Áudio é maior risco no avanço do uso de deepfake em eleições

IA foi utilizada para influenciar política de ao menos 16 países em 2023, diz relatório

Patrícia Campos Mello

SÃO PAULO Às vésperas da eleição para a Prefeitura de Chicago, nos Estados Unidos, viralizou um vídeo em que um homem dizia: "Antigamente, um policial podia matar 17 ou 18 pessoas e ninguém nem piscava. Essa conversa de 'tire os recursos da polícia' vai levar ao caos e à ilegalidade".

O homem do vídeo era igualzinho ao candidato à prefeitura Paul Vallas — e tinha a mesma voz. Mas era um vídeo de-epfake, uma manipulação feita com inteligência artificial, que havia sido postada em uma conta recém-criada no X (antigo Twitter), e que fingia ser um veículo de mídia com o nome de Chicago Lakefront News.

A campanha de Vallas denunciou o vídeo, que foi imediatamente retirado da rede social. Mas já era tarde. O deepfake havia sido compartilhado milhares de vezes. Vallas perdeu a eleição para Brandon Johnson — que, justamente, disputava os votos dos eleitores moderados e era crítico da violência policial.

A eleição em Chicago, em fevereiro de 2023, foi prenúncio da avalanche de áudios, vídeos e imagens eleitorais falsas que estava por vir.

Segundo levantamento da Freedom House, em 2023, a inteligência artificial generativa foi usada em pelo menos 16 países para criar vídeos, imagens ou áudios para "semear dúvidas, difamar opositores ou influenciar o debate público".

Deepfakes — imagens, áudios ou vídeos criados com a ajuda de modelos de inteligência artificial — estão mais realistas e baratos. Inúmeras empresas oferecem serviços de criação de vídeos ou áudios sintéticos por preços a partir de US$ 5 por mês (cerca de R$ 25).

"O uso disseminado de deepfakes para manipular processos políticos e eleições deixou de ser uma questão teórica. É uma realidade", disse Henry Ajder, especialista em IA que já trabalhou com Meta, Adobe e Comissão Europeia.

"A partir de agora, a tecnologia só vai melhorar. Os deepfakes vão ficar cada vez mais baratos e realistas. E a quantidade de coisas que podem ser falsificadas vai se expandir muito."

A popularização da desinformação política alimentada por IA ocorre em um momento particularmente delicado — cerca de metade da população do planeta vota em nível nacional ou regional em 2024, pouco lugares têm regulação em vigor, as big techs reduziram equipes de segurança e os sistemas de detecção não são eficientes para identificar áudios falsos.

Na reta final da eleição parlamentar da Eslováquia, em setembro passado, o líder do partido que liderava as pesquisas foi atingido por um deepfake.

Na gravação, uma voz parecida com a de Michal Simecka, líder do partido Progressista, falava de um esquema para fraudar a eleição comprando votos de integrantes da minoria étnica roma. No fundo, uma imagem de Simecka.

O partido denunciou o áudio, classificado como falso pela agência France Presse. Ele foi rotulado como desinformativo no Facebook, mas não foi removido. O Direção Social-Democracia, partido populista pró-Rússia, derrotou o Progressista e conquistmaioria no Parlamento.

Nos EUA, eleitores democratas de New Hampshire receberam ligações com uma voz muito parecida à do presidente Joe Biden instando-os a não participar das primárias no estado, no fim de janeiro.

Segundo pesquisadores, o áudio foi criado com o software da startup de clonagem de voz Eleven Labs.

"O tipo de conteúdo sintético que mais consegue enganar as pessoas são os áudios gerados por IA, pois bastam três segundos da voz de alguém para treinar o modelo e conseguir um deepfake convincente", disse Ben Colman, presidente da Reality Defender, empresa de detecção de deepfakes.

Antes, as vozes clonadas soavam robóticas e artificiais. Agora, a tecnologia analisa milhões de vozes, padrões nos fonemas e nas pausas, e replica tudo de forma muito realista. É mais fácil notar manipulações em vídeos ou imagens do que em áudios.

Os detectores de IA não têm acompanhado a velocidade da evolução da tecnologia.

"As ferramentas de detecção avançaram muito, mas ainda têm um longo caminho a percorrer. Nunca chegaremos a 100% de precisão, então quais são outras coisas — como a alfabetização midiática — que precisamos combinar com o avanço tecnológico disso?", afirma Katie Harbath, chefe de assuntos globais da Duco Experts e ex-diretora de políticas públicas do Facebook.

