Localização da matéria

VEÍCULO: DIÁRIO DO AÇO
CADERNO: OPINIÃO
ACESSADO EM: 25-01-2022
PUBLICADO EM: 22-01-2022

Link: https://cutt.ly/5I4hnsb

22 de janeiro, de 2022 | 18:00

OPINIÃO

Perigo x brincadeira: entenda os riscos do deepfake

Divulgação

Maria Cristina Diez *

"Há ferramentas bastante eficientes capazes de desmascarar de forma muito rápida e fácil as tentativas de manipulação e uso da imagem e da voz de pessoas"

Se você já deparou com alguma montagem do seu rosto com um corpo que não é seu, numa performance que definitivamente também não é sua, você já tem uma noção razoável do que é um deepfake. Alguns aplicativos gratuitos permitem "te encaixar" em diferentes vídeos, tornando a brincadeira até divertida, mas por trás dela mora um grande perigo, e que já entrou no radar dos sistemas de segurança digital.

O problema é que o deepfake está longe de ficar só no campo das brincadeirinhas. Há casos até de vídeos pornográficos utilizando rostos de pessoas conhecidas ou ainda de aplicações de figuras influentes fazendo afirmações polêmicas, que beiram o absurdo. Por ser produzidos com base em arquivos de código aberto, o resultado do aprendizado desses softwares tem sido movimentações faciais cada vez mais próximas da realidade e de maneira cada vez mais fácil de manipulação.

Pra piorar, a "trolagem" evoluiu junto com os avanços tecnológicos. Hoje existem softwares que permitem que qualquer pessoa manipule também vozes a partir de uma captura verdadeira, emitindo uma mensagem oral que jamais foi pronunciada pelo dono. Associadas a uma pessoa real, imagem e voz numa harmonia perfeita promovem uma encenação falsa, mas que engana bastante para quem não está familiarizado com esses apps.

Isso, é claro, vem gerando um debate ético sobre essas simulações, já que, levadas a termo num ambiente político, por exemplo, podem destruir por completo a imagem de uma pessoa pública. Em pleno ano eleitoral, torna-se mais fácil o desafio de entender os perigos existentes por trás de um deepfake. Até conseguir provar que a imagem é manipulada, o estrago já foi feito.

Além disso, esse tipo de simulação também faz aumentar o risco de uso de uma identidade pessoal para burlar sistemas acesso de segurança por meio de onboarding digital. A distância que separa o original e do falso está cada vez menor, e isso obriga a Inteligência Artificial a trabalhar de forma mais firme na busca por soluções que eliminem eventuais experiências negativas nesse campo.

Talvez a forma mais eficiente de contra-atacar o deepfake seja por meio da chamada Liveness, ou 'prova de vida'. O sistema oferece garantia de autenticação e vivacidade de um registro facial e de voz, com a vantagem de poder ser implementado via aplicativo no ambiente mobile ou por meio da web. Sua avaliação é feita a partir de um vídeo-selfie produzido na hora pelo usuário.

É um processo que complementa o sistema de biometria facial para a redução de fraudes. E, da mesma forma como o deepfake avança junto com novas incorporações tecnológicas, também a prova de vida é amparada em conceitos de machine learning que conseguem registrar com maior precisão as leituras feitas sistematicamente de um rosto no ato do onboarding.

Os ataques cibernéticos tendem a continuar usando rostos conhecidos em brincadeiras com fins escusos. Mas há ferramentas bastante eficientes capazes de desmascarar de forma muito rápida e fácil as tentativas de manipulação e uso da imagem e da voz de pessoas para ingressar em seus sistemas. Essa é uma batalha em que o bem está ganhando.

* Diretora comercial e de marketing da Most Specialist Technologies - cristina@most.com.br