# RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA: O QUE É E POR QUE É UM PROBLEMA?

O avanço tecnológico é muito importante em diversas esferas na vida. Cirurgia com nano robôs, eletricidade, ferramentas de geolocalização para monitoramento de devastação ambiental são exemplos disso. Mas nem toda nova tecnologia é boa (a bomba atômica, por exemplo) ou bem-vinda para ser implementada em algumas áreas da vida.

» **O reconhecimento facial para a segurança pública é um exemplo de uso de tecnologia que tem sido questionado, e inclusive banido, justamente por aqueles que a desenvolveram.**

## QUEM JÁ APERTOU O PAUSE NO USO DO RECONHECIMENTO FACIAL PARA FINS DE VIGILÂNCIA?

» **A cidade de São Francisco/EUA (Vale do Silício) reconhecida por ser um pólo de inovação tecnológica no mundo, baniu o uso do reconhecimento facial pela polícia e outras agências públicas[1].**

Além de São Francisco, nos EUA, pelo menos Minneapolis, Boston[2], Cambridge (onde ficam Harvard e o MIT, outro pólo de desenvolvimento desta tecnologia), Portland, Berkeley, Oakland e Summerville também baniram o reconhecimento facial pra fins de vigilância[3]. Na Europa, em outubro de 2021, o Parlamento Europeu também votou a favor do banimento dessa tecnologia[4] para fins de policiamento, após manifestação pró banimento da Autoridade Europeia para a Proteção de Dados (AEPD)[5]. E pouco a pouco estão extendendo tais proibições

1 https://epocanegocios.globo.com/Tecnologia/noticia/2019/05/centro-da-revolucao-tecnologica-sao-francisco-bane-o-uso-de-reconhecimento-facial-pelo-governo.html

2 https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban/

3 https://www.aclu.org/news/topic/stopping-face-recognition-surveillance

4 https://www.insideprivacy.com/artificial-intelligence/european-parliament-votes-in-favor-of-banning-the-use-of-facial-recognition-in-law-enforcement/

5 https://www.istoedinheiro.com.br/reconhecimento-facial-deve-ser/

para escolas, como é o caso da França, onde a CNIL (Comissão Nacional de Informática e Liberdades) proibiu que um colégio de Nice e outro de Marselha usassem reconhecimento facial para controlar o acesso dos alunos aos estabelecimentos[6] e da Suécia, onde o reconhecimento foi banido nas escolas[7].

» **Para além do Poder Público, em 2020, grandes empresas como IBM, Microsoft e Amazon declararam que não venderiam mais essa tecnologia para fins de policiamento[8].**

Porque então vamos utilizar uma tecnologia cujos determinados usos são rejeitados por seus próprios desenvolvedores? Você usaria um remédio que o criador não usa por medo das consequências?

## E NO BRASIL? COMO ANDA A IMPLEMENTAÇÃO DO RECONHECIMENTO FACIAL PARA SEGURANÇA PÚBLICA?

Por aqui estamos andando contra a corrente. Enquanto países que desenvolveram essa tecnologia estão restringindo seu uso, a partir de 2019 houve uma expansão da implementação dessa tecnologia, hoje presente em ao menos 20 estados das cinco regiões do país, mesmo que preocupações relacionadas à defesa da privacidade e ao **potencial discriminatório** da tecnologia tenham sido levantadas por diversos especialistas.

## COMO FUNCIONA ESSA TECNOLOGIA?

A tecnologia do reconhecimento facial se utiliza de imagens do rosto para identificar métricas específicas da pessoa, como a distância entre os olhos, largura do queixo e o comprimento da boca. Com essas informações (dados biométricos), é calculada uma espécie de assinatura facial. Mais tarde, essa "assinatura" é comparada com outras já armazenadas em um banco de dados e, quando as assinaturas faciais são compatíveis, se dá o reconhecimento de

6 https://iapp.org/news/a/cnil-bans-high-school-facial-recognition-programs/

7 https://www.neweurope.eu/article/sweden-bans-facial-recognition-technology-in-schools/

8 https://www.forbes.com/sites/larrymagid/2020/06/12/ibm-microsoft-and-amazon-not-letting-police-use-their-facial-recognition-technology/?sh=903928518871

alguém de forma automatizada.

