê-los digitalmente para cenas que exigem uma aparência mais jovem. Um exemplo notável é o uso de *deepfakes* no filme "Rogue One: A Star Wars Story", onde o rosto do ator Peter Cushing foi recriado digitalmente para o papel do Grand Moff Tarkin (Dimitropoulos, 2020).

Os *deepfakes* podem ajudar na preservação e reconstrução de patrimónios culturais. Por exemplo, recriar digitalmente líderes culturais ou figuras históricas pode permitir que futuras gerações interajam de maneira mais tangível com a história. Isso é particularmente útil em museus e exposições culturais, onde as representações realistas podem enriquecer a experiência dos visitantes (George; George, 2023).

Na medicina, os *deepfakes* podem ser usados para simular cenários clínicos complexos para a formação de médicos e enfermeiros. Essa tecnologia pode criar vídeos que demonstram procedimentos médicos detalhados ou simulam interações com pacientes, proporcionando um ambiente de aprendizagem seguro e controlado (Qureshi; Khan, 2024).

Também as empresas de marketing e publicidade podem usar *deepfakes* para criar campanhas publicitárias inovadoras e personalizadas. A tecnologia pode gerar anúncios em

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

que celebridades ou figuras públicas endossam produtos de maneira mais autêntica e personalizada, aumentando o *engagement* do público (Fialho, 2023; Gouveia, 2023).

Portanto, enquanto os *deepfakes* são frequentemente associados a preocupações negativas, as suas aplicações construtivas demonstram um potencial significativo para trazer benefícios reais em várias esferas da sociedade. Reconhecer e explorar essas utilizações positivas é fundamental para maximizar os avanços que a tecnologia pode oferecer, ao mesmo tempo que se mitigam os seus riscos.

2.4 A expansão da penetração da Internet e a promoção da Literacia Digital em Angola

Angola, localizada na costa ocidental da África, tem uma população de cerca de 32 milhões de habitantes, com Luanda como a sua capital (INE, 2016). A economia é impulsionada por recursos naturais como petróleo e diamantes, mas enfrenta desafios significativos em desenvolvimento socioeconómico, incluindo altos índices de pobreza e desigualdade. A desigualdade é acentuada entre áreas urbanas e rurais, com acesso à tecnologia e internet sendo mais prevalente em áreas urbanas (*The World Bank Group*, 2022). Segundo dados recentes, apenas uma pequena fração da população tem acesso regular à internet, com disparidades acentuadas entre diferentes grupos socioeconómicos (Mbinza, 2024).

O governo angolano, através do Plano Nacional de Desenvolvimento 2023-2027, reconhece a importância da inclusão digital e tem tomado medidas para promover a literacia digital (Decreto Presidencial n.º 225/23). No entanto, a implementação enfrenta desafios devido a limitações orçamentárias e à necessidade de maior coordenação. A infraestrutura de TICs está em desenvolvimento, com esforços contínuos para expandir a conectividade e melhorar a infraestrutura tecnológica. Segundo o *The World Bank Group* (2019), o desenvolvimento da infraestrutura de TIC é fundamental para promover a inclusão digital e o crescimento económico em Angola. A expansão da conectividade e a redução dos custos de acesso à internet são essenciais para garantir que todos os cidadãos, incluindo aqueles com deficiência visual, possam beneficiar dos recursos digitais disponíveis.

O Executivo angolano estabeleceu como meta elevar a taxa de penetração da Internet em Angola para 80%, aumentando de 8,9 milhões para 18,8 milhões de utilizadores até 2027 (Silva, D., 2024).

Segundo o Livro Branco das Tecnologias de Informação e Comunicação 2019-2022[4], para garantir que todos se beneficiem do uso das Telecomunicações e TIC, o Estado deve promover a igualdade de oportunidades e assegurar uma abordagem segura e harmonizada na proteção de processos, dados e conexões digitais. O Executivo angolano planeia realizar ações de sensibilização e capacitação para educar os cidadãos, especialmente crianças e jovens, sobre o uso positivo e seguro das TIC e da Internet. Estas iniciativas vão abordar a cidadania digital e a literacia digital, bem como os riscos da navegação online, com o objetivo de promover a confiança e a segurança entre os utilizadores. A modernização do sistema de ensino e a promoção da info-inclusão desde a infância são considerados pilares centrais. Além disso, o Executivo pretende criar uma Estratégia Nacional para a Inclusão Digital, que visa proporcionar inclusão digital e desenvolver uma cultura digital focada em competências digitais. Embora o ambiente digital ofereça grandes oportunidades económicas e sociais, também apresenta riscos para a identidade, a privacidade e a intimidade (República de Angola, 2019).

