Espaço Aberto ›

Conheça o Espaço Aberto na editoria de Opinião do Estadão. Veja análises e artigos de opinião em colunas escritas por convidados e publicadas pelo Estadão.

Opinião • | Para além da demonização do 'deepfake'

Normas jurídicas e medidas técnicas podem proporcionar certa proteção, mas a população bem informada deve ser a primeira linha de defesa acerca dos riscos do 'deepfake'

Por Rony Vainzof

15/04/2024 | 03h00

A inteligência artificial (IA) é potencializadora da democracia, e não sua detratora, em que pese o grande risco se for empregada para fins ilícitos nas eleições. O assunto precisa e está sendo trabalhado com urgência. Primeiro, é importante lembrar que a IA é muito mais do que *deepfake*. Aliás, mesmo o *deepfake* pode ser utilizado para fins lícitos, se não empregado para a prática de

influência perante o eleitorado. Vejamos, a seguir, alguns casos de *deepfake* para o bem.

No Museu Dalí, na Flórida, o *deepfake* de Salvador Dalí dá as boas-vindas aos visitantes, contando-lhes sobre o artista e a sua arte. Isso permite aos visitantes uma sensação de proximidade, personalização e vínculo com o pintor e as próprias obras. Também é possível tirar uma selfie com o "avatar" de Dalí. Em 2019, David Beckham fez um apelo para acabar com a malária em nove idiomas, numa campanha global por meio do *deepfake* da sua voz. **Um comercial de 55 segundos** da instituição Malaria No More usou a tecnologia para que o jogador famoso se tornasse multilíngue. O seu discurso começa em inglês e, depois, passa para outros oito idiomas com dublagem convincente. É o poder da voz de uma celebridade que pode, com a tecnologia, ser ouvida em diversas línguas.

Já a sincronização labial por meio do *deepfake* está sendo aproveitada para melhorar a acessibilidade do conteúdo para pessoas com problemas de audição. Ao gerar movimentos labiais precisos e sincronizados, a tecnologia contribui para preencher lacunas de comunicação e proporcionar uma experiência mais inclusiva. Imagine a possibilidade de um candidato conseguir melhorar o diálogo com pessoas com deficiências auditivas por meio da melhoria nos movimentos labiais – ou, até mesmo, com um *deepfake* dele mesmo se comunicando na Língua Brasileira de Sinais, a Libras.

Em Xangai, durante o período de confinamento ocasionado pela pandemia de covid-19, um professor utilizou uma versão animada (*anime*) de si mesmo para aumentar a atenção dos alunos nas aulas para ajudá-los a se concentrar melhor. Ainda na área da educação, os *deepfakes* podem animar fotos e filmagens históricas,

beneficiar de figuras históricas para tornar a experiência dos alunos mais atraente e imersiva. Por sua vez, candidatos a eleições, por meio do uso da tecnologia, poderiam responder, de forma personalizada, a dúvidas sobre promessas de campanha mediante o seu respectivo *deepfake*, em vez de um simples texto ou vídeo no site ou nas redes sociais.

Além disso, **só a IA generativa gera 66% a mais de eficiência ao ser humano, em média** (Nilsen Norman) – ou seja, candidatos a prefeitos e vereadores, no Brasil, que não tenham recursos financeiros ou tempo de televisão suficientes poderiam aprimorar campanhas de marketing, peças publicitárias e estratégias de engajamento para mostrar aos eleitores os planos de governo com menor custo e mais eficiência.

Por outro lado, **como já afirmou o atual presidente do Tribunal Superior Eleitoral (TSE)**, ministro Alexandre de Moraes, a IA é uma realidade, um avanço tecnológico, mas que pode ser desvirtuado pelo ser humano. Até se comprovar que aquilo que foi divulgado não é verdade, milhões de pessoas podem ter acesso. Depois, nem todas terão acesso ao desmentido. Mesmo as que tiverem, nem todas acreditarão. Segundo o ministro, ainda, a sanção deve ser drástica: quem se utilizar de IA para manipular a vontade do eleitor para ganhar as eleições, se descoberto for, haverá cassação do registro – e, se eleito, cassação do mandato.

Mas quais são as medidas para mitigar os riscos de quem utiliza a tecnologia para o mal? Primeiro, deve haver transparência, mesmo que contextual, quando candidatos e partidos utilizarem conteúdo sintético para que os eleitores possam compreender que a tecnologia foi empregada. Mais: a inserção de marca d'água (medida técnica) pode facilitar a identificação por algoritmos para eventual remoção do conteúdo gerado por IA que seja

classificar conteúdos como falsos, verdadeiros, enganosos ou descontextualizados. Ainda, por mais que seja complexo, que as redes sociais se comprometam com o TSE para serem mais diligentes no emprego de tecnologia a fim de tentar identificar e remover *deepfakes* ilícitos. Nesse sentido, vale entender a iniciativa do *The Coalition for Content Provenance and Authenticity (C2PA)*, que busca criar padrões para promover autenticidade de conteúdo.

Por fim (e mais importante), criar muita conscientização e informação para a sociedade sobre este novo patamar de *fake news*. Isso significa que a realidade, agora, pode ser distorcida com muita profundidade. Mais do que nunca, precisamos desconfiar e checar tudo antes de acreditar no que estamos vendo. Normas jurídicas e medidas técnicas podem proporcionar certa proteção, mas a população bem informada deve ser a primeira linha de defesa acerca dos riscos do *deepfake*. Educação sobre o tema à sociedade é fundamental, talvez até mais do que demonizar ou proibir o uso de qualquer tecnologia.

*

É CONSULTOR DE PROTEÇÃO A DADOS DA FEDERAÇÃO DO COMÉRCIO DE BENS, SERVIÇOS E TURISMO DO ESTADO DE SÃO PAULO (FECOMERCIOSP)

Opinião por Rony Vainzof

É consultor de Proteção a Dados da Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomercioSP)