Circula em conjunto com: CORREIO PETROPOLITANO E CORREIO SERRANO

Inteligência Artificial ameaça eleições por todo o mundo

Uso mundial de deepfakes para manipulações avança e áudio é o maior risco

Designed by Freepik

IA generativa foi usada para tentar influenciar a política em ao menos 16 países em 2023, mostra relatório internacional

Por Patrícia Campos Mello (Folhapress)

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

A campanha de Vallas denunciou o vídeo, que foi rapidamente retirado da rede social. Mesmo assim, já era tarde. O deepfake havia sido compartilhado milhares de vezes. Vallas acabou perdendo a eleição para Brandon Johnson --que, justamente, disputava com ele os votos dos eleitores moderados e era um crítico da violência policial.

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

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

Os deepfakes --imagens, áudios ou vídeos criados com a ajuda de modelos de inteligência artificial-- têm se tornado muito 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 à Folha de S.Paulo 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, poucos lugares têm regulação em vigor, as big techs reduziram suas equipes de segurança e os sistemas de detecção não são muito eficientes, em especial para identificar áudios falsos.

Na reta final da eleição parlamentar da Eslováquia, no fim de setembro do ano passado, o líder do partido que estava à frente nas pesquisas foi atropelado por um áudio deepfake.

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

O partido denunciou o áudio, que foi classificado como falso pela agência France Presse. O conteúdo foi rotulado como desinformativo no Facebook, mas não foi removido. O Direção Social-Democracia, partido populista pró-Rússia, derrotou o Progressista e conquistou o maior número de assentos no Parlamento.

Nos EUA, eleitores democratas de New Hampshire receberam ligações automatizadas com uma voz muito parecida com a do presidente Joe Biden instando-os a não participar das primárias do partido 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, porque basta ter 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 consegue replicar tudo de forma muito realista. É muito mais fácil notar manipulações em vídeos ou imagens --como as mãos deformadas e sombras estranhas-- 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 existe um único sistema de detecção, uma bala de prata. É preciso entender as limitações, porque haverá vários resultados conflitantes", diz Ajder.

A regulação do uso de IA em eleições --e de forma geral-- ainda engatinha.

No Brasil, uma minuta de resolução do TSE (Tribunal Superior Eleitoral), que precisa ser aprovada até março, obriga o uso de rótulos informando o uso de inteligência artificial em anúncios políticos e proíbe que a tecnologia seja aplicada para adulterar áudios e vídeos.

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

As empresas estabeleceram regras de uso exigindo a 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 a aplicação das regras.

Na União Europeia, a lei de IA foi aprovada em dezembro e ainda não entrou em vigor. Nos EUA, apenas alguns estados --Minnesota, Michigan, Washington, Califórnia, e Texas-- aprovaram leis regulando 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 inteiramente as big techs por conteúdo deepfake que circular 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, apenas rotular as mídias sintéticas, como propõe o TSE, não será suficiente. "Isso vai ser como enxugar gelo. Colocam o rótulo de mídia manipulada em um anúncio, e logo surge outro", afirma.

Além disso, 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 mergulharam em uma operação de controle de danos e reforçaram suas equipes de "confiança e segurança".

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

Nos EUA, as plataformas estão receosas em 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 deepfakes. 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 Donald Trump, mais uma vez, foi 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", disse Trump, em sua rede social, a Truth Social. Todas as gafes mostradas no anúncio eram públicas e tinham sido amplamente noticiadas.

COMO RECONHECER DEEPFAKES E USO DE IA OU AUTOMAÇÃO NAS ELEIÇÕES

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.

Veja 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 consegue replicar de forma eficiente o barulho da respiração da pessoa ou o som ambiente

Em um vídeo, há discrepâncias sutis entre o movimento dos lábios e o que é dito

Redes de 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 ao se examinar as imagens uma ao lado da outra

Imagens geradas por IA às vezes têm falhas nas mãos, orelhas, lábios, olhos e cabelo. Também podem apresentar diferenças em tom ou textura da pele

Barba, óculos e pintas também 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 entre publicações (automação ou pessoas contratadas)

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

Copa do Mundo de veteranos deve ter Ronaldinho e Kaká

O Brasil vai participar da Copa do Mundo de veteranos, e terá entre seus representantes os campeões mundiais Ronaldinho Gaúcho e Kaká, que conquistaram a taça em 2002.

A Inglaterra sediará o torneio em junho deste ano, em que apenas jogadores com mais de 35 anos poderão participar. As informações são do jornal inglês, DailyMail.

Pelo Brasil, é especulada a participação de Kaká, Ronaldinho Gaúcho e Rivaldo - ex-vencedores do Bola de Ouro, além de Cafu e Roberto Carlos. Cafu, inclusive, é muito celebrado na Inglaterra, onde diversos veículos especializados o inserem na seleção mundial de todos os tempos.

As últimas oito seleções campeãs do mundo irão participar, são elas: Inglaterra, Argentina, Brasil, França, Alemanha, Itália, Espanha e Uruguai.

São elegíveis para o torneio apenas jogadores que tenham atuado por suas seleções nacionais ou disputado mais de 100 jogos nas primeiras divisões de seus respectivos países.

FORMATO DA COMPETIÇÃO

Por conta da idade mais avançada dos selecionados, as partidas terão 70 minutos ao invés de 90 e ocorreram em formato mata-mata. Em caso de empate a disputa vai para os pênaltis.

Serão 18 jogadores "convocados" e não haverá limite de substituições. Cada equipe terá direito a técnico, preparador físico e médico.

O torneio se chamará EPG Cup, pois é organizado pelo Elite Players Group (Grupo de Jogadores de Elite - EPG), grupo formado, no ano passado, por ex-jogadores de futebol e empresários esportivos.

Os capitães das equipes, serão os membros fundadores da organização: Emerson (Brasil), Steve McManaman (Inglaterra), Esteban Cambiasso (Argentina), Christian Karembeu (França), Kevin Kuranyi (Alemanha), Marco Materazzi (Itália), Michel Salgado (Espanha) e Diego Lugano (Uruguai).

O torneio será realizado entre o fim da Liga dos Campeões, em 1º de junho, e o início da Eurocopa 2024, em 14 de junho. A princípio, não foi divulgada tranmissão para o Brasil.