"Não há um único sistema de detecção, uma bala de prata. É preciso entender as limitações, pois haverá vários resultados conflitantes", diz Ajder.

A regulação do uso de IA em eleições ainda engatinha.

No Brasil, minuta de resolução do TSE (Tribunal Superior Eleitoral), que precisa ser aprovada até março, obriga o uso de rótulos informando uso de IA em anúncios políticos e proíbe sua aplicação para adulterar áudios e vídeos.

O texto parece criar a obrigação das plataformas de identificarem esses conteúdos e removerem, se for o caso. Mas as big techs insistiram, em audiência pública no TSE, que a responsabilidade pela identificação do uso de IA é dos candidatos e partidos, não delas.

As empresas estabeleceram regras de uso exigindo rotulagem de anúncios políticos que usam IA e proibindo conteúdo sintético que interfira no processo democrático ou questione a integridade do sistema eleitoral. Não há, porém, fiscalização sobre sua aplicação.

Na União Europeia, a lei de IA foi aprovada em dezembro e ainda não entrou em vigor. Nos EUA, só alguns estados — Minnesota, Michigan, Washington, Califórnia, e Texas — regulamentaram o uso de IA em comunicação eleitoral. Uma lei federal tramita na Câmara, mas sem perspectiva de aprovação rápida.

A Índia anunciou que terá regras duras para responsabilizar as big techs por conteúdo deepfake nas plataformas. As eleições gerais do país começam em abril.

"Algumas plataformas adotaram políticas para mídia manipulada. Mas não adianta dizer 'isso não é permitido' se você não fiscalizar e aplicar essas políticas. Portanto o governo tem a responsabilidade de forçar as plataformas [a fazerem isso)", diz Ajder.

"Os criadores dessas novas ferramentas de IA, por sua vez, têm a responsabilidade de desenvolver medidas de segurança para seus produtos."

Para Jeffrey Blevins, professor de jornalismo e relações internacionais da Universidade de Cincinnati, só rotular as mídias sintéticas, como propõe o TSE, não basta. "Vai ser como enxugar gelo. Põem o rótulo de mídia manipulada em um anúncio, e logo surge outro".

E a proliferação das mídias sintéticas ocorre em um momento em que as plataformas estão menos preparadas — e dispostas — a intervir.

Após os escândalos da Cambridge Analytica e a interferência russa na eleição americana de 2016, as big techs criaram uma operação de controle de danos e reforçaram as equipes de "confiança e segurança".

Agora, estão no movimento inverso. O X demitiu boa parte da equipe de moderação após Elon Musk comprar a empresa. Até hoje, um áudio fake de outubro passado em que o líder do partido Trabalhista da Inglaterra, Keir Starmer, xinga e humilha um assistente segue lá sem alerta de mídia manipulada.

Nos EUA, as plataformas temem fazer moderação ou colaborar com autoridades após serem acusadas por políticos de direita de censurarem visões conservadoras.

Tudo isso deságua em um outro problema — os fake de-epfakes. Como vai ficar muito difícil dizer o que é verdadeiro e o que é IA, alegar deepfake vai virar escudo de muitos políticos flagrados em ilegalidades ou gafes.

O ex-presidente republicano Donald Trump, mais uma vez, foi o pioneiro.

Na eleição de 2016, abraçou a estratégia de chamar de fake news tudo quanto era notícia de que ele não gostava. Desta vez, a arma é o fake deepfake. Em dezembro, ele criticou um anúncio político que mostrava muitas de suas gafes, como o episódio em que ele não conseguia pronunciar a palavra "anônimo" e quando confundiu o nome de uma cidade na Califórnia — chamou de Pleasure o município de Paradise.

"Os pervertidos e perdedores do fracassado Lincoln Project [grupo de republicanos anti-Trump] estão usando inteligência artificial em propagandas na TV para que eu pareça estar tão mal quanto Joe Biden", declarou Trump, em sua rede social, a Truth Social. Todas as gafes mostradas no anúncio eram públicas e tinham sido amplamente noticiadas.

Existem inúmeros softwares, muitos deles gratuitos, que ajudam a detectar uso de IA. Nenhum deles é 100% eficiente. Sempre é necessário usar mais de um e ter um humano para analisar o contexto das publicações. A IA está avançando rapidamente, e muitas técnicas de detecção podem se tornar obsoletas.