Embora a infraestrutura de telecomunicações tenha melhorado, muitas áreas rurais ainda têm dificuldade de acesso à internet de alta qualidade. O custo elevado de dispositivos digitais é uma barreira significativa. Apenas cerca de 2% da população rural tem acesso à internet, comparado a 33% nas áreas urbanas (INE, 2023). A ausência de programas educacionais e de formação em competências digitais limita a capacidade das pessoas de utilizarem efetivamente a tecnologia (Nações Unidas; Programa das Nações Unidas para o Desenvolvimento, 2023). Há uma escassez de plataformas e materiais didáticos adaptados para deficientes visuais, dificultando o acesso à informação e à educação digital (Ferati et al., 2016; Hewitt; He, 2021). As desigualdades económicas limitam a capacidade das pessoas de investir em educação e tecnologia. A taxa de pobreza tem vindo a crescer todos os anos, passando de mais de 12 milhões de pessoas (41,7%) em 2019 para mais de 16 milhões

[4] Esta é a versão mais atualizada, sendo que à data da redação do artigo, estava aberto ao público contribuições para a nova edição do Livro Branco das TIC 2023-2027.

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

(49,4%), em 2022 e estima-se que esse número continue a aumentar, restringindo o acesso a tecnologias digitais (Mukuta, 2024).

Embora existam esforços governamentais para promover a inclusão digital, muitas políticas ainda são insuficientes ou mal implementadas.

3 PROCESSOS METODOLÓGICOS

Foi realizado um estudo de caso específico em Angola para observar como os *deepfakes* estão a ser usadas e quais são os impactos locais. Este estudo inclui a análise de incidentes de *deepfakes* reportados na mídia angolana, bem como a avaliação das respostas institucionais a tais incidentes.

3.1 Estudo de caso

Nesta investigação, o instrumento utilizado incide no método do Estudo de Caso, com análise de conteúdo. O Estudo de Caso é uma metodologia de investigação científica de cariz qualitativo. A crescente importância das metodologias qualitativas na investigação científica deve-se, por um lado, a uma certa desvalorização da investigação, desenvolvida à luz do paradigma positivista, e, por outro, à necessidade de desenvolver novas abordagens metodológicas que permitam dar resposta a problemáticas emergentes (Campenhoudt et al., 2019).

Também Yin (2009) afirma que o Estudo de Caso é um método que investiga em profundidade um fenómeno atual, no seu contexto da vida real, no presente, especialmente quando os limites entre o fenómeno e o contexto não são claramente evidentes.

De acordo com Cohen et al. (2005), o estudo de caso é caracterizado pela análise aprofundada de dados provenientes de várias fontes, podendo envolver observação tanto participante quanto não participante. Este método é não intervencionista e empático, oferecendo uma visão holística do fenómeno estudado e permitindo uma compreensão detalhada de casos específicos. Os objetivos principais incluem a contextualização, análise e interpretação de casos individuais ou situações específicas, entender a complexidade dos comportamentos dentro de um contexto particular, contribuir para ações e intervenções, e proporcionar uma visão imersiva da realidade estudada. Em síntese, o Estudo de Caso é uma

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

investigação empírica (Yin, 2009) que se baseia no raciocínio indutivo que depende fortemente do trabalho de campo e que se baseia em fontes de dados múltiplas e variadas.

Iacobucci e Churchill (2018) concluem que, na verdade, os objetivos que orientam um Estudo de Caso podem ser em tudo coincidentes com os da investigação educativa em geral: explorar, descrever, explicar, avaliar e/ou transformar.

2.2 Recolha e análise de dados

A pesquisa documental é uma técnica crucial para a análise das tecnologias de *deepfake*, focalizando a revisão da literatura existente sobre as suas aplicações, riscos e regulamentações em diversos contextos. Este processo envolve a análise detalhada de artigos académicos, relatórios técnicos e notícias relevantes sobre o tema.

O levantamento desses documentos permite uma compreensão aprofundada das bases teóricas e práticas associadas aos *deepfakes.* A revisão documental ajuda a identificar as melhores práticas para a mitigação dos efeitos negativos associados a essa tecnologia, destacando tanto as abordagens para prevenir abusos quanto as estratégias de regulamentação eficazes.

A análise inclui o exame das implicações dos *deepfakes* na sociedade, como a sua influência na disseminação de desinformação e a forma como as legislações estão a evoluir para enfrentar esses desafios. A revisão ajuda a compor um panorama abrangente sobre como os *deepfakes* são utilizados e regulamentados, contribuindo para a formulação de recomendações para lidar com os problemas emergentes associados a essa tecnologia (Westerlund, 2019).

4 RESULTADOS E DISCUSSÃO

4.1 Deepfakes: uma realidade emergente em Angola

Apesar das suas aplicações positivas, os *deepfakes* são amplamente reconhecidos pelos riscos significativos que apresentam à sociedade. Estes riscos incluem a disseminação de desinformação, manipulação política, violação de privacidade e segurança pessoal, além de fraudes e extorsão (Chawki, 2024; Chesney; Citron, 2019; Kharvi, 2024).