## E ONDE MORA O PERIGO?

### Uma tecnologia falha e imprecisa que automatiza desigualdades.

No processo de identificação das métricas faciais da pessoa, os algoritmos podem cometer erros devido a expressões faciais, rosto mal iluminado, envelhecimento, entre outros. Além disso, boa parte desses algoritmos foram treinados a reconhecer rostos a partir de bancos de dados em que não há pessoas racializadas, e nem mesmo mulheres, ou pessoas trans, de maneira representativa, resultando em maior dificuldade para algoritmo criar uma assinatura facial acurada para essas populações. Em estudo que marcou o campo[9], a pesquisadora do MIT, Joy Buolamwini, e a cientista de dados Timnit Gebru, se dedicaram a apontar viéses de gênero e raça em diferentes sistemas de reconhecimento facial. Avaliaram os sistemas da Microsoft, Facebook e IBM, tendo em vista que alguns deles eram vendidos para governos.

» **E os resultados foram: esses sistemas dão respostas de forma acurada quando os sujeitos são homens brancos, mas a proporção de acertos cai no caso de homens negros e é menor ainda no caso de mulheres negras.**

Ou seja, mulheres negras ficam mais sujeitas a falsos positivos. Na análise de erro da Microsoft, por exemplo, demonstrou-se que 93,6% das imagens que tiveram o gênero equivocado eram de rostos negros.

Outra pesquisa mais recente, feita por uma das maiores empresas de reconhecimento facial, a francesa Idemia, também afirmou que a tecnologia possuía maior probabilidade de identificar de forma incorreta mulheres negras em relação às mulheres brancas ou homens brancos em relação a homens negros.

» **Entre mulheres brancas a taxa de erro foi de 1 para cada 10 mil, no de mulheres negras, a taxa foi de 1 para 1 mil, ou seja, 10 vezes mais chance de erro. Os sistemas presentes no mercado possuem uma precisão que varia entre 75,8%**

9 http://gendershades.org/

**e 87,5% quando aplicadas em população racializada, o que tem resultados em diversos erros com consequências graves.**

» **A American Civil Liberties Union chegou a realizar um teste com o Rekognition, tecnologia da Amazon, que identificou de maneira equivocada 28 membros do congresso norte americano como sendo de perfis de uma base de dados de encarcerados[10]. A maioria dos casos de falso positivo foi de congressistas negros.**

Na prática, aqui no Brasil, já temos casos em que essa grande margem de erro, principalmente para a população negra, resultou em restrição de direitos, como aconteceu no Rio de Janeiro, quando uma mulher foi detida no segundo dia de uso dessa tecnologia[11].

Essa tecnologia também é visivelmente **discriminatória** quando falamos de pessoas trans ou não binárias, já que os sistemas de reconhecimento facial são treinados em uma visão binária de gênero com determinadas marcações normativas do que representa cada gênero, como mostra a pesquisa realizada pela Coding Rights[12]. Assim, não só no campo da segurança pública, na assistência social, o uso da tecnologia de reconhecimento facial pode ser o responsável pela suspensão de benefícios lícitos e a abertura de processos contra pessoas titulares legítimas de benefícios sociais.

» **Por exemplo, devido ao "equívoco do sistema" uma jovem trans foi impedida de usar a sua gratuidade no transporte público no Distrito Federal.**

Se um sistema é implementado com uma falsa crença de neutralidade tecnológica, mas erra ao identificar certas identidades, torna-se mais complexo provar que o erro é do sistema. Cidadãos ficam mais propensos a situações de abuso policial. Como você provaria que você não é alguém procurado se uma máquina disse que é você?

10 https://www.theguardian.com/technology/2018/jul/26/amazon-facial-rekognition-congress-mugshots-aclu

11 https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913

12 https://medium.com/codingrights/tecnologias-de-reconhecimento-facial-na-verifica%C3%A7%C3%A3o-de-identidades-trans-7d3ac3f49b92

## Vigilância Massiva vs Proteção de Dados e Privacidade

Já que as câmeras que detêm esta tecnologia estão espalhadas pelas ruas, muitas vezes, a captura dos dados biométricos para o reconhecimento facial (e o posterior armazenamento) **é obtida sem consentimento,** diferente de quando você cede sua identificação por digital, uma ação realizada conscientemente.

» **Um exemplo disso foi o caso do Metrô (ViaQuatro) de São Paulo[13] que foi condenado a pagar 100 mil reais quando comprovado que houve captação da imagem de usuários do transporte público sem consentimento, e pior, para fins comerciais.**

Além disso, para que essa tecnologia funcione para fins de segurança pública, seria necessário filmar todos que passam pela câmera, **num experimento de vigilância massiva**, contrário ao princípio da presunção de inocência. O uso da tecnologia de RF significa na prática a violação de Direitos Fundamentais, como: a privacidade, a liberdade de ir e vir, a inviolabilidade da honra e da imagem das pessoas, já que captura dados sensíveis das pessoas quando essas estão em espaço público.