O conteúdo é disseminado por perfis de redes sociais recém-criados ou com nomes que parecem ser de veículos de notícias. Veículos de mídia estabelecidos não compartilham as imagens, áudios ou vídeos.

> O uso disseminado de deepfakes para manipular processos políticos e eleições deixou de ser uma questão teórica. É uma realidade
>
> **Henry Ajder**
> especialista em IA que trabalhou com Meta, Adobe e Comissão Europeia

Como reconhecer a manipulação

Há softwares, muitos gratuitos, que ajudam a detectar uso de IA. Nenhum é 100% eficiente, sendo necessário o uso de mais de um e um humano para analisar o contexto. O conteúdo é disseminado por perfis recém-criados ou com nomes que parecem ser de veículos de notícias nas redes sociais

OUTROS INDÍCIOS

- Em áudio, as pausas entre as palavras são todas iguais ou muito inconsistentes
- As frases soam artificiais
- A pronúncia de algumas palavras é estranha
- Na maioria das vezes, a IA não replica de forma eficiente a respiração da pessoa ou o som ambiente
- Em vídeo, há discrepâncias sutis entre o movimento dos lábios e o que é dito
- Perfis falsos em redes sociais usando fotos geradas por IA costumam ter os olhos e bocas das "pessoas" todos na mesma altura do rosto — isso pode ser visto examinando as imagens lado a lado
- Imagens geradas por IA às vezes têm falhas em mãos, orelhas, lábios, olhos e cabelo. Também podem ter diferenças em tom ou textura da pele
- Barba, óculos e pintas podem ter aparência estranha
- Em vídeos, a pessoa pisca demais ou nunca pisca
- Perfis postam centenas de vezes por dia, muitas vezes com intervalo muito curto

Fonte: Digital Forensics Lab do Atlantic Council, Hany Farid da Universidade da Califórnia em Berkeley, MIT Media Lab

FORÇA AÉREA 1 COM LULA A BORDO ABORTA DECOLAGEM

O jato Airbus A319 da Força Aérea Brasileira que transportava o presidente Lula (PT) no domingo (4) precisou abortar a decolagem no aeroporto de Congonhas, em São Paulo. O avião decolava às 16h44, mas houve um problema e o procedimento foi interrompido. O jato deu meia volta e foi liberado para o voo cerca de 20 minutos depois Reprodução

Marinha e FGV organizam primeira pós em inteligência artificial para sistemas militares

BRASÍLIA Uma parceria da Marinha com a FGV (Fundação Getulio Vargas) resultou no primeiro curso de IA (inteligência artificial) voltado a sistemas militares ministrado no Brasil.

O curso de pós-graduação em Inteligência Artificial Aplicada a Sistemas Militares é destinado a oficiais que participam de programa de aperfeiçoamento do corpo de fuzileiros navais.

Esse programa visa aprimorar os conhecimentos científicos tecnológicos e doutrinários dos militares para o exercício operativo de cargos e funções em unidades e grupamentos operativos de fuzileiros navais, com ênfase no caráter expedicionário desses destacamentos.

De acordo com comunicado da Marinha, o objetivo é "adequar a capacitação à velocidade da evolução tecnológica e doutrinária no nível tático de condução da guerra".

"A parceria com a FGV é uma importante conquista, que seguramente trará resultados significativos para o Corpo de Fuzileiros Navais", afirmou, no comunicado, o comandante do Pessoal de Fuzileiros Navais, vice-almirante Pedro Gueiros Taulois.

"A expectativa é que os alunos aproveitem ao máximo essa oportunidade de estudar esse tema de absoluta relevância. A inteligência artificial é uma realidade cada vez mais impactante nas capacidades militares dos principais atores mundiais e a Marinha do Brasil está atenta a isso."

A aula inaugural foi ministrada na FGV no dia 31 de janeiro, por Alexandre Rocha Violante, doutor em Estudos Estratégicos pela Universidade Federal Fluminense e capitão de mar e guerra da reserva da Marinha.

"A produção do saber científico e tecnológico, um aspecto fundamental na construção das nações modernas, está intrinsecamente relacionada a Segurança e Defesa Nacional", destacou Violante, também no comunicado.

"Essa evolução é contínua, e todo desenvolvimento tecnológico tem uma inter-relação acadêmica entre civis e militares, que deve ser a mais democrática e republicana possível, para que toda a sociedade ganhe com isso."