As tecnologias de reconhecimento facial

Por **SÉRGIO AMADEU DA SILVEIRA***

Os riscos de efeitos extremamente nocivos para às sociedades.

Existe uma lógica reforçada pela atual supremacia neoliberal de que toda tecnologia inventada deve ser utilizada. Uma variante desse pensamento pode ser encontrada na frase "quando uma tecnologia é de interesse mercantil não há como barrá-la". Entretanto, os fatos indicam outras possibilidades. Muitas tecnologias foram proibidas e outras, depois de um certo período, foram banidas.

Por exemplo, armas químicas são consideradas inaceitáveis e os países democráticos não as utilizam. Diversos pesticidas foram abolidos, como o perigoso DDT. Em 2015, centenas de personalidades, entre elas, Noam Chomsky e Stephen Hawking assinaram uma carta aberta intitulada "*Autonomous Weapons: An Open Letter From AI & Robotics Researchers*" reivindicando o banimento das armas de inteligência artificial. A União Europeia definiu uma moratória à transgenia por mais de cinco anos. Enfim, diversas tecnologias sempre foram reguladas pelas democracias, uma vez que sua fabricação ou uso poderiam trazer riscos e efeitos extremamente nocivos para às sociedades.

Atualmente, cresce uma mobilização mundial pelo banimento das tecnologias de reconhecimento facial. Em 2019, antes da pandemia, aos legisladores de São Francisco, na Califórnia, decidiram proibir a utilização do reconhecimento facial pelas agências locais, incluindo a polícia e as autoridades de transporte. Foi definido também que qualquer tecnologia de vigilância precisa ser aprovada pelos administradores da cidade, não podendo mais ser considerada uma decisão exclusivamente técnica. O motivo é simples. Os benefícios do reconhecimento facial não compensam seus riscos e usos perigosos. Segundo diversos conselheiros da cidade de São Francisco, essa tecnologia tem sido utilizada para fragilizar ainda mais grupos sociais marginalizados.

Segundo a Rede de Observatórios de Segurança, no Brasil, 90% das pessoas presas por reconhecimento facial são negras. A biometria de identificação a partir dos rostos, em geral, utiliza os chamados algoritmos de *deep learning* ou aprendizado profundo, um dos ramos do guarda-chuva das tecnologias de inteligência artificial que dependem de muitos dados para adquirirem qualidade aceitável. Em geral, esses algoritmos são treinados em bancos de dados de fotos para aperfeiçoarem a extração de padrões faciais e sua capacidade de identificarem rostos.

A pesquisadora do MIT-Media Lab, Joy Buolamwini, tem demonstrado que os algoritmos de aprendizagem de máquina podem discriminar com base em classe, raça e gênero. Em um texto assinado com Timnit Gebru, denonimado *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Buolamwini analisou 3 sistemas comerciais de classificação de gênero a partir de um conjunto de fotos. Eles constataram que as mulheres de pele mais escura são o grupo mais mal classificado (com taxas de erro de até 34,7%).

É importante compreender como funciona um sistema algorítmico de reconhecimento facial. Trata-se de um processo automatizado que compara uma imagem captada por uma câmera ou dispositivo de coleta com as imagens armazenadas em um banco de dados. Uma das primeiras missões do algoritmo é conseguir detectar o rosto da pessoa dentro da imagem. Depois da detecção do rosto, ele precisa ser alinhado, colocado virtualmente em determinada posição que facilite a fase seguinte que é a de extração de medidas. O algoritmo, conforme seu treinamento anterior, irá medir a distância entre olhos, entre os olhos e o nariz, a posição da boca, a textura da pele, enfim irá extrair medidas da imagem, irá quantificá-la.

Em seguida, conforme seu modelo, irá comparar a imagem quantificada com cada uma das fotografias digitalizadas e

inseridas em seu banco de dados. Assim, o algoritmo vai emitindo uma pontuação enquanto compara duas imagens, dois rostos, o do seu alvo e o que está armazenado na estrutura de dados. Como procurei aqui mostrar até aqui, os sistemas de reconhecimento são probabilísticos. Eles não podem responder se aquela imagem é ou não é de determinada pessoa. Eles fornecem percentuais de semelhança e diferença.

