Deepfake em ano de eleições: como prevenir e identificar

Tecnologia

8 Março, 2024 | 3 minutos de leitura

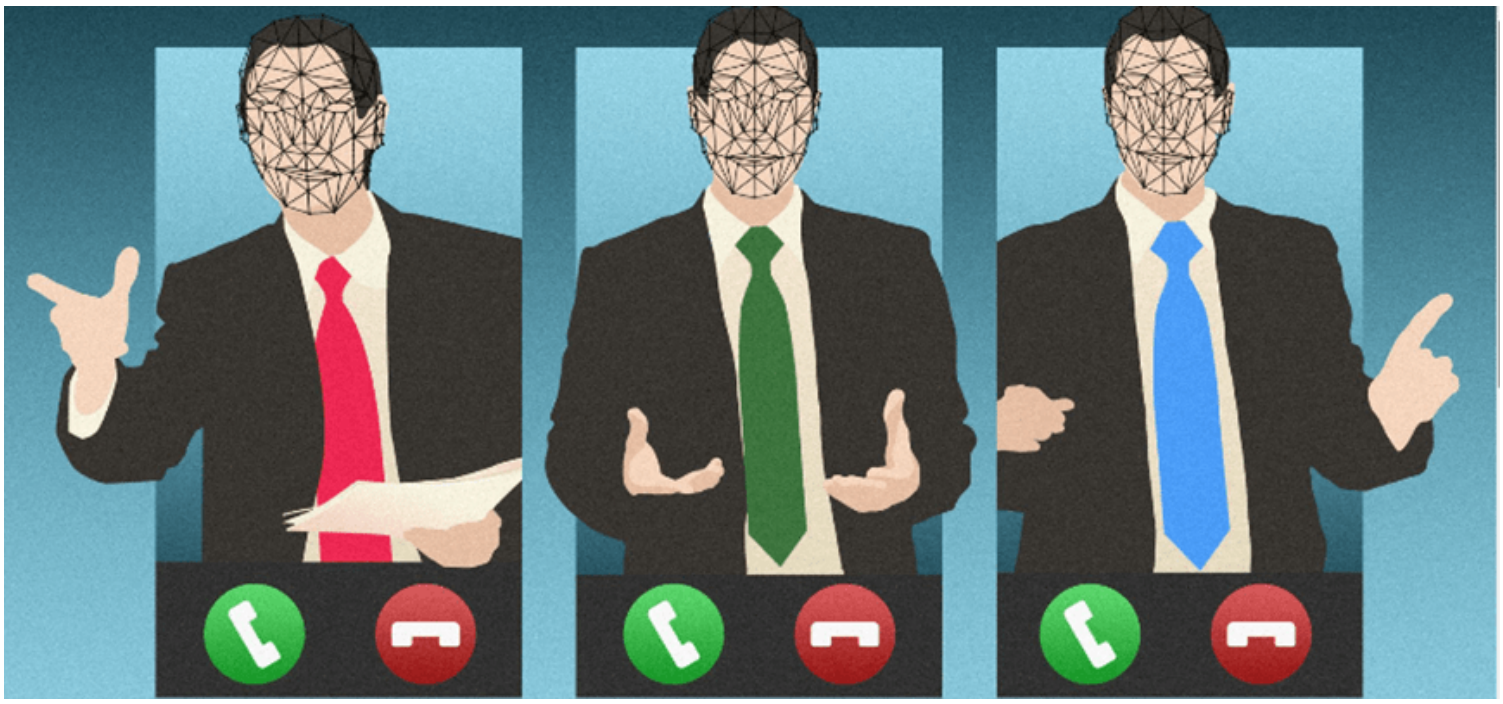
Em 2024, cerca de **40 países no Mundo vão realizar eleições**, incluindo Portugal, e o *deepfake* representa uma preocupação particular ao nível de campanhas de desinformação altamente disseminadas nas várias redes sociais.

A ENISA (Agência Europeia para a Segurança das Redes e da Informação) no relatório "Threat Landscape", destaca o **aumento nos *chatbots* de IA, *deepfakes* e tecnologias semelhantes** e recomenda que Governos, setor privado e os meios de comunicação social se mantenham em particular alerta para detetar e combater a desinformação online impulsionada por IA.

O *Deepfake*, a tecnologia de IA utilizada para criar perfis, vídeos, imagens e áudios falsos de pessoas reais, é já amplamente usado para tentativas de burlas, manipular a opinião pública, espalhar notícias falsas e provocar desconfiança e confusão entre o público.

A tecnológica VisionWare partilha alguns casos de *deepfakes*, na esfera política, e deixa **sete pistas** para que o cidadão consiga detetar estes esquemas:

1. Incongruências na pele e em partes do corpo
2. Sombras à volta dos olhos
3. Padrões de pestanejo invulgares
4. Brilho invulgar nos óculos
5. Movimentos labiais incompatíveis ou irrealistas
6. Coloração não natural dos lábios em relação ao rosto
7. Manchas irrealistas no rosto



O Caso do Volodymyr Zelensky

A 16 de março de 2022, o canal de TV Ukraine 24 parecia ter sido tomado por hackers pró-russos, com a transmissão de uma mensagem supostamente escrita pelo presidente Zelensky a pedir a rendição dos soldados ucranianos.

Nesse mesmo dia, vídeos *deepfake* que usaram o rosto de Volodymyr Zelensky foram transmitidos no Telegram, a promover a mesma mensagem de que os soldados ucranianos deveriam render-se às forças russas.

O Caso da Eslováquia

Nas eleições legislativas da Eslováquia, no ano passado, dias antes das eleições foram partilhados, nas redes sociais, áudios *deepfake* de um dos principais candidatos. Entre os áudios falsos ouvia-se Michal Šimečka a debater formas de falsificar as eleições com a compra de votos da comunidade local.

Šimečka denunciou imediatamente como falso e apesar de ter sido confirmado que o áudio mostrava sinais de manipulação por meio de IA, a gravação foi publicada 48 horas antes da abertura das urnas. As gravações tornaram-se virais nas redes sociais e muitas pessoas acreditaram. Šimečka, o candidato cujo partido se diz estaria mais em concordância com os valores e interesses ocidentais, foi derrotado por um oponente que apoiava laços mais estreitos com Moscovo.

Tik Tok une-se ao Polígrafo para combater desinformação política