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

Uma das principais preocupações com os *deepfakes* em Angola é o seu potencial para espalhar desinformação. Podem ser usados vídeos manipulados para criar notícias falsas, desacreditando figuras públicas e políticos. Estes vídeos podem ser extremamente convincentes e têm o potencial de influenciar a opinião pública e até resultados eleitorais. Os *deepfakes* também representam uma ameaça significativa à privacidade individual. A facilidade de acesso a software de código aberto para criar *deepfakes* significa que qualquer pessoa pode criar vídeos manipulados de outros, muitas vezes com fins maliciosos.

Em 2017, circulou nas redes sociais um vídeo[5] manipulado que mostrava o ex-presidente angolano, José Eduardo dos Santos, em situações comprometedoras que nunca ocorreram. Este incidente foi amplamente discutido e é considerado o primeiro caso de deepfake conhecido no país. Este caso destaca a presença e os riscos associados aos *deepfakes* em Angola, especialmente no que diz respeito à desinformação e manipulação de figuras públicas.

Outro exemplo, surge num relatório denominado "Freedom on the Net 2023: The Repression Power of Artificial Intelligence", indicando que a empresa Mind Force, sediada em Israel, operava uma rede de contas em Angola e que publicava conteúdo em apoio ao partido no poder, o Movimento Popular de Libertação de Angola (MPLA), e contra o principal partido da oposição do país, União Nacional para a Independência Total de Angola (UNITA), tornado Angola entre os países com mais discursos pró-governo manipulados 'online' (Sebastião, 2023).

Recentemente, imagens do Presidente da República de Angola, João Lourenço, e da sua esposa, Ana Dias Lourenço, foram manipuladas em vídeos e disseminadas nas redes sociais, como WhatsApp, Facebook e TikTok. Esses vídeos falsificados mostravam o presidente e a sua esposa a fazerem declarações e ações que nunca ocorreram (figura 1).

[5] Vídeo disponível em: https://www.facebook.com/tvgcangolabrasil/posts/1418046151693113/?utm_source=chatgpt.com

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

Figura 1 – Imagens dos vídeos sobre o casal presidencial publicados nas redes socias WhatsApp e Tiktok

Nos últimos anos, a TV Zimbo, um dos principais canais de televisão em Angola, foi alvo de incidentes envolvendo *deepfakes*. Foram extraídos vídeos das suas transmissões, tendo sido manipulados e posteriormente publicados nas redes sociais, incluindo Facebook, WhatsApp e TikTok. Essas edições incluíam a alteração de rostos e vozes para fazer com que figuras públicas e apresentadores de notícias dissessem coisas que nunca disseram. Esses vídeos manipulados não só prejudicaram a reputação da TV Zimbo, como também tiveram sérias implicações para a desinformação e a confiança pública. A rápida disseminação nessas redes aumentou o alcance e o impacto dos vídeos falsos. Muitos utilizadores de redes sociais acreditaram que os vídeos eram genuínos, o que levou à disseminação de desinformação. Em alguns casos, isso resultou em reações negativas e debates acalorados sobre temas sensíveis, exacerbando tensões sociais e políticas (Figura 2).

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

Figura 2 - Vídeos extraídos do jornal da Tv Zimbo manipulados através da tecnologia *deep fake*

Noutra publicação partilhada no TikTok é visível um vídeo com uma montagem envolvendo personalidades de destaque da história e política de Angola: o primeiro presidente, Agostinho Neto; o ex-presidente José Eduardo dos Santos; o atual presidente João Lourenço; e Adalberto da Costa Júnior, líder da oposição (figura 3).

Figura 3 – Adalberto da Costa Júnior em (falsa) interação com o Presidente falecido José Eduardo dos Santos, João Lourenço e Agostinho Neto

A figura 3 foi retirada de um vídeo manipulado digitalmente, utilizando tecnologia de *deepfake,* onde Adalberto da Costa Júnior, atual líder da oposição em Angola, é mostrado a

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

interagir com o ex-presidente José Eduardo dos Santos, já falecido. Esta montagem falsa cria a ilusão de um diálogo ou interação inexistente entre ambos, manipulando a narrativa histórica e política. A utilização de *deepfakes* para criar um conteúdo que insinua interações entre figuras históricas e contemporâneas levanta preocupações significativas no contexto angolano.

A escolha destas figuras não é arbitrária. José Eduardo dos Santos representa um período significativo da história angolana, com forte simbolismo político e social. Por outro lado, Adalberto da Costa Júnior, enquanto figura proeminente da oposição, simboliza a crítica ao governo atual e a defesa de reformas no sistema político. A manipulação desta interação pode ser interpretada como uma tentativa de reforçar ou questionar narrativas políticas vigentes, explorando o impacto emocional e simbólico das personalidades envolvidas.

Outro vídeo refere-se à visita do presidente norte-americano Joe Biden, a 2 de dezembro a Angola (figura 4).

Figura 4 – Joe Biden a dançar na visita a Angola

O vídeo mostra o Presidente dos Estados Unidos, Joe Biden, na visita de dia 2 de dezembro de 2024 a Angola, envolvido numa dança tradicional. Esta representação, apesar de ser fictícia, foi amplamente partilhada em redes sociais como *WhatsApp* e *TikTok*, criando

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

confusão e até entusiasmo entre alguns utilizadores que acreditaram na veracidade do conteúdo.

4.2 Impacto das Deepfakes

As *deepfakes*, enquanto tecnologia emergente, têm vindo a demonstrar um impacto significativo em várias esferas da sociedade angolana, revelando vulnerabilidades institucionais, económicas, culturais e de segurança. Embora ainda relativamente incipiente em termos de disseminação generalizada no país, os exemplos reportados sublinham os desafios que Angola enfrenta para lidar com as implicações desta tecnologia.

Jacinto Marques, Arquiteto de Cibersegurança e Deteção de Ameaças, destaca a crescente preocupação com o impacto potencial dos *deepfakes* na estabilidade democrática em Angola. Ele explora como esta tecnologia, que permite a criação de conteúdos de áudio e vídeo extremamente realistas e falsificados, pode afetar negativamente a integridade do discurso público e os processos políticos num país que está a passar por transformações significativas rumo a uma democracia mais inclusiva e transparente. Salienta que a ameaça é amplificada pelo potencial dos *deepfakes* para incitar agitação social e política, exacerbar divisões e fomentar desconfiança. Defende, ainda, a necessidade urgente de sensibilização e contramedidas para mitigar esses riscos. Sugere que é essencial educar o público sobre a existência e os efeitos dos *deepfakes,* além de desenvolver tecnologias robustas para detectar e combater conteúdos manipulados. Também é crucial estabelecer medidas legislativas e regulamentares que responsabilizem os criadores e disseminadores de *deepfakes,* ao mesmo tempo que se preserva a liberdade de expressão. A promoção da literacia midiática e do pensamento crítico também é importante para capacitar os cidadãos a avaliar criticamente a informação digital. O autor é claro: para proteger a democracia angolana, é necessário adotar uma abordagem multifacetada que combine inovação tecnológica com medidas educacionais e legislativas. Sem tais intervenções, os *deepfakes* poderão ter consequências graves para o discurso público, a estabilidade política e a coesão social em Angola (Marques, 2024).

Um dos principais impactos das *deepfakes* em Angola está relacionado com a confiança nas instituições. O uso de vídeos manipulados para criar desinformação sobre

figuras políticas tem gerado instabilidade e desconfiança na opinião pública. A capacidade de criar e disseminar mensagens falsas com aparência autêntica não apenas fragiliza a confiança institucional, como também mina a coesão social.

O setor empresarial angolano também não está imune aos riscos impostos pelas *deepfakes*. Embora não se registem publicamente casos de grande escala no país, as fraudes empresariais com *deepfakes* representam uma ameaça crescente, como o exemplo citado anteriormente de Silva, R. (2024). A ausência de mecanismos eficazes de deteção de *deepfakes* pode expor empresas a riscos financeiros significativos e comprometer a sua reputação.

A segurança pessoal também surge como uma área particularmente vulnerável. *Deepfakes* podem ser utilizadas para difamar indivíduos ou fabricar conteúdos comprometedores, colocando em risco a integridade, privacidade e até a segurança física das vítimas. Este uso malicioso é especialmente preocupante em plataformas digitais amplamente utilizadas, como redes sociais, que facilitam a rápida disseminação de informações manipuladas.

Culturalmente, Angola enfrenta desafios adicionais relacionados com a manipulação do património imaterial. A criação de *deepfakes* que adulterem representações culturais autênticas pode comprometer a integridade de tradições e práticas locais, desinformando as gerações futuras e enfraquecendo a identidade nacional. Este impacto, embora indireto, pode ter implicações profundas para o reconhecimento e preservação do património cultural angolano.

Adicionalmente, a disseminação de *deepfakes* tem o potencial de intensificar tensões sociais. A criação de conteúdos manipulados com fins divisivos pode agravar conflitos preexistentes, amplificando discursos de ódio ou fomentando desconfiança entre diferentes comunidades e grupos sociais. Este risco é particularmente relevante num contexto onde desigualdades socioeconómicas e dinâmicas étnicas já representam desafios significativos.

Face a este cenário, é fundamental que Angola adote uma abordagem proativa para compreender e mitigar os impactos das *deepfakes*.

4.3 Desafios e Prevenção

A tecnologia deepfake coloca desafios significativos a nível global, mas em Angola os impactos são amplificados devido às limitações tecnológicas, lacunas legislativas e baixa literacia digital. Este capítulo analisa os principais obstáculos enfrentados pelo país na identificação e combate aos *deepfakes*, bem como propõe estratégias preventivas adaptadas ao contexto local.

