REVISTA MUNDO EM MOVIMENTO
Uninassau-Caruaru
1(1): 75-89, 2024
ISSN: 2966-2176

REGULAMENTAÇÃO DOS DEEP FAKES NO BRASIL: DESAFIOS JURÍDICOS E SOLUÇÕES TECNOLÓGICAS

REGULATION OF DEEP FAKES IN BRAZIL: LEGAL CHALLENGES AND TECHNOLOGICAL SOLUTIONS

Emanuelly Ignez Alves Silva
Graduanda em Bacharelado em Direito – UniNassau Caruaru. E-mail: manulvs44@gmail.com

Filipe Eduardo Macedo de Menezes
Professor universitário na UNINASSAU CARUARU. Mestre em Direito pela Universidade Católica de Pernambuco (UNICAP). Advogado com especialização em Direito Civil e Empresarial pela Universidade Federal de Pernambuco (UFPE). Alma Mater pela Universidade Federal da Paraíba (UFPB). E-mail: patriota.menezes@gmail.com

RESUMO: O avanço da inteligência artificial (IA) tem proporcionado inovações impressionantes, entre as quais se destacam os deep fakes, que consistem na criação de vídeos, áudios e imagens falsos com alta precisão e realismo. Essa tecnologia, desenvolvida com algoritmos de aprendizado profundo, permite a manipulação de rostos e vozes de forma tão convincente que pode enganar o público. Inicialmente utilizados em contextos de entretenimento, os deep fakes logo foram adotados para práticas criminosas, como fraudes, manipulação política e ataques à reputação de indivíduos. No Brasil, a crescente utilização dessa ferramenta evidenciou a necessidade de uma regulamentação específica, uma vez que as leis atuais não cobrem integralmente os desafios impostos por essa nova

forma de crime digital. O Projeto de Lei nº 1272/2023 surge como uma tentativa de criminalizar a adulteração de vídeos e áudios por meio de IA, prevendo penas proporcionais ao impacto causado. Além da questão jurídica, o estudo também aborda soluções tecnológicas, como o Liveness, uma ferramenta de autenticação biométrica que verifica a autenticidade de imagens e vídeos, prevenindo fraudes digitais. A integração dessa tecnologia em setores como o financeiro, onde grandes volumes de dados são processados, traz uma proteção adicional contra essas manipulações. Portanto, este artigo reflete sobre a urgência de criar leis específicas e adotar tecnologias inovadoras para mitigar os riscos impostos pelos deep fakes, protegendo a sociedade. A combinação de medidas preventivas, como soluções biométricas, com uma legislação eficaz é fundamental para garantir a segurança digital e punir adequadamente os criminosos, além de explorar os desafios que empresas e instituições enfrentam na implementação dessas soluções, bem como a necessidade de adaptação às novas ameaças digitais.

PALAVRAS-CHAVE: Deep Fakes, Inteligência Artificial, Cibercrimes, Legislação, Liveness.

ABSTRACT: The advancement of artificial intelligence (AI) has led to impressive innovations, among which deep fakes stand out—highly precise and realistic falsifications of videos, audio, and images. This technology, developed through deep learning algorithms, enables the manipulation of faces and voices so convincingly that it can deceive the public. Initially used in entertainment contexts, deep fakes were quickly adopted for criminal purposes, such as fraud, political manipulation, and attacks on individuals' reputations. In Brazil, the growing use of this tool has highlighted the need for specific regulation, as current laws do not fully address the challenges posed by this new form of digital crime. Bill No. 1272/2023 emerges as an attempt to criminalize the alteration of videos and audio through AI, establishing penalties proportional to the damage caused. Beyond the legal issue, the study also addresses technological solutions such as Liveness, a biometric authentication tool that verifies the authenticity of images and videos, preventing digital fraud. The integration of this technology into sectors such as finance, where large volumes of data are processed, provides additional protection against these manipulations. Therefore, this

article reflects on the urgency of creating specific laws and adopting innovative technologies to mitigate the risks posed by deep fakes, safeguarding society. The combination of preventive measures, such as biometric solutions, with effective legislation is essential to ensure digital security and adequately punish criminals. Furthermore, the study explores the challenges that companies and institutions face in implementing these solutions and the need to adapt to new digital threats.

KEYWORDS: Deep Fakes, Artificial Intelligence, Cybercrimes, Legislation, Liveness.

