

Ana Camelo

**MUITO ALÉM DE UM
VÍDEO FALSO**

Usos e abusos das deepfakes¹

Apesar da consideração e discussão de algumas aplicações potencialmente positivas de deepfakes, como uso terapêutico para trauma, luto, ou transtorno de estresse pós-traumático²³, estas e outras aplicações da tecnologia levantam uma série de questões éticas⁴, políticas, econômicas e jurídicas importantes, contudo, por vezes pouco nomeadas. Neste ensaio, buscomapear algumas dimensões que compõem esse debate para além da camada superficial dos temas e impactos recorrentemente mais citados e analiso possíveis estratégias para superá-los.

As estatísticas chamam atenção para a multiplicação de casos e danos causados nos setores financeiros e corporativos⁵, especialmente visados com ataques que simulam vozes e rostos de altos executivos para autorizar transferências fraudulentas. O caso da multinacional Arup, no qual uma funcionária foi enganada a transferir \$25 milhões para fraudadores - que usaram tecnologia deepfake e se passaram pelo CFO da empresa em uma videoconferência, e a clonagem de voz e imagens do YouTube do CEO de um importante grupo de publicidade do mundo também para golpe aplicado via WhatsApp, ilustram os desafios a serem encarados. A tecnologia também tem sido utilizada para fraudar processos seletivos e de contratação de empresas dos EUA, resultando não apenas em prejuízo financeiro, mas também risco institucional e de segurança nacional⁶. Dados da consultoria Gartner⁷ chamam atenção para a possibilidade de, até 2028, 1 em cada 4 candidatos a emprego no mundo todo será falso.

¹ Pesquisadora do Centro de Ensino e Pesquisa em Inovação (CEPI FGV Direito SP). Doutora em Política Científica e Tecnológica; Mestre em divulgação científica e cultural. Ambos pela Unicamp. <http://lattes.cnpq.br/4264807675267479>

² Minnen, A. v, et al. Initial development of perpetrator confrontation using deepfake technology in victims with sexual violence-related PTSD and moral injury. *Journal of Digital Psychology*, v. 12, n. 3, p. 45–60, 2022. Disponível em: <https://pmc.ncbi.nlm.nih.gov/articles/PMC9435301/> . Acesso em: 9 set. 2025.

³ DEEPFAKE therapy. IMDb, 2023. Disponível em: <https://www.imdb.com/pt/title/tt12672938/> . Acesso em: 9 set. 2025.

⁴ Fuguy, A.; Jamali, Lily. A, man shot dead in road rage 'returns' to address his killer. BBC, 2025. Disponível em: <https://www.bbc.com/news/articles/cq808px90wxo> . Acesso em: 9 set. 2025.

⁵ Oliveira, N.. 5 Golpes com Deepfake que Ameaçam Empresas: Como a Engenharia Social Avançada Está Explorando a Alta Gestão. IT Show, 2023. Disponível em: <https://itshow.com.br/golpes-deepfake-empresas-riscos> . Acesso em: 9 set. 2025.

⁶ Thapa, A.; Son, H. How deepfake AI job applicants are stealing remote work. CNBC, 11 jul. 2025. Disponível em: <https://www.cnbc.com/2025/07/11/how-deepfake-ai-job-applicants-are-stealing-remote-work.html> . Acesso em: 9 set. 2025.

⁷ Stamford, C.. Gartner survey shows just 26% of job applicants trust AI will fairly evaluate them. Gartner Newsroom, 31 jul. 2025. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2025->

Segundo dados do Banco Central, no Brasil, fraudes com deepfakes provocaram R\$ 2,5 bilhões em perdas no mercado financeiro⁸. Há também relatos do uso de deepfakes para acesso às contas gov.br, criando vulnerabilidades inesperadas⁹.

