KONRAD ADENAUER STIFTUNG

TECNOLOGIA, SEGURANÇA E DIREITOS

Os usos e riscos de sistemas de reconhecimento facial no Brasil

Org. Daniel Edler Duarte
Eleonora Mesquita Ceia

Tecnologia, Segurança e Direitos

Os usos e riscos de sistemas de reconhecimento facial no Brasil

KONRAD ADENAUER STIFTUNG

Editora responsável
Susanne Käss

Organização
Daniel Edler Duarte
Eleonora Mesquita Ceia

Coordenação Editorial
Luiz Gustavo Carlos
Reinaldo J. Themoteo

Revisão
Daniel Edler Duarte

Design gráfico e diagramação
Claudia Mendes

Dados Internacionais para Catalogação na Publicação (CIP)
Lumos Assessoria Editorial – Bibliotecária Priscila Pena Machado CRB-7/6971

T255 Tecnologia, Segurança e Direitos: Os usos e riscos de sistemas de reconhecimento facial no Brasil / organização Daniel Edler Duarte e Eleonora Mesquita Ceia. — Rio de Janeiro : Konrad Adenauer Stiftung, 2022. Dados eletrônicos (pdf).

Inclui bibliografia.
ISBN 978-65-89432-29-6

1. Tecnologia da informação - Aspectos sociais. 2. Vigilância eletrônica. 3. Sistemas de segurança. 4. Privacidade, Direito de. 5. Reconhecimento facial. 6. Inteligência computacional. 7. Proteção de dados. I. Duarte, Daniel Edler. II. Ceia, Eleonora Mesquita. III. Título.

CDD 006.42

FUNDAÇÃO KONRAD ADENAUER
Representação no Brasil: Rua Guilhermina Guinle, 163 · Botafogo
Rio de Janeiro · RJ · 22270-060
Tel.: 0055-21-2220-5441 · Telefax: 0055-21-2220-5448
adenauer-brasil@kas.de · www.kas.de/brasil

Sumário

Agradecimentos

A publicação deste livro se deve ao trabalho e apoio de muita gente e cabe aqui agradecer a todos que participaram desse projeto.

Começamos a planejar a publicação ainda em 2021, quando percebemos a demanda por um livro que reunisse a reflexão sobre usos e regulações de tecnologias de reconhecimento facial no Brasil. A disseminação de câmeras nos centros urbanos e em zonas rurais estava a todo vapor, mas as pesquisas ainda se encontravam compartimentalizadas nos campos do direito, da sociologia digital e dos estudos de vigilância. Com exceção das mobilizações coletivas promovidas por instituições da sociedade civil, havia pouco diálogo entre os muitos autores e autoras que se debruçavam sobre o tema.

Ao longo de meses, fizemos diversas reuniões para mapear as principais controvérsias em torno da vigilância biométrica. Enquanto profissionais de segurança pública se mostravam preocupados com a insegurança jurídica de suas inovações e defendiam formas de regulação que equilibrassem os riscos de abusos com os ganhos para a investigação criminal e o policiamento ostensivo, pesquisadores e movimentos sociais alertavam para os efeitos deletérios dos vieses algorítmicos e da expansão do "vigilantismo". O livro que os leitores e leitoras têm agora em mãos foi pensado como uma resposta a essas preocupações.

Agradecemos, portanto, a todos que tomