Por Rodrigo Kramper (*)

O deepfake trata-se do uso da Inteligência Artificial para emular a voz e, ou, expressões faciais de uma pessoa com base em vídeos, áudios ou fotos disponíveis on-line. Ou seja, a partir de dados de áudio e imagem, o software é capaz de produzir imagens e sons que se assemelham a humanos.

A tecnologia tem gerado tanto interesse que a busca pelo termo, na ferramenta de captação de trends Exploding Topics, cresceu mais de 2.200% entre 2017 e 2021. O problema do deepfake está no fato de que é cada vez mais difícil distinguir entre o que é real e o que é falso.

Há três tipos essenciais de deepfake: a reconstituição facial, cujo software molda a face de uma pessoa em outra, mantendo as características da primeira; a sintetização de fala, ou seja, a produção da voz humana - ambas as técnicas foram utilizadas no programa humorístico Greg Shapiro da renúncia de Donald Trump; e a geração facial, que cria um rosto, de uma pessoa que não existe, a partir de imagens de pessoas reais.

Para as organizações, o deepfake representa dois riscos principais: a engenharia social e a perda de reputação. A engenharia social é a manipulação psicológica de usuários de forma a induzi-los a compartilhar dados confidenciais ou realizar ações inadequadas. Uma reportagem do Wall Street Journal mostrou que criminosos emularam a voz do CEO de uma companhia e conduziram uma chamada telefônica com um funcionário solicitando uma transferência de 243 mil dólares a um parceiro.

A Universidade Amsterdam conduziu uma pesquisa na qual foi apresentado, para 287 pessoas, um deepfake de um político holandês proferindo um discurso controverso e a maior parte dos participantes assumiu que o vídeo era verdadeiro. No Brasil, um fato semelhante ocorreu nas eleições presidenciais de 2018, no qual um deepfake de cunho sexual do então candidato João Dória foi disseminado nas mídias.

Diante desse formato, no qual líderes podem ser facilmente expostos, qual seria o impacto para a imagem de uma organização ao ter um vídeo de seu CEO fazendo discursos racistas ou corruptos ou ainda protagonizando cenas pornográficas? É importante lembrar que os executivos são alvos fáceis porque concedem entrevistas, proferem palestras, ou seja, têm suas imagens veiculadas em diversos momentos e mídias, o que pode ser um acervo de matérias primas para criminosos.

Para se proteger desses riscos, executivos e organizações precisam estar atentos em três aspectos. O treinamento de funcionários é uma das principais formas de prevenir que criminosos tenham êxito em atuações maliciosas. Por isso, é necessário adotar programas de conscientização sobre os riscos dos deepfakes e estabelecer uma cultura crítica em relação a abordagens convincentes, mas que parecem fora de lugar, ou seja, é a cultura do acreditar, mas checar os fatos. Como citado, podemos, sim, receber um telefonema do CEO, mas é importante sinalizar mensagens atípicas, como a de agilizar um pagamento de 243 mil dólares de um negócio que ninguém conhece.

Além dos treinamentos, investir em tecnologias emergentes também é uma proteção às empresas no combate às ações maliciosas. Alguns avanços já estão sendo feitos na direção de tecnologias que detectam deepfakes, incluindo mecanismos de adversarial machine learning.

Por fim, implementar um comitê de gestão de crises colocará à disposição da empresa pessoas e estruturas prontas para analisar e atestar a falsidade da informação, além de responder e comunicar à opinião pública em situações nas quais os deepfakes emergem.

(*) **Rodrigo Kramper** é líder da prática de Advanced Data & Analytics Solutions da ICTS Protiviti, empresa especializada em soluções para gestão de riscos, compliance, auditoria interna, investigação, proteção e privacidade de dados.

Fonte: Image Comunicação, em 03.09.2021