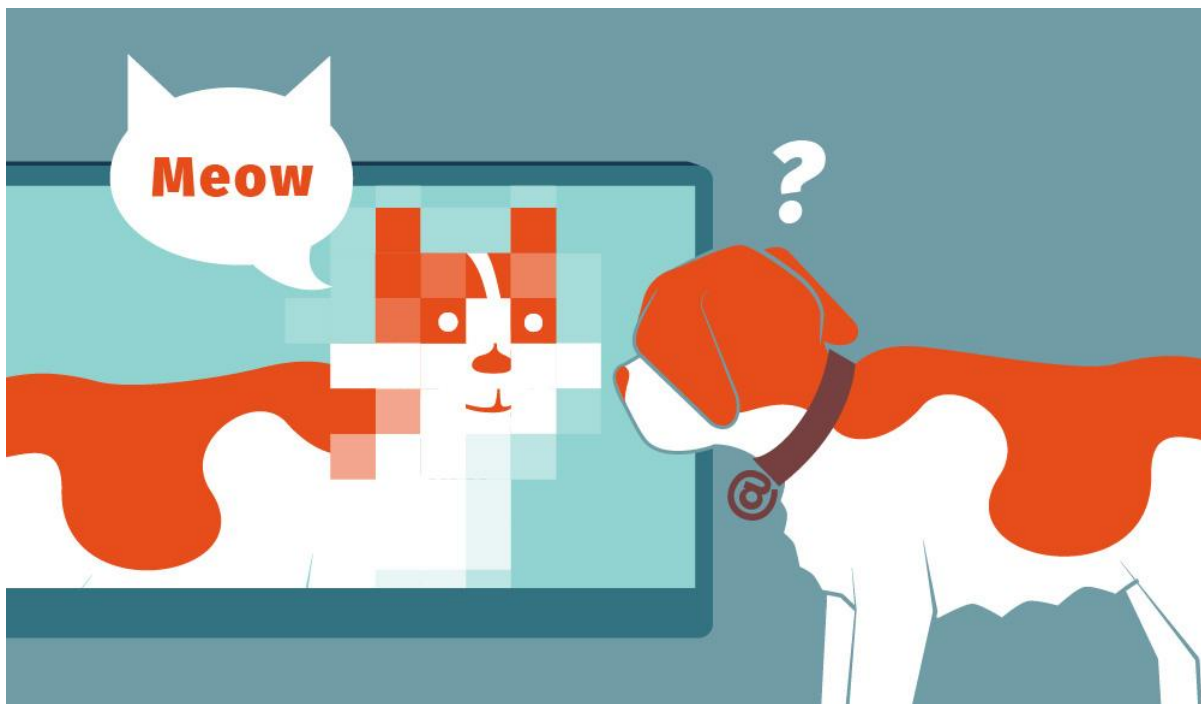


Figura 1. Deepfakes – when video evidence lies (iBarry, s/d)¹⁰

Enquanto alguns conteúdos gerados pela tecnologia deepfake são usados para fins de entretenimento, como em canais de televisão na Coreia do Sul para ler notícias¹¹ ou emulando dublês digitais realistas, substituindo rostos, imitando vozes e movimentos em cenas impossíveis ou difíceis de filmar¹², muitos usos são maliciosos e explorados para difamação ou golpes. Várias figuras públicas já tiveram suas

[07-31-gartner-survey-shows-just-26-percent-of-job-applicants-trust-ai-will-fairly-evaluate-them](#).

Acesso em: 9 set. 2025.

⁸ PINHEIRO, P P.. Como o mercado financeiro é afetado pelas fraudes por deepfake? Febraban Tech, 19/12/2023. Disponível em: <https://febrabantech.febraban.org.br/especialista/patricia-peck-pinheiro/como-o-mercado-financeiro-e-afetado-pelas-fraudes-por-deepfake> . Acesso em: 9 set. 2025.

⁹ OECD. Operation Face Off Targets AI-Driven Fraud on GOV.BR AI. OECD.AI, 2025. Disponível em: <https://oecd.ai/en/incidents/2025-05-13-e91f> . Acesso em: 9 set. 2025.

¹⁰ Deepfakes – when video evidence lies. Disponível em: <https://www.ibarry.ch/en/internet-risks/deep-fake/>. Acesso em 29 out. 2025.

¹¹ Debusmann Jr, Bernd. A evolução do deepfake, futuro da criação de conteúdo. BBC Brasil, 2022. Disponível em: <https://www.bbc.com/portuguese/geral-60431825> . Acesso em: 9 set. 2025.

¹² FOLHA DE S.PAULO. Atores de Hollywood temem uso de inteligência artificial, e buscam novo acordo, 6/6/2023. Disponível em: <https://www1.folha.uol.com.br/tec/2023/06/atores-de-hollywood-buscam-novo-acordo-sobre-uso-de-dubles-digitais-com-ia.shtml> . Acesso em: 9 set. 2025.

imagens e vozes manipuladas e se tornaram manchetes vinculadas ao fenômeno¹³. Enquanto isso, as redes sociais são inundadas por vídeos criados digitalmente usando as identidades de médicos famosos para promover curas milagrosas¹⁴, além da tecnologia poder ser utilizada para alterar imagens ou registros médicos para fins de fraude, como fraude de seguro¹⁵.

As estatísticas são alarmantes e há algumas projeções de que casos envolvendo *phishing* e fraude por deepfake dispararam, crescendo 822% no Brasil entre o primeiro trimestre de 2023 e o mesmo período de 2024¹⁶.

