Riscos decorrentes do reconhecimento facial em espaços públicos

Nos idos de 2002, Steven Spielberg estourava as bilheterias mundiais com o distópico filme *Minority Report*, que se passa em uma fantasiosa Washington de 2054. Nela, os delitos seriam evitados por atuação de uma "*divisão pré-crime"*, setor policial incumbido de punir o culpado antes mesmo de ele cometer o ilícito, medida que erradicou a taxa de homicídios. O sistema, considerado infalível, é baseado em previsões de três *"pre-cogs"*, seres mutantes capazes de prever o futuro. Tamanha perfeição é colocada em xeque por um de seus principais agentes, John Anderton (Tom Cruise), quando os *"pre-*

r um homem que ele sequer conhece.

Anos depois, a realidade copia a ficção, em ao menos dois aspectos: a vontade de se prevenir crimes, a qualquer custo, e a fé cega em sistemas considerados à prova de falhas, mas que na prática estão longe dessa excelência técnica. Iniciativas de combate ao crime — seja prevenção ou repressão — com uso de tecnologias inovadoras estão se tornando cada vez mais comuns. Por trás delas, os órgãos de segurança nutrem discursos que exaltam a eficiência e neutralidade de sistemas tecnológicos, como se fossem o único e melhor caminho no enfrentamento a ilegalidades.

Esquecem-se, contudo, de que tecnologias não se desenvolvem sozinhas. Elas, na verdade, carregam vieses do contexto de seu desenvolvimento: uma sociedade que discrimina vai gerar tecnologias discriminatórias. Esquece-se também que elas não nascem prontas e blindadas contra erros.

Além disso, riscos de violações de direitos fundamentais próprios do sistema de justiça criminal ganham outra escala quando da utilização de tecnologias. Por exemplo: uma coisa é ter policiais com vieses racistas que abordam pessoas negras sem justificativa para tanto. Outra é ter um sistema de tecnologia monitorando toda a população de um determinado lugar — podendo chegar a milhões de pessoas — com viés racista. Ambos os casos são gravíssimos, mas o último deles, em razão da escala, pode gerar consequências ainda maiores, pela prática ininterrupta e número altíssimo de pessoas atingidas. É dizer que a tecnologia pode ser um instrumento de perpetuação e disseminação do racismo praticado cotidianamente pelas polícias no Brasil.

Talvez o exemplo recente mais paradigmático disso seja a utilização, nos Estados Unidos, do Compas (*Correctional Offender Management Profiling for Alternative Sanctions*), um software desenvolvido para, supostamente, avaliar o risco de um indivíduo reincidir em práticas criminosas. Um exercício de futurologia digno de *Spielberg*, realizado com base em informações de questionários sobre a pessoa avaliada, que levam em conta diferentes informações sobre a vida de um indivíduo [1]. Com esses dados, o programa "decide" se a pessoa pode ou não ser solta, se deve pagar fiança, ou se está apta a receber liberdade condicional.

O uso do Compas levantou muitas polêmicas. Vale ressaltar três delas: a sua inefetividade (uma pesquisa do Dartmouth College concluiu que leigos acertam mais em suas previsões sobre reincidência do que o próprio software) [2]; a sua falta de transparência (ninguém sabe ao certo como o software chega às suas conclusões); e, por fim, o seu viés discriminatório, questão inclusive já sinalizada pela Suprema Corte de Wisconsin e por diversos grupos antirracismo [3].

No Brasil, outras formas de usos de tecnologias na área da segurança pública vêm sendo debatidas. A título de exemplo, atualmente encontra-se em debate o Projeto Smart Sampa, cujo edital foi publicado em 5 dezembro de 2022, prevendo a instalação de 20 mil câmeras de reconhecimento facial e policiamento preventivo pela capital paulista. O objetivo seria tanto o de identificar foragidos da justiça, por meio de cruzamento da imagem com bancos de dados de órgãos públicos, quanto identificar situações consideradas suspeitas. Curiosamente (ou não), o texto original trazia critérios de análise como "vadiagem" e "cor", expressões posteriormente substituídas por "estrutura corporal".

O projeto foi altamente questionado por diferentes entidades da sociedade civil e encontra-se atualmente suspenso, aguardando decisão do Tribunal de Contas do Município de São Paulo [4]. As críticas apresentadas ao projeto encontram ressonância naquelas feitas no âmbito da utilização do Compas e traduzem uma preocupação crescente com o aumento do vigilantismo estatal em democracias consolidadas.

Para iniciar o debate sem incorrer no risco de generalização, listamos abaixo os principais pontos de atenção de uma tecnologia específica: o uso de reconhecimento facial para identificação de suspeitos e foragidos.

Pesquisas ao redor do mundo têm mostrado que essas tecnologias erram e, como consequência disso, pessoas são presas ilegalmente [5]. Esse percentual de eficácia tende a diminuir nos casos de mulheres, negros e transexuais, gerando distorções discriminatórias. Na prática, com o uso dessas ferramentas, torna-se mais provável que haja falha na identificação de uma mulher negra do que de um homem branco.

Um levantamento da Rede de Observatórios de Segurança, realizado entre março e outubro de 2019, monitorou as experiências iniciais de cinco estados brasileiros com tecnologias de reconhecimento facial mediante câmeras de segurança: Bahia, Rio de Janeiro, Santa Catarina, Paraíba e Ceará e identificou que 90,5% dos presos por monitoramento facial no Brasil eram negros [6]. A tecnologia, aqui, definitivamente não é neutra.