Alguns sistemas podem oferecer o percentual de confrontação de diversas imagens e oferecer alternativas de rostos para identificar um alvo determinado. O treinamento dos algoritmos é fundamental para sejam capazes de extrair padrões das fotografias, uma vez que devem retirar padrões de imagens em diversas posições. Esse processo necessita de milhares de fotos para a realização do treinamento. Muitas vezes precisam de reforços e etiquetagem realizada por humanos.

A ação dos drones militares que usam sistemas de identificação facial podem nos ajudar a compreender esse problema. O pesquisador Gregory S. McNeal, no texto "*US Practice of Collateral Damage Estimation and Mitigation*", analisou os efeitos colaterais dos ataques realizados por drones. Tais veículos aéreos não tripulados possuem câmeras de alta resolução que permitem identificar alvos. McNeal avaliou os danos colaterais cometidos pelos drones que resultaram em mortes de civis no Iraque e no Afeganistão. Concluiu que 70% deles decorreram de erros na detecção de identidades, ou seja, envolveram a chamada falha na "identificação positiva". Mas o que seria uma identificação positiva em um sistema probabilístico? Semelhanças de 80%? 90%? 98%? Qual o percentual aceitável para considerarmos que uma pessoa procurada foi detectada?

O reconhecimento facial é uma biometria e compõem a categoria dos chamados dados sensíveis. Podem criar estigmas. Precisam ter seus usos analisados a partir do princípio da precaução. Atualmente são utilizados para a identificação das classes perigosas e os segmentos marginalizados. Permitem a perseguição de alvos em tempo real. Os sistemas automatizados de reconhecimento facial reforçam preconceitos e ampliam o racismo estrutural na sociedade, bem como, favorecem o assédio de homossexuais, transexuais e ativistas indesejáveis para a Polícia. São tecnologias de acossamento, de vigilantismo e perseguição.

No Brasil, sou considerado uma pessoa branca. Dada a minha idade e tipo físico, caso um sistema algorítmico da polícia me identificasse erroneamente, a partir das câmeras do bairro de classe média que moro, provavelmente teria uma abordagem mais civilizada. Poderia até ser levado para uma Delegacia de Polícia. Lá o erro do sistema de reconhecimento facial seria detectado e o "falso positivo" seria denunciado.

Todavia, imagine um jovem negro chegando do trabalho no Jardim Ângela ou em Sapopemba e sendo erroneamente identificado pelo sistema de reconhecimento facial como um perigoso criminoso. A depender da unidade Rota que o abordasse talvez não teria nenhuma chance de permanecer vivo. Afirmo que as tecnologias de reconhecimento facial podem contribuir, hoje, para as práticas de extermínio de jovens negros nas periferias. Podem servir para a perseguição política de lideranças dos movimentos sociais, principalmente nas áreas onde as milícias estão justapostas na máquina do Estado.

Além disso, a identificação biométrica é um dispositivo típico dos velhos artifícios da eugenia. São utilizados para identificar imigrantes e segmentos indesejáveis na Europa e Estados Unidos. Na China servem a um autoritarismo inaceitável em uma democracia. Pessoas identificadas pelas câmeras ligadas aos sistemas de reconhecimento facial realizando ações não recomendáveis terão sua pontuação alterada e passarão a ter dificuldades de ter benefícios do Estado.

Sem possibilidade de defesa, sem poder contestar o modelo de probabilidade do reconhecimento, o policiamento ubíquo por meio de câmeras que alimentam os sistemas de reconhecimento facial não são aceitáveis nas democracias. Precisamos impedir a sua ampliação. Na verdade, precisamos bani-los se pretendermos ter coerência mínima com o princípio da precaução. Não podemos utilizar uma tecnologia que utilizam sistemas algorítmicos que são falhos e que ainda não permitem uma adequada explicação. Precisamos banir as tecnologias de reconhecimento facial até que possam ser socialmente não-discriminatórias, auditáveis e mais seguras.

***Sergio Amadeu da Silveira** *é professor da Universidade Federal do ABC. Autor, entre outros livros, de* Software livre – a luta pela liberdade do conhecimento *(Conrad).*