Além da produção e disseminação de notícias falsas; bullying e difamação, são cada vez mais comuns aplicações em situações de violência doméstica de gênero com o uso de deepfakes para ameaçar, chantagear e abusar das vítimas; para influenciar processos eleitorais e manipular disputas políticas. Durante as eleições municipais de 2024, a candidata à reeleição à prefeitura da cidade de Bauru, no interior de São Paulo, foi vítima da circulação, em redes sociais, de conteúdo sintético. Nas imagens divulgadas estrategicamente durante o período eleitoral, o corpo de Suéllen Rosim é exposto em nudez¹⁷.

É interessante também considerar que "brasileiros são o 2º maior público de aplicativo que 'troca rostos' de políticos e celebridade"¹⁸.

O argumento por trás desses exemplos, que não são exaustivos frente a diversidade e quantidade de usos da tecnologia, é que este é um problema social,

¹³ Tilia, Caroline. Celebidades brasileiras são vítimas da IA: aprenda a reconhecer conteúdos falsos. Forbes Tech, jan. 2025. Disponível em: <https://forbes.com.br/forbes-tech/2025/01/celebidades-brasileiras-sao-vitimas-da-ia-aprenda-a-reconhecer-conteudos-falsos/>. Acesso em: 9 set. 2025.

¹⁴ Simone Machado. Brasil. Deepfakes são usados para aplicar golpes em beneficiários do INSS. BBC Brasil, 2025. Disponível em: <https://www.bbc.com/portuguese/articles/c8788pv7z7jo>. Acesso em: 9 set. 2025.

¹⁵ FOLHA DE S.PAULO. Anúncios usam deepfake para aplicar golpes em beneficiários do INSS; saiba como se proteger. Folha de S.Paulo, maio 2025. Disponível em: <https://www1.folha.uol.com.br/mercado/2025/05/anuncios-usam-deepfake-para-aplicar-golpes-em-beneficiarios-do-inss-saiba-como-se-protoger.shtml>. Acesso em: 9 set. 2025.

¹⁶ SERASA EXPERIAN. Brasil tem recorde nas tentativas de fraude registradas em janeiro. Sala de Imprensa Serasa Experian, 2025. Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/indicadores/brasil-tem-recorde-nas-tentativas-de-fraude-registradas-em-janeiro-aponta-serasa-experia>. Acesso em: 9 set. 2025.

¹⁷ CARTA CAPITAL. Candidata à reeleição em Bauru (SP) é vítima de 'deepfake' em campanha. Carta Capital, 2024. Disponível em: <https://www.cartacapital.com.br/politica/candidata-a-reeleicao-em-bauru-sp-e-vitima-de-deepfake-em-campanha/>. Acesso em: 27 out. 2025.

¹⁸ RUDNITZKI, Ethel. Yes, nós temos deepfake: brasileiros são o 2º maior público de aplicativo que "troca rostos" de políticos e celebridades. Agência Pública, 13 ago. 2020. 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-celebridades/>. Acesso em: 9 set. 2025.

tecnológico, político e econômico que precisa ser enfrentado de forma a reconhecer a sua complexidade e urgência, especialmente em tempos de Inteligência Artificial Generativa. "Espera-se que a IA generativa aumente o risco de deepfakes" e "nunca foi tão fácil criar conteúdo falso — ou tão difícil de detectar"¹⁹, chama a atenção análise da Deloitte focada no setor bancário que se extrapola aqui para as demais ameaças criadas por essas ferramentas.

Compromissos pela integridade da informação

Embora não sejam tão amplamente divulgados quanto os casos envolvendo famosos, os crimes envolvendo "pessoas comuns" também se multiplicam por meio de deepfakes de áudio e vídeo que imitam a voz de parentes ou amigos. Esta capacidade torna possível criar áudio e vídeo de pessoas reais dizendo e fazendo coisas que nunca disseram ou fizeram e essa realidade impõe enfrentarmos não apenas os danos e consequências, mas as suas causas e as incertezas que marcam a discussão.

Uma das principais preocupações é que a capacidade de distorcer a realidade deu um salto exponencial na erosão da integridade informacional e as medidas de remediação são insuficientes e não acompanham a velocidade da evolução tecnológica.

Diante do fato de que talvez muito pouco saibamos sobre as possibilidades, os riscos e os impactos gerados pela tecnologia, urge o desafio de lidar com a incerteza, com o fato de que existem coisas que não sabemos que não sabemos.

Enquanto observa-se uma tendência importante no debate sobre evolução das ameaças cibernéticas, regulação e desenvolvimento tecnológico para identificar e rotular esse tipo de conteúdo, o argumento deste texto é que precisamos ampliar o debate na interface com uma abordagem centrada em direitos humanos, necessidade de cooperação global, lacunas na detecção e divulgação e o desafio de encarar manipulações mais sofisticadas.