1. INTRODUÇÃO

A era contemporânea é marcada por avanços tecnológicos que transformam profundamente a forma como a sociedade interage e se organiza. Desde o século XX, a inteligência artificial (IA) tem evoluído significativamente, permitindo o desenvolvimento de sistemas capazes de simular comportamentos humanos e realizar tarefas cognitivas com base em dados extensos. Um dos exemplos mais notórios dessa evolução são os deepfakes, mídias manipuladas que alteram rostos, vozes e expressões, simulando situações nunca ocorridas. Embora tenham aplicações legítimas, como no cinema e na publicidade, seu uso inadequado para fraudes, difamações e desinformação apresenta riscos severos.

> As deep fakes corroerão a confiança em uma ampla gama de instituições públicas e privadas e essa descredibilidade afetará além dos órgãos, dos funcionários, tais como juízes, legisladores, dentre outros. (CHESNEY & CITRON, 2019)

As eleições de 2018 no Brasil demonstraram o impacto destrutivo dessa tecnologia, com sua utilização em campanhas de desinformação que confundiram o público e polarizaram debates políticos (Silva, 2019). Esses eventos evidenciam como os deepfakes podem comprometer a confiança pública e intensificar divisões sociais, sobretudo quando associados à manipulação de informações em larga escala.

Além dos danos sociais, a tecnologia facilita crimes como extorsão, fraude e roubo de identidade, tornando-se uma ameaça crescente. A complexidade desse cenário exige uma resposta jurídica robusta. No Brasil, instrumentos como o Código Penal (Decreto-Lei nº 2.848/1940) e o Marco Civil da Internet (Lei nº 12.965/2014) fornecem diretrizes iniciais para abordar crimes digitais, mas não contemplam integralmente os desafios impostos pelos deepfakes. Nesse contexto, o Projeto de Lei nº 1272/2023 busca preencher essa lacuna ao prever penalidades específicas para a produção e disseminação de conteúdos manipulados.

Outro aspecto crucial é a adoção de tecnologias preventivas. Ferramentas como o Liveness, que utiliza autenticação biométrica para detectar manipulações em imagens e vídeos, representam avanços importantes na mitigação de riscos associados à IA. Essas soluções tecnológicas complementam as regulamentações e fortalecem a proteção da sociedade digital.

Este artigo analisa a evolução da inteligência artificial e o papel dos algoritmos na criação de deepfakes, destacando seus impactos sociais e jurídicos no Brasil. Também discute a urgência de regulamentações específicas e o papel de soluções tecnológicas no enfrentamento dessas questões.

2. DEEP FAKES: UMA INOVAÇÃO TECNOLÓGICA COMPLEXA E SEUS IMPACTOS

Deepfake é uma tecnologia emergente que usa inteligência artificial (IA) e aprendizado profundo para criar conteúdos audiovisuais manipulados de maneira realista. O termo resulta da combinação de "deep learning" (aprendizado profundo) e "fake" (falso), destacando sua base tecnológica. Segundo Goodfellow, Bengio e Courville (2016), o deep learning é um avanço da IA, baseado no aprendizado de máquina, que permite aos computadores aprender de forma autônoma, analisando dados e identificando padrões sem programação específica.

O uso dos deepfakes ganhou notoriedade em 2017, quando um usuário do Reddit começou a compartilhar vídeos com rostos de celebridades inseridos em cenas de filmes e séries, evidenciando o poder dos algoritmos envolvidos. Esses algoritmos possibilitam a fusão de imagens e a manipulação de áudio, criando vídeos tão convincentes que podem enganar até observadores atentos.

O aprendizado de máquina, base da tecnologia, permite que sistemas computacionais analisem grandes volumes de dados e gerem previsões sem comandos programados para cada situação. Assim, os deepfakes ilustram a aplicação dessas tecnologias, trazendo tanto potenciais quanto desafios éticos e sociais.

A criação de deepfakes exige vastos conjuntos de dados sobre uma pessoa (como imagens ou vídeos), tornando a simulação mais convincente. Inicialmente explorados em contextos recreativos, os deepfakes se expandiram para áreas preocupantes, como a disseminação de

desinformação e manipulação de opiniões públicas, com vídeos falsificados distorcendo discursos de figuras públicas, gerando confusão e desconfiança nas redes sociais. Isso afeta a percepção pública e interfere em processos democráticos, destacando a urgência de regulamentação.

As implicações são profundas, levantando questões éticas sobre privacidade e consentimento. A criação de conteúdos falsos pode resultar em campanhas de desinformação, chantagem e assédio, afetando tanto indivíduos quanto figuras públicas. Além disso, a capacidade de criar conteúdos falsificados de alta qualidade desafia a legislação existente, deixando vítimas desprotegidas e dificultando a responsabilização dos criadores e disseminadores desses conteúdos.

Um exemplo claro dos riscos dos deepfakes é o caso do vídeo manipulado de Joe Biden, presidente dos Estados Unidos, supostamente fazendo declarações ofensivas a eleitores após sua desistência da corrida presidencial de 2024. Segundo Dauer (2024), o vídeo, manipulado com IA, mostrava Biden fazendo discursos de ódio, como "Meus caros americanos, eu quero aproveitar o momento pra falar sobre as merdas odiosas que vocês têm falado sobre mim", o que não era verdade. A manipulação foi identificada como deep fake, mostrando como essas tecnologias podem distorcer a verdade e manipular a percepção pública, ameaçando processos democráticos.

3. DEEP FAKES GROTESCOS: CARACTERÍSTICAS E DESAFIOS JURÍDICOS

Os deep fakes grotescos destacam-se por manipulações digitais deliberadamente exageradas, caracterizadas por distorções visuais evidentes, caricaturas e absurdos gráficos. Apesar de sua evidente falsidade, esses conteúdos têm sido usados para promover desinformação, incitar campanhas de ódio e comprometer reputações, demonstrando que seu impacto vai além do aspecto estético (Almenara, 2021). Os avanços tecnológicos na criação de deep fakes têm ampliado sua capacidade de enganar audiências e causar danos significativos, mesmo quando essas manipulações são visivelmente artificiais.

No contexto jurídico brasileiro, os deep fakes grotescos apresentam desafios complexos. O Código Penal Brasileiro (Brasil, 1940) prevê crimes como calúnia (art. 138), difamação (art. 139) e falsidade ideológica (art. 299), que podem ser aplicados a algumas dessas manipulações digitais. Por exemplo, a utilização de um deep fake grotesco para acusar falsamente alguém de um crime pode ser enquadrada como calúnia, enquanto o uso de distorções visuais ou sonoras para difamar uma pessoa pode configurar difamação.

A comparação com as falsificações grosseiras de cédulas de real ilustra bem o ponto: assim como as falsificações visivelmente falsas não são tratadas como crimes de moeda falsa, mas sim como estelionato (art. 171 do Código Penal), os deep fakes grotescos, ainda que visivelmente falsos para a maioria, podem ser usados para prejudicar indivíduos específicos, seja por meio de humilhação pública ou manipulação de decisões.

Essas distorções digitais, independentemente da clareza de sua falsidade, podem causar danos reais e irreparáveis às vítimas. O uso de

manipulações grotescas, como vídeos de figuras públicas sendo retratadas em contextos absurdos ou difamatórios, não apenas prejudica a reputação de pessoas envolvidas, mas também enfraquece a confiança pública e a integridade das informações circuladas nas plataformas digitais.

A comparação com crimes como o estelionato reforça que, mesmo quando a falsidade é óbvia para uma parte do público, os deep fakes grotescos podem ser explorados com a intenção de prejudicar vítimas específicas, ilustrando que o impacto das manipulações está relacionado não apenas com a sofisticação técnica, mas também com a intenção por trás do uso e os danos causados.

4. REGULAMENTAÇÃO DOS DEEP FAKES: CENÁRIO GLOBAL E NACIONAL

O fenômeno dos deep fakes tem gerado preocupações significativas globalmente, levando a nações como os Estados Unidos e a União Europeia a adotar regulamentações específicas para mitigar os impactos dessa tecnologia. Nos Estados Unidos, por exemplo, o Estado da Califórnia foi um dos pioneiros ao sancionar a Assembly Bill 730 em 2018, que proíbe o uso de deep fakes com intenção de enganar eleitores ou prejudicar candidatos durante períodos eleitorais. A lei exige que qualquer vídeo manipulando a imagem de um candidato político, com a intenção de enganar o eleitorado, seja claramente identificado como tal e cria penalidades para os responsáveis pela criação ou distribuição de tais vídeos (California Legislative Information, 2018). A implementação dessa legislação em nível estadual representa um avanço no combate à manipulação da informação

e à integridade do processo eleitoral, sendo uma das primeiras ações jurídicas focadas diretamente na regulamentação de deep fakes.

Na União Europeia, os debates sobre a regulamentação de deep fakes estão se intensificando, com a Comissão Europeia trabalhando em diretrizes e regulamentações que garantam que as tecnologias, como as de manipulação de vídeos e imagens, respeitem direitos fundamentais como a privacidade e a dignidade humana, ao mesmo tempo que buscam combater abusos dessa tecnologia. A proposta de Regulamento de Inteligência Artificial (AI Regulation) da Comissão Europeia, que está sendo discutida em 2021, inclui medidas específicas para a criação e uso de deep fakes. A intenção é assegurar que essas tecnologias não sejam usadas para causar danos significativos a indivíduos ou à sociedade, garantindo o equilíbrio entre inovação e proteção dos direitos dos cidadãos. Essa abordagem abrange desde o combate à desinformação até a criação de mecanismos de fiscalização mais rigorosos, a regulamentação busca integrar diretrizes éticas e técnicas, promovendo o uso responsável das inovações tecnológicas enquanto coíbe abusos (União Europeia, 2021).

No Brasil, embora existam marcos legais importantes, como o Marco Civil da Internet (Brasil, 2014) e a Lei Geral de Proteção de Dados Pessoais (Brasil, 2018), que oferecem uma base jurídica relevante para a proteção de dados e a responsabilização por crimes digitais, ainda não há uma legislação específica que trate dos deep fakes. A situação pode estar mudando com a proposta do Projeto de Lei nº 1272/2023, atualmente em discussão no Congresso Nacional. O projeto propõe penalidades para aqueles que produzirem ou disseminarem vídeos manipulados com o uso de inteligência artificial, com o intuito de prejudicar a imagem ou a

reputação de alguém (Brasil, 2023). Isso evidencia a crescente preocupação no país com o uso indevido dessa tecnologia em contextos sensíveis, como o político e o eleitoral, onde a manipulação de vídeos e imagens pode prejudicar diretamente a integridade da democracia e a confiança pública.

A experiência de outros países, como os Estados Unidos e a União Europeia, demonstram que a regulação dos deep fakes deve ser mais abrangente, tratando da prevenção, da responsabilização e da conscientização pública.

5. PROJETO DE LEI N° 146/2024 E A REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO BRASIL: A NECESSIDADE DE UM MARCO ESPECÍFICO

Projeto de Lei nº 146/2024, atualmente em tramitação no Senado Federal, propõe uma alteração no Código Penal Brasileiro (Decreto-Lei nº 2.848, de 1940) para estabelecer uma causa de aumento de pena em crimes contra a honra e uma hipótese qualificada para o crime de falsa identidade, quando houver o uso de tecnologia de inteligência artificial (IA) para alterar imagens ou sons humanos. Essa modificação surge como resposta à crescente utilização de deep fakes e outras manipulações audiovisuais geradas por IA, que têm o potencial de distorcer a realidade e causar danos significativos à imagem e reputação de indivíduos, especialmente em contextos de desinformação e fraudes.

Esse projeto de lei reflete a necessidade urgente de atualizar a legislação brasileira para lidar com os desafios impostos pelo avanço das

tecnologias de IA, especialmente considerando o impacto social dos deep fakes. Esses conteúdos, embora falsificados, são muitas vezes tão realistas que causam grande dano à integridade pública e à confiança da sociedade. O PL visa alinhar o Brasil às melhores práticas internacionais na regulação da IA, com ênfase no uso ético e responsável dessa tecnologia.

Se aprovado, o Projeto de Lei nº 146/2024 representaria um avanço significativo no enfrentamento dos abusos tecnológicos, ao complementar outras legislações, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (LGPD), que já estabelecem normas para a proteção digital e da privacidade, mas não oferecem uma resposta específica aos desafios trazidos pelos deep fakes (Brasil, 2014; Brasil, 2018). Enquanto a LGPD protege dados pessoais, ela não aborda diretamente as manipulações de conteúdo digital, como vídeos ou imagens adulteradas, criando uma lacuna importante na legislação.