» **Para além disso há o risco de eventuais vazamentos de dados sensíveis, como são os dados biométricos, além de irreversíveis, nos deixam muito mais expostos a fraudes[14].**

Por exemplo, como provar que alguém usou sua cara (no caso, seus dados biométricos do rosto) para alguma transação, mas que esse alguém não era você? Como evitar outros usos desses dados, se não temos como trocar nossa biometria da maneira trocamos uma senha?

Por fim, há de se lembrar da importância em resguardar a privacidade de crianças e adolescentes. Se para um passeio escolar precisamos de autorização dos responsáveis para que o menor de idade participe, porque devemos normalizar a captura e o tratamento de seus dados biométricos? Pela impossibilidade

13 https://idec.org.br/idec-na-imprensa/viaquatro-e-condenada-por-reconhecimento-facial-sem-autorizacao-no-metro-de-sp

14 https://www.wsj.com/articles/faces-are-the-next-target-for-fraudsters-11625662828?page=1

de sistemas de tecnologias de reconhecimento facial serem utilizados em espaços públicos sem coletar dados de menores e incapazes, eles representam uma ameaça aos direitos de indivíduos dessa faixa etária.

## O CUSTO-BENEFÍCIO NÃO COMPENSARIA AS EVENTUAIS FALHAS?

Pode-se argumentar que toda tecnologia é passível de erro, o problema é que os erros gerados pela tecnologia de reconhecimento facial na segurança pública são imensuráveis para a vida de um indivíduo. Pesquisa feita pela Defensoria Pública mostra que 80% dos réus absolvidos por erros em reconhecimento fotográfico no RJ ficaram mais de 1 ano presos[15].

» ***Um match pode significar o fim da liberdade de um indivíduo, em um país em que os erros judiciais são latentes.*** **Isso em um país que já tem índices assombrosos de encarceramento de inocentes, em sua maioria negros e pobre.**

Além disso, vale lembrar que nossos gestores públicos quase sempre trabalham com orçamentos apertadíssimos, o que não explicaria o alto investimento em uma tecnologia falha.

» **Em Detroit, nos Estados Unidos, o chefe de polícia da cidade, afirmou que o sistema de reconhecimento facial DataWorks Plus, que custou à cidade US$1 milhão de dólares, tem uma taxa de erro de aproximadamente 96%[16].**

Aqui no Brasil, o estado do Rio de Janeiro pretende gastar quase meio milhão de reais instalando câmeras na favela do Jacarezinho enquanto esse dinheiro faz falta em áreas como saúde e educação[17], ou até mesmo em formação e orientação de forças de segurança pública.

15 https://g1.globo.com/rj/rio-de-janeiro/noticia/2022/05/05/80percent-dos-reus-absolvidos-por-erros-em-reconhecimento-fotografico-no-rj-ficaram-mais-de-1-ano-presos-diz-estudo-da-defensoria-publica.ghtml

16 https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time

17 https://opanoptico.com.br/Caso/um-rio-de-cameras-com-olhos-seletivos-uso-do-reconhecimento-facial-pela-policia-fluminense/

# RECONHECIMENTO FACIAL DEVE SER BANIDO. VEJA DEZ RAZÕES:

» Reconhecimento facial e visão computacional são técnicas altamente imprecisas, em especial sobre pessoas racializadas.

» A imprecisão da tecnologia e infrações de direitos humanos são mais intensas para pessoas trans.

» A seletividade penal é norma nas polícias e judiciário brasileiros.

» Tecnologias digitais vistas como “neutras” ou “objetivas” favorecem ainda mais excessos de policiais.

» O mercado de inteligência artificial esconde o funcionamento de seus sistemas usando a defesa por “segredo de negócio” ou “inexplicabilidade algorítmica”.

» Tecnologias biométricas no espaço público pressupõem e fortalecem uma sociedade vigilantista.

» Não podemos pressupor boa-fé de corporações de tecnologia.

» Vazamentos de dados vitimam empresas de tecnologias de todos os portes.

» A infraestrutura de vigilância aumenta o potencial violento de projetos autoritários.

» O custo-benefício para captura de condenados não justifica a vigilância massiva.

Esse material foi produzido por Centro de Estudos de Segurança e Cidadania | CESeC, Coding Rights, Instituto Brasileiro de Defesa do Consumidor | IDEC e MediaLab UFRJ