Um dos principais desafios enfrentados por Angola é a limitação tecnológica. A detecção de *deepfakes* requer ferramentas avançadas baseadas em inteligência artificial e sistemas de análise digital, que frequentemente estão fora do alcance das instituições nacionais devido a restrições financeiras e falta de pessoal técnico qualificado (Mbinza, 2024). Além disso, a desigualdade no acesso à internet entre áreas urbanas e rurais agrava a incapacidade de responder de forma eficaz às ameaças digitais, deixando grande parte da população vulnerável (*The World Bank Group*, 2022).

No campo jurídico, Angola enfrenta lacunas legislativas. A ausência de uma regulamentação específica para abordar o uso malicioso de *deepfakes* dificulta a responsabilização de indivíduos ou organizações que disseminam conteúdos falsificados. Embora existam esforços para regulamentar os media digitais (Lusa, 2024), as disposições atuais não acompanham a velocidade da evolução tecnológica, expondo o país a riscos significativos de desinformação e manipulação política.

Outro obstáculo crítico é a baixa literacia digital. Uma grande parcela da população, particularmente nas zonas rurais, tem acesso limitado à educação tecnológica e pouca consciência dos perigos associados às tecnologias de manipulação de mídia. A falta de conhecimento sobre como verificar a autenticidade de conteúdos digitais contribui para a disseminação rápida de desinformação, dificultando ainda mais a capacidade de mitigar os danos associados aos *deepfakes* (Nações Unidas; Programa das Nações Unidas para o Desenvolvimento, 2023).

Por fim, a falta de cooperação internacional limita o acesso de Angola a recursos técnicos e know-how necessários para combater os *deepfakes* de forma eficaz. A natureza transnacional desta tecnologia exige colaborações entre países e organizações internacionais, que ainda são insuficientes no contexto angolano.

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

Para mitigar os impactos dos *deepfakes*, Angola necessita de adotar uma abordagem abrangente que combine esforços legislativos, tecnológicos, educacionais e institucionais.

A implementação de uma legislação robusta que regule a criação e disseminação de *deepfakes* é essencial. Este quadro legal deve incluir sanções para o uso malicioso de conteúdos manipulados e regulamentar o uso ético da tecnologia em contextos comerciais e educacionais. Além disso, a proteção da privacidade e da reputação de figuras públicas e cidadãos deve ser uma prioridade.

Angola deve investir em ferramentas avançadas de inteligência artificial para a detecção de *deepfakes*. Tecnologias baseadas em algoritmos de análise facial e sincronização labial são cruciais para identificar manipulações.

A educação digital deve ser integrada no currículo escolar e complementada por campanhas de sensibilização em comunidades. Estas iniciativas devem capacitar os cidadãos a identificar conteúdos manipulados e a avaliar criticamente as informações consumidas online (Marques, 2024). O desenvolvimento de competências digitais desde a infância é essencial para criar uma sociedade mais resiliente às ameaças tecnológicas.

Angola deve reforçar parcerias com organizações internacionais e países tecnologicamente avançados para aceder a recursos técnicos e formação especializada. A colaboração com iniciativas globais de cibersegurança, como a Interpol e a União Africana, pode facilitar o intercâmbio de conhecimentos e a implementação de soluções eficazes.

As instituições de comunicação social desempenham um papel crucial na detecção e combate à desinformação. Equipas de fact-checking bem treinadas e o uso de ferramentas digitais de verificação podem aumentar a confiança pública nos media nacionais. A criação de programas de formação para jornalistas em análise de conteúdo digital é uma medida importante para fortalecer o papel dos meios de comunicação.

A implementação de uma estratégia coordenada que envolva o governo, o setor privado e a sociedade civil é essencial. Esta estratégia deve focar-se no desenvolvimento de infraestruturas tecnológicas, no fortalecimento das capacidades institucionais e na educação do público sobre os riscos associados aos *deepfakes*.

5 CONSIDERAÇÕES FINAIS

O estudo sobre os *deepfakes* em Angola revelou uma série de dados cruciais, alinhados com os objetivos propostos para a pesquisa.

Primeiramente, discutiu-se o impacto dos *deepfakes* na política, mídia, segurança pessoal e privacidade dos cidadãos angolanos. A tecnologia *deepfake* representa uma ameaça significativa à integridade do discurso público e à confiança nas instituições democráticas. Os *deepfakes* podem ser usados para manipular a percepção pública de figuras políticas e eventos, criar desinformação e abalar a confiança em processos políticos e instituições. Além disso, essas tecnologias podem comprometer a privacidade individual e aumentar o risco de segurança pessoal ao criar conteúdos falsificados que podem ser utilizados para enganar e explorar pessoas.

Em segundo lugar, foram identificados os principais obstáculos enfrentados por Angola na identificação e combate aos *deepfakes*. Estes desafios incluem limitações tecnológicas, como a falta de ferramentas avançadas para detectar *deepfakes*, e deficiências legais, uma vez que a legislação atual não está totalmente equipada para lidar com as complexidades dos *deepfakes.* A falta de conscientização pública e a escassez de formação específica também são barreiras significativas. Sem uma abordagem coordenada que inclua melhorias tecnológicas e educacionais, Angola enfrenta dificuldades em combater eficazmente os *deepfakes* e proteger a integridade da informação.