Outro argumento vem sob o viés da privacidade e proteção de dados. A biometria facial (dado pessoal coletado pelas tecnologias de reconhecimento) é considerado por diversas legislações — incluindo a brasileira — como um dado sensível e merecedor de proteção especial. As iniciativas de uso de câmeras de reconhecimento facial por órgãos de segurança pública implicariam na coleta em massa e indiscriminada de dados sensíveis da população como um todo, o que seria desproporcional pensando nos resultados práticos da medida.

Além disso, tais tecnologias falham sistematicamente quando o assunto é transparência, auditabilidade e responsabilidade dos agentes — Estado e provedor da tecnologia — perante as pessoas que têm seus dados tratados. O modo de funcionamento dessas ferramentas costuma ser uma caixa-preta, o que impede sua sujeição ao escrutínio público e a defesa daquele que fora identificado e relacionado a um crime.

Por fim, sob um viés garantista penal, o uso de câmeras de reconhecimento facial no espaço público é tratar todo mundo como um potencial criminoso, através da checagem ininterrupta de identidade. É algo diferente das tradicionais câmeras de segurança, que gravam imagens que normalmente só são verificadas após algum acontecimento. Nessa nova realidade, a presunção de inocência é posta à prova.

O uso de câmeras de reconhecimento facial também levanta o debate sobre o vigilantismo e o controle do Estado. Se, há algumas décadas, um governo que controlava os passos de seus cidadãos era visto como algo totalitário, agora essa possibilidade está nas mãos de Estados que se pretendem democráticos.

Diante desse cenário, diferentes países não têm poupado esforços para regular o uso dessas tecnologias. Olhando para o cenário global, podemos identificar três maneiras de lidar com isso em termos de regulamentação.

A primeira delas visa proibir o uso de reconhecimento facial para fins de segurança pública. A segunda maneira por meio de uma moratória, em que o projeto de uso da tecnologia é restringido e/ou suspenso até o atendimento de condições variáveis. Por fim, seria ainda possível uma regulamentação com abordagem baseada em riscos, com o objetivo de minimizar impactos negativos em liberdades individuais causados pelo uso da tecnologia. As regras dessa última abordagem podem incluir a obediência expressa a princípios, a necessidade de relatórios de impacto, medidas de responsabilização, exigências de ordem judicial, etc.

No Brasil, o debate regulatório em torno do uso de reconhecimento facial para fins de segurança pública vem ganhando fôlego. A título de exemplo, em 2022, por iniciativa de 50 parlamentares com o apoio de organizações da sociedade civil, foram introduzidos projetos de lei para proibir o reconhecimento facial para fins de segurança pública (iniciativa conhecida como Tire Meu Rosto da Sua Mira) [7].

Em suma, o desejo de utilização de tecnologias inovadoras no combate ao crime é comum a diversos gestores públicos, que sonham com soluções dignas de filmes de ficção científica. Contudo, os riscos a direitos fundamentais e liberdades individuais não podem ser ignorados. Principalmente no contexto da justiça criminal e segurança pública, cada projeto e iniciativa exige uma análise crítica de seus riscos e de sua falibilidade, para que não leve à perda indevida da liberdade — seja por monitoramento abusivo, seja por prisões ilegais. Na vida real, não há soluções fáceis, futurologia ou efeitos especiais.

[1] São considerados: antecedentes criminais, o uso ou não de drogas, problemas financeiros, o envolvimento familiar em crimes, o local de residência (e sua estabilidade), o histórico de violência, além de dados absolutamente vagos, como *criminal thinking* (pensamentos criminosos) e *criminal personality* (algo que nos lembra a genérica expressão, muito utilizada no Brasil, personalidade voltada para o crime) A tabela de itens do software está disponível no guia Practitioner's Guide to Compas Core, p. 27. Confira-se em: https://s3.documentcloud.org/documents/2840784/Practitioner-s-Guide-to-COMPAS-Core.pdf.

[2] Pesquisa disponível em: https://home.dartmouth.edu/news/2018/01/court-software-may-be-no-more-accurate-web-survey-takers-predicting-criminal-risk

[3] Ver: https://www.bbc.com/portuguese/brasil-37677421; https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[4] Diversas organizações da sociedade civil protocolaram no Ministério Público do Estado uma representação contra o edital da Prefeitura de São Paulo e, em janeiro deste ano, foi instaurado inquérito civil para apurar o risco de violações aos direitos humanos causado pelo Projeto. O Município de São Paulo terá que informar ao MP, por exemplo, "quais bancos de dados serão utilizados para a realização do reconhecimento facial". Ver em: https://g1.globo.com/sp/sao-paulo/noticia/2022/11/30/idec-e-mais-de-50-organizacoes-acionam-mp-contra-edital-da-prefeitura-de-sp-que-quer-contratar-sistema-de-monitoramento-facial.ghtml

[5] A título de exemplo: https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

[6] Disponível em: http://observatorioseguranca.com.br/novas-tecnologias-para-os-suspeitos-de-sempre/.

[7] Ver em: https://tiremeurostodasuamira.org.br/carta-aberta/