

DEEPFAKES

Definição

O termo *deepfake* resulta da junção de “deep learning” (aprendizagem profunda) e “fake” (falso). Designa conteúdos audiovisuais (vídeo, imagem ou áudio) criados ou manipulados por IA para simular, com elevado realismo, a identidade, o rosto ou a voz de uma pessoa real. A expressão tornou-se pública em 2017 (Coura et al., 2026).

Três modalidades frequentes



TROCA DE ROSTO

Substituição do rosto de uma pessoa pelo de outra num vídeo existente.



CLONAGEM DE VOZ

Reprodução sintética de uma voz humana a partir de pequenas amostras.



SINCRONIZAÇÃO LABIAL

Alteração dos movimentos da boca para simular declarações.

As duas faces da tecnologia

USOS LEGÍTIMOS

- ✓ Produção cinematográfica
- ✓ Dobragem multilingue automática
- ✓ Recriação digital autorizada
- ✓ Campanhas educativas e culturais



USOS ILÍCITOS

- ✗ Usurpação de identidade
- ✗ Fraude por comprometimento de correio eletrónico empresarial
- ✗ Desinformação política
- ✗ Pornografia não consensual



Quatro riscos principais

FINANCEIRO

Fraude e engenharia social

Usurpação de identidade /voz sintética em esquemas de fraude empresarial (ThreatMark, 2025; CNCS, 2025)

POLÍTICO

Desinformação eleitoral

Manipulação audiovisual para amplificar desinformação e influenciar processos democráticos (Coura et al., 2026)

PESSOAL

Violação da imagem e da intimidade

Conteúdos íntimos não autorizados podem causar danos civis e psicológicos significativos.

SOCIAL

Erosão da confiança pública

Dificuldade em distinguir evidência autêntica de conteúdo sintético (“crise da verdade”) (IA no Trabalho, 2026).

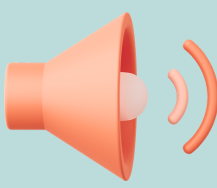
Sinais que devem alertar

SINAIS VISUAIS



- Iluminação incoerente
- Contornos imprecisos
- Desfasamento som-imagem
- Distorções na boca
- Movimentos pouco naturais
- Pormenores anatómicos (mãos, dentes, orelhas, pele...)

SINAIS SONOROS



- Entoação artificial
- Ritmo demasiado regular
- Ausência de pausas respiratórias
- Ruído de fundo inconsistente
- Voz “mecânica” ou “sintética”

Nota: estes sinais não constituem prova definitiva; servem para justificar verificação adicional.

Como proteger-se

01

LITERACIA MEDIÁTICA

Para uma leitura crítica (confirmar a fonte original, cruzar com meios credíveis e evitar partilhas impulsivas)

02

FERRAMENTAS DE DETEÇÃO

Sistemas automáticos que analisam píxeis/metadados; não são infalíveis (UncovAI, 2026).

03

LEI E DENÚNCIA

O Regulamento da IA da UE exige transparência para conteúdos sintéticos que induzam em erro (Comissão Europeia, 2025).

Referências Bibliográficas

Centro Nacional de Cibersegurança. (2025). *Relatório de cibersegurança em Portugal – tema riscos & conflitos* (6.ª ed.). <https://www.cncs.gov.pt/docs/rel-riscosconflitos2025-obcibercncs.pdf>

Comissão Europeia. (2025, 10 de novembro). *Comissão Europeia lança processo para código de boas práticas sobre conteúdos criados por IA*. Digital.gov.pt. <https://digital.gov.pt/noticias/comissao-europeia-lanca-processo-para-codigo-de-boas-praticas-sobre-conteudos-criados-por-i>

Coura, A. B., Borges de Liz, K., & Gomes, K. E. (2026, 27 de fevereiro). *Deepfake e inteligência artificial generativa - desafios regulatórios para as eleições de 2026*. Migalhas. <https://www.migalhas.com.br/depeso/450480/deepfake-e-ia-generativa--desafios-regulatorios-para-as-eleicoes-2026>

IA no Trabalho. (2026, 28 de janeiro). *A crise da verdade: Como identificar deepfakes e proteger sua imagem em 2026*. <https://ianotrabalho.com/como-identificar-deepfakes-2026/>

ThreatMark. (2025, 30 de maio). *AI vs. Fraud: The future of fraud defense* [White paper]. <https://www.threatmark.com/wp-content/uploads/2025/05/ThreatMark-AI-vs-Fraud-The-Future-of-Fraud-Defense-Whitepaper.pdf>

UncovAI. (2026). *10 best deepfake detection tools of 2026: Real-time guide*. <https://uncovai.com/best-deepfake-detection-tools-2026/>

Guia - Deepfakes © 2026 by LIDERA is licensed under CC BY-NC-SA 4.0.