O impacto das deepfakes no que acreditamos, no que vemos e quem pode ser acreditado também abre espaço para questionamento da própria noção de “prova

¹⁹ LALCHAND, S. et al. Deepfake banking fraud risk on the rise. Deloitte Insights, 29 maio 2024. Disponível em: <https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html>. Acesso em: 9 set. 2025.

visual” não apenas na mídia, na ciência e também na justiça. Já existem artigos que problematizam a capacidade de manipular vídeos e áudios falsificados e altamente realistas que podem comprometer a integridade da memória coletiva²⁰ e também enganar juízes, jurados e partes envolvidas, comprometendo a credibilidade das provas apresentadas e influenciando decisões judiciais de forma indevida²¹²².

Diante desse cenário, não se pode desconsiderar outros fatores como o design das deepfakes (treinados para simular a realidade), as plataformas que permitem ou restringem o uso de filtros dessa natureza, a decisão de investir, difundir ou regular as deepfakes, todos têm natureza e efeitos políticos inevitáveis, já que moldam realidades possíveis e distribuem riscos. Por isso, também no começo deste texto, argumentei que este é um desafio complexo, interdisciplinar e multissetorial. A tecnologia sozinha não é capaz de combater e minimizar totalmente a escala e os danos das deepfakes, embora ferramentas avançadas de detecção baseadas em inteligência artificial (IA) sejam essenciais no enfrentamento do problema.

De fato, existem ferramentas relativamente sofisticadas que utilizam IA para identificar deepfakes em tempo real, analisando padrões faciais, inconsistências temporais, movimentos labiais versus áudio e outros sinais sutis de manipulação invisíveis ao olho humano. Porém, a rápida evolução das técnicas de deepfake cria um ciclo contínuo, no qual novos métodos de falsificação desafiam as ferramentas de detecção, exigindo atualização constante dos modelos de IA. A detecção não é infalível e algoritmos podem ter dificuldades com deepfakes sofisticados ou desconhecidos²³. Além disso, a tecnologia não resolve questões que envolvem julgamento crítico humano ou avaliação do contexto, que são essenciais para mitigar os impactos das deepfakes. A resposta mais eficaz ao problema requer uma abordagem multidimensional, integrando tecnologia de ponta com políticas públicas,

²⁰ ALAIMO, Kara. Deepfakes causam danos duradouros às crianças; veja como protegê-las. CNN Brasil, 3 jan. 2025. Disponível em: <https://www.cnnbrasil.com.br/saude/deepfakes-causam-danos-duradouros-as-criancas-veja-como-protege-las/>. Acesso em: 9 set. 2025.

²¹ SILVA, João; OLIVEIRA, Maria. Deepfakes e os desafios jurídicos contemporâneos. Revista Rumos, v. 1, n. 7, p. 45–60, 2024. Disponível em: <https://revistas.unicerp.edu.br/index.php/rumos/article/download/2525-278x-v1n7-6/2525-278x-v1n7-6/1268>. Acesso em: 9 set. 2025.

²² LEXLEGAL. Deepfakes em provas judiciais: estamos preparados para a manipulação de evidências digitais? LexLegal, 2025. Disponível em: <https://lexlegal.com.br/deepfakes-em-provas-judiciais-estamos-preparados-para-a-manipulacao-de-evidencias-digitais/>. Acesso em: 9 set. 2025.

²³ OLIVEIRA, Marcos de. Deepfakes: o novo estágio tecnológico das notícias falsas. Revista Pesquisa FAPESP, 2025. Disponível em: <https://revistapesquisa.fapesp.br/deepfakes-o-novo-estagio-tecnologico-das-noticias-falsas/>. Acesso em: 9 set. 2025.

educação midiática, regulamentação, cooperação internacional e sensibilização social para reconhecimento e combate a conteúdos falsos. A tecnologia funciona como primeira linha de defesa, capaz de bloquear, sinalizar e reduzir a disseminação de conteúdos falsos. Também são necessárias leis que obriguem transparência na identificação de conteúdo gerado por IA e maior responsabilização dos envolvidos.

A análise proposta através do artigo "What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape"²⁴, de forma bastante construtiva, lembra que "desafios impostos pelos deepfakes não são totalmente inéditos, mas sim uma extensão das discussões em andamento sobre a disseminação de conteúdo nocivo e ilegal". A necessidade de conhecimento baseado em evidências e pesquisa empírica é fundamental e perene.

Portanto, o reconhecimento da dimensão política do design e da aplicação de deepfakes talvez seja um primeiro caminho. Deepfakes não são apenas "ferramentas técnicas", mas sobretudo políticas, tecnologias que podem fortalecer ou minar a confiança pública em inúmeros e diversos segmentos.

²⁴ WEST, Sarah; KRAFFT, Peter M. What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape. *New Media & Society*, 2024. Disponível em: <https://journals.sagepub.com/doi/10.1177/14614448241253138> . Acesso em: 9 set. 2025.