A proposta do PL nº 146/2024 surge como uma resposta para preencher essas lacunas e garantir a responsabilização de quem faz uso indevido de IA para manipular a imagem de indivíduos, especialmente em áreas sensíveis como política e eleições. O PL propõe medidas mais precisas que permitirão ao Brasil avançar na regulamentação do uso de tecnologias de manipulação audiovisual, especialmente em um cenário onde as implicações dos deep fakes se estendem ao campo político e à reputação de cidadãos e figuras públicas. A aprovação desse projeto não só aperfeiçoaria as regulamentações existentes, mas também garantiria uma proteção mais robusta contra os abusos tecnológicos, alinhando o Brasil a um modelo internacional que equilibre inovação e ética.

6. SOLUÇÕES TECNOLÓGICAS E DESAFIOS NO COMBATE AOS DEEP FAKES: O PAPEL DO LIVENESS PASSIVO

Uma das soluções mais promissoras contra os deep fakes é o Liveness Passivo, que utiliza algoritmos avançados de machine learning para detectar fraudes em vídeos e imagens manipuladas. O Liveness Passivo funciona analisando sutilezas que são imperceptíveis ao olho humano, como inconsistências nos movimentos faciais, variações na iluminação e texturas anômalas. A tecnologia também pode detectar sinais de manipulação, como falhas nos reflexos dos olhos ou movimentos labiais inverossímeis, tornando-se essencial para a autenticação digital (Costa, 2020; Almenara, 2021).

O Liveness Passivo já é utilizado em setores como tecnologia e serviços bancários para prevenir fraudes financeiras e garantir a segurança de transações online. No entanto, sua aplicação pode ser expandida para redes sociais, onde a disseminação de deep fakes é alarmante. Essa tecnologia pode identificar conteúdos manipulados e criar um ambiente online mais seguro.

Apesar das vantagens, a implementação do Liveness Passivo enfrenta desafios. O custo da tecnologia é um obstáculo, pois requer investimentos substanciais em infraestrutura e treinamento, dificultando a adoção por pequenas empresas e startups, que ficam vulneráveis à manipulação (Rudnitzki, 2020). Além disso, as redes sociais resistem à adoção de soluções como essa, enfrentando o dilema entre liberdade de expressão e controle sobre conteúdos manipulados. O processamento de grandes

volumes de dados pessoais também gera preocupações sobre privacidade e consentimento.

Para que o Liveness Passivo desempenhe seu papel eficazmente, é necessário um esforço coordenado entre desenvolvimento tecnológico e regulamentação, ética e proteção de direitos. Políticas públicas que incentivem a adoção dessas tecnologias, assegurando acessibilidade para empresas de todos os portes, são essenciais. Também é importante estabelecer diretrizes claras para proteger a privacidade dos usuários (Almenara, 2021).

A eficácia do Liveness Passivo depende de um ecossistema regulatório que favoreça sua adoção. A colaboração entre o setor público e privado e a conscientização sobre a proteção contra manipulação digital são cruciais para criar um ambiente digital mais seguro e resiliente aos desafios dos deep fakes.

CONSIDERAÇÕES FINAIS

A regulamentação dos deep fakes no Brasil é um desafio que exige uma abordagem multidisciplinar, combinando avanços tecnológicos e soluções jurídicas. A criação de normas específicas, como o Projeto de Lei nº 1272/2023, representa um passo importante na responsabilização de quem manipula conteúdos digitais de forma prejudicial. No entanto, para que essas regulamentações sejam eficazes, é fundamental que estejam alinhadas a soluções tecnológicas, como o Liveness Passivo, que podem atuar de forma preventiva na detecção de fraudes.

A experiência internacional demonstra que uma legislação robusta, integrada a ferramentas de autenticação e verificação, é crucial para enfrentar a sofisticação dos deep fakes. A implementação dessas tecnologias deve ser facilitada por políticas públicas que incentivem sua adoção e garantam o acesso igualitário a todos os setores, inclusive os mais vulneráveis economicamente. Além disso, é imperativo equilibrar a proteção contra manipulações digitais com a preservação de direitos fundamentais, como a privacidade e a liberdade de expressão, criando um ambiente seguro para a inovação tecnológica e a interação social no meio digital.

Nesse sentido, o Brasil tem a oportunidade de se alinhar às melhores práticas globais, aprimorando a legislação existente e desenvolvendo um marco regulatório específico que proteja os cidadãos e a integridade das informações em um cenário digital cada vez mais vulnerável. O caminho para mitigar os danos causados pelos deep fakes passa, portanto, pela

REFERÊNCIAS

ALMENARA, I. (2021). **Algoritmo é capaz de desmascarar deepfakes analisando o movimento dos olhos.** Canaltech. https://canaltech.com.br/inteligencia-artificial/algoritmo-e-capaz-de-desmascarar-deepfakes-analisando-o-movimento-dos-olhos-180574/. Acesso em: 19 set. 2024.