Por fim, a sensibilização do público e dos profissionais sobre a existência e os perigos dos *deepfakes* é fundamental. Recomenda-se a implementação de campanhas de sensibilização para educar cidadãos e profissionais sobre os riscos associados aos *deepfakes* e a necessidade de uma abordagem crítica em relação ao consumo de mídia. Incentivar a educação em literacia digital e segurança cibernética desde a escola, juntamente com a formação contínua para profissionais de mídia e segurança, ajudará a preparar a sociedade para enfrentar esses desafios.

Em suma, para mitigar os riscos dos *deepfakes* em Angola, é essencial adotar uma abordagem multifacetada que inclua a criação de um regime jurídico robusto, o desenvolvimento de tecnologias de detecção avançadas, e a promoção da conscientização e

Reverte Revista de Estudos e Reflexões Tecnológicas da Fatec Indaiatuba

educação. Assim, Angola pode proteger a integridade da comunicação social e garantir um ambiente digital mais seguro e informado.

REFERÊNCIAS

CAMPENHOUDT, Luc; QUIVY, Raymond; MARQUET, Jacques. **Manual de Investigação em Ciências Sociais**. Lisboa: Gradiva, 2019.

CHAWKI, Mohamed. Navigating legal challenges of *deepfakes* in the American context: a call to action. **Cogent Engineering**, vol. 11, no. 1., 2024. https://doi.org/10.1080/23311916.2024.2320971

COHEN, Louis; MANION, L.awrence; MORRISON, Keith. **Research methods in education** (5th Ed). Routledge Falmer, 2005.

CYBER SEGURANÇA ANGOLA. **1º Caso de DeepFake em Angola, com um video de José Eduardo dos Santos.** 2019. Dsponível em: https://www.facebook.com/tvgcangolabrasil/posts/1418046151693113/?utm_source=chatgpt.com Acesso: 12 de jan. 2025.

DECRETO PRESIDENCIAL N.º 225/23 DO PRESIDENTE DA REPÚBLICA. Diário da República, n.º 227, I Série, de 30 de novembro de 2023. Disponível em: https://www.mpla.ao/wp-content/uploads/2023/12/PLANO-DE-DESENVOLVIMENTO-NACIONA-2023-2027.pdf Acesso: 12 de jan. 2025

DIMITROPOULOS, Stav. **A new film with a dead star? Thanks to CGI and deepfake technology, it's possible,** 2020. Disponível em: https://expmag.com/2020/10/a-new-film-with-a-dead-star-thanks-to-cgi-and-deepfake-technology-its-possible/ Acesso: 13 de jan. 2025

FERATI, Mexhid *et al.* Web Accessibility for Visually Impaired People: Requirements and Design Issues. *In*: FERATI, Mexhid *et al.* **Usability- and Accessibility-Focused Requirements Engineering**. Cham: Springer International Publishing, 2016. p. 79-96. ISBN 9783319459158. Disponível em: https://doi.org/10.1007/978-3-319-45916-5_6. Acesso: 12 de jan. 2025

FIALHO, Simone. **O bom uso de Deepfake amplia horizontes para o marketing**. 2023. Disponivel em: https://www.linkedin.com/pulse/o-bom-uso-de-deepfake-amplia-horizontes-para-marketing-simone-fialho/ Acesso: 13 de jan. 2025

GEORGE, Shaji; GEORGE, Hovan. *Deepfakes*: The Evolution of Hyper realistic Media Manipulation. **Partners Universal Innovative Research Publication (PUIRP***),* vol. 1, no. 2, 2023, 58-74. https://doi.org/10.5281/zenodo.10148558

GOODFELLOW, Ian *et al.* Generative adversarial networks. **Communications of the ACM**, vol. 63, no. 11, p. 139-144, 22 Out. 2020. Available from: https://doi.org/10.1145/3422622. Acesso: 13 de jan. 2025.

GOSSE, Chandell; BURKELL, Jacquelyn. Politics and porn: how news media characterizes problems presented by deepfakes. **Critical Studies in Media Communication**, vol. 37, no. 5, p. 497-511, 19 Oct. 2020. Disponível em: https://doi.org/10.1080/15295036.2020.1832697. Acesso: 13 de jan. 2025.

Gouveia, Marco. **A Ascendência do DeepFake Advertising: Uma Reflexão**. Marketeer. 2023. Disponível em: https://marketeer.sapo.pt/a-ascendencia-do-deepfake-advertising-uma-reflexao/ Acesso: 13 de jan. 2025.

GUPTA, Gourav *et al.* A Comprehensive Review of DeepFake Detection Using Advanced Machine Learning and Fusion Methods. **Electronics**, vol. 13, no. 1, p. 95, 25 Dez. 2023. Disponível em: https://doi.org/10.3390/electronics13010095. Acesso: 13 de jan. 2025.