ATHENIENSE, A. (2019). **O que é Deepfake? Saiba como funciona e porque tecnologia pode afetar a política.** Alexandre Atheniense Advogados. https://www.alexandreatheniense.com.br/o-que-e-deepfake-

saiba-como-funciona-e-porque-tecnologia-pode-afetar-a-politica/. Acesso em: 19 set. 2024.

BRASIL. (2014). **Lei nº 12.965, de 23 de abril de 2014. Dispõe sobre a legislação civil sobre proteção de dados pessoais e Marco Civil da Internet**. https://www.planalto.gov.br/ccivil_03/leis/l12965.htm. Acesso em: 20 ago. 2024.

BRASIL. (2018). **Lei nº 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados Pessoais.** https://www.planalto.gov.br/ccivil_03/leis/2018/l13709.htm. Acesso em: 20 ago. 2024.

BRASIL. (2023). **Projeto de Lei nº 1272, de 2023. Altera a Lei nº 9.610, de 19 de fevereiro de 1998, para criminalizar a adulteração de vídeos e áudios utilizando inteligência artificial.** http://www.camara.leg.br/propostas-legislativas/2272674. Acesso em: 20 ago. 2024.

BRASIL. (2024). **Projeto de Lei nº 146, de 2024. Estabelece normas gerais sobre a inteligência artificial e sua utilização no Brasil.** http://www.senado.gov.br/propostas-legislativas/1462024. Acesso em: 20 ago. 2024.

CHESNEY, R., & CITRON, D. K. (2019). **Deep fakes: A looming challenge for privacy, democracy and national security.** California Law Review, 107(6). https://ssrn.com/abstract=3213954. Acesso em: 15 out. 2024.

COSTA, C. (2020). **Cada vez mais sofisticados, deepfakes vieram para ficar.** Jornal da USP. https://jornal.usp.br/cultura/cada-vez-mais-sofisticados-deepfakes-vieram-para-ficar/. Acesso em: 19 set. 2024.

DAUER, L. (2024). **É #FAKE vídeo que mostra Biden xingando eleitores após desistir da corrida presidencial.** g1. https://g1.globo.com/. Acesso em: 19 set. 2024.

GOULART, E. (2023). **A Lei de Inteligência Artificial da União Europeia.** Conjur. https://www.conjur.com.br/2023-dez-20/a-lei-de-inteligencia-artificial-da-uniao-europeia/. Acesso em: 19 set. 2024.

GUILOU, P. (2020). **Qual é o princípio de funcionamento de um algoritmo de inteligência artificial?** Medium. https://medium.com/@pierre_guillou/qual-%C3%A9-o-principio-de-funcionamento-de-um-algoritmo-de-intelig%C3%AAncia-artificial-d68619ce2b#. Acesso em: 20 set. 2024.

LAVAGNOLI, S. (2020). **Como surgiu a Inteligência Artificial?** OpenCADD. https://www.opencadd.com.br/blog/como-surgiu-a-inteligencia-artificial. Acesso em: 20 out. 2024.

MACHADO, A. (2020). **Especialistas explicam como computador de Carolina Dieckmann foi hackeado.** O Globo. https://oglobo.globo.com/rio/especialistas-explicam-como-computador-de-carolina-dieckmann-foi-hackeado-4895771. Acesso em: 19 set. 2024.

RUDNITZKI, E. (2020). **Yes, nós temos deepfake: brasileiros são o 2º maior público de aplicativo que "troca rostos" de políticos e celebridades. Pública.** Disponível em: https://apublica.org/2020/08/yes-nos-temos-deepfake-brasileiros-sao-o-2o-maior-publico-de-aplicativo-que-troca-rostos-de-politicos-e-celebridade. Acesso em: 19 set. 2024.

UNIÃO EUROPEIA. (2021). **Proposta de Regulamento do Parlamento Europeu e do Conselho que Estabelece Regras Harmonizadas em Matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e altera Determinados Atos Legislativos Da União.** Bruxelas, 21 abr. 2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206. Acesso em: 19 set. 2024.