HEWITT, Dylan H.; HE, Yingchen. Internet Accessibility for Blind and Visually-Impaired Users: An Evaluation of Official U.S. State and Territory COVID-19 Websites. **Proceedings of the Human Factors and Ergonomics Society Annual Meeting**, vol. 65, no. 1, p. 154-158, Sept. 2021. Disponível em: https://doi.org/10.1177/1071181321651051. Acesso: 13 de jan. 2025.

IACOBUCCI, Dawn; CHURCHILL, Gilbert. **Marketing Research: Methodological Foundations** (12.ª ed.). Nashville, TN: Earlie Lite Books, Inc. 2018.

INSTITUTO NACIONAL DE ESTATÍSTICA DE ANGOLA. **Projecção da população 2014-2050**. 2016. Disponível em: https://www.ine.gov.ao/Arquivos/arquivosCarregados//Carregados/Publicacao_637586861813829303.pdf Acesso: 13 de jan. 2025.

INSTITUTO NACIONAL DE ESTATÍSTICA DE ANGOLA. **Relatório sobre Cibersegurança e Serviços Digitais- Inquérito ao Emprego em Angola (IEA) I Trimestre 2021.** 2023. Disponível em: https://www.ine.gov.ao/Arquivos/arquivosCarregados/Carregados/Publicacao_638143506802949387.pdf Acesso: 13 de jan. 2025.

JUAN, Patricia. **The relationship between Artificial Intelligence and Crime: Deepfake as a threat for a technologic world**. 23rd Annual Conference of European Society of Criminology. Florencia. 2023.

KAUR, Achhardeep *et al.* Deepfake video detection: challenges and opportunities. **Artificial Intelligence Review**, vol. 57, no. 6, 29 May 2024b. Disponível em: https://doi.org/10.1007/s10462-024-10810-6. Acesso: 14 Jan. 2025.

KHARVI, Prakash L. Understanding the Impact of AI-Generated Deepfakes on Public Opinion, Political Discourse, and Personal Security in Social Media. **IEEE Security & Privacy**, p. 2-9, 2024. Disponível em: https://doi.org/10.1109/msec.2024.3405963. Acesso: 14 Jan. 2025.

KIETZMANN, Jan *et al.* Deepfakes: Trick or treat? **Business Horizons**, vol. 63, no. 2, p. 135-146, Mar. 2020. Disponível em: https://doi.org/10.1016/j.bushor.2019.11.006. Accesso: 14 Jan. 2025.

ŁABUZ, Mateusz; NEHRING, Christopher. On the way to deep fake democracy? Deep fakes in election campaigns in 2023. **European Political Science**, 26 Apr. 2024. Disponível em: https://doi.org/10.1057/s41304-024-00482-9. Acesso: 14 Jan. 2025.

LUSA. **Angola: Governo prepara regulamento contra "desinformação".** 2024. Disponível em: https://www.dw.com/pt-002/preocupado-com-o-fen%C3%B3meno-da-desinforma%C3%A7%C3%A3o-governo-angolano-prepara-regulamento/a-68041568 Acesso: 14 Jan. 2025.

MADDOCKS, Sophie. 'A Deepfake Porn Plot Intended to Silence Me': exploring continuities between pornographic and 'political' deep fakes. **Porn Studies**, vol. 7, no. 4, p. 415-423, 4 June 2020. Disponível em: https://doi.org/10.1080/23268743.2020.1757499. Acesso: 14 Jan. 2025.

MARQUES, Jacinto. **A ameaça dos deepfakes à democracia angolana - Jacinto Marques**. 2024. Disponível em https://www.club-k.net/index.php?option=com_content&view=article&id=53116:a-ameaca-dos-*deepfakes*-a-democracia-angolana-jacinto-marques&catid=17&Itemid=1067&lang=pt Acesso: 14 Jan. 2025.

MBINZA, Pedro. **Acesso à internet em Angola atinge mais de 11 milhões de subscritores entre 2021 e 2023.** 2024. Disponível em: https://www.forbesafricalusofona.com/acesso-a-internet-em-angola-atinge-mais-de-11-milhoes-de-subscritores-entre-2021-e-2023/ Acesso: 14 Jan. 2025.

MOLINA, Adriano Cezar; BERENGUEL, Orlando Leonardo. Deepfake: A evolução das fake news. **Research, Society and Development**, vol. 11, no. 6, p. e56211629533, 10 Mai 2022. Disponível em: https://doi.org/10.33448/rsd-v11i6.29533. Acesso: 14 Jan. 2025.

MOLINA, Adriano Cezar; BERENGUEL, Orlando Leonardo. Deepfake: A evolução das fake news. **Research, Society and Development**, vol. 11, no. 6, p. e56211629533, 10 Mai 2022a. Disponível em: https://doi.org/10.33448/rsd-v11i6.29533. Acesso: 14 Jan. 2025.

MUKUTA, Coque. **Quase metade da população de Angola vive na pobreza**. 2024. Disponível em: https://www.voaportugues.com/a/quase-metade-da-popula%C3%A7%C3%A3o-de-angola-vive-na-pobreza/7495227.html Acesso: 14 Jan. 2025.

NAÇÕES UNIDAS & PROGRAMA DAS NAÇÕES UNIDAS PARA O DESENVOLVIMENTO (2023). **Angola Science, Technology & Innovation Policy Review**. Disponível em: https://unctad.org/system/files/official-document/dtlstict2022d7_en.pdf Acesso: 14 Jan. 2025.

NOONAN, Luke. **Deepfake: Delírio ou realidade? Como a IA abusa da nossa confiança.** 2024. Disponível em: https://www.metacompliance.com/pt/blog/security-awareness-training/deepfake Acesso: 14 Jan. 2025.

PARIS, Britt; DONOVAN, Joan. **Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidenc***e.* Data & Society. 2019. Disponível em: https://datasociety.net/wp-content/uploads/2019/09/DataSociety_*Deepfakes*_Cheap_Fakes.pdf Acesso: 14 Jan. 2025.

PAWELEC, Maria. Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions. **Digital Society**, vol. 1, no. 2, Ago. 2022. Disponível em: https://doi.org/10.1007/s44206-022-00010-6. Acesso: 14 Jan. 2025.

PFEFFERKORN, Riana. **The threat posed by deepfakes to marginalized communities**. 2021. Disponível em: https://www.brookings.edu/articles/the-threat-posed-by-*deepfakes*-to-marginalized-communities/ Acesso: 14 Jan. 2025.

QURESHI, Jamshir; KHAN, Samina. Artificial Intelligence (AI) *Deepfakes* in Healthcare Systems: A Double-Edged Sword? Balancing Opportunities and Navigating Risks. **Preprints,** 1-9. 2024. https://doi.org/10.20944/preprints202402.0176.v1

DE RANCOURT-RAYMOND, Audrey; SMAILI, Nadia. The unethical use of deepfakes. **Journal of Financial Crime**, vol. 30, no. 4, p. 1066-1077, 19 Mai 2022. Disponível em: https://doi.org/10.1108/jfc-04-2022-0090. Acesso: 14 Jan. 2025.

REPÚBLICA DE ANGOLA. **Livro Branco das Tecnologias de Informação e Comunicação 2018 – 2022.** 2019. Disponível em: https://cdn.sepe.gov.ao/sepe/documentos/LBTIC19-22.pdf. Acesso: 14 Jan. 2025.

ROE, Jasper; PERKINS, Mike. **Deepfakes and higher education: a research agenda and scoping review of synthetic media.** 2024. Disponível em: https://www.researchgate.net/publication/380034882_*Deepfakes*_and_Higher_Education_A_Research_Agenda_and_Scoping_Review_of_Synthetic_Media Acesso: 14 Jan. 2025.

SATARIANO, Adam; MOZUR, Paul. **The People Onscreen Are Fake. The Disinformation Is Real**. The New York Times. 2023. Disponível em: https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html Acesso: 14 Jan. 2025.

Sebastião, J. **Angola entre os países com mais discursos pró-governo manipulados 'online'.** 2023. Disponível em: https://www.menosfios.com/angola-entre-os-paises-com-mais-discursos-pro-governo-manipulados-online/ Acesso: 14 Jan. 2025.

SILVA, D.. *Angola prevê elevar a taxa de utilizadores*. **Jornal de Angola**. 2024. Disponível em: https://www.jornaldeangola.ao/ao/noticias/angola-preve-elevar-a-taxa-de-utilizadores/ Acesso: 14 Jan. 2025.

SILVA, R. *Como um "deepfake" custou 25 milhões de dólares à empresa por detrás da Ópera de Sydney*. **Jornal de Negócios**. 2024. Disponível em: https://www.jornaldenegocios.pt/empresas/detalhe/como-um-deepfake-custou-25-milhoes-de-dolares-a-empresa-por-detras-da-opera-de-sydney Acesso: 14 Jan. 2025.

THE WORLD BANK GROUP. **Broadband for All: A Digital Infrastructure Moonshot for Africa**. 2019. Disponível em: https://www.broadbandcommission.org/working-groups/digital-infrastructure-moonshot-for-africa/ Acesso: 14 Jan. 2025.

THE WORLD BANK GROUP. **Angola Country Climate and Development Report**. 2022. Disponível em: https://documents1.worldbank.org/curated/en/099150012022242096/pdf/P1769171f457c3010198d31b375aaddd937.pdf Acesso: 14 Jan. 2025.

WESTERLUND, M. (2019). The Emergence of Deepfake Technology: A Review. **Technology Innovation Management Review**, *vol. 9, no.* 11, pp. 39-52.

YIN, Robert. **Case Study Research: design and methods** (4 ed.). Thousand Oaks: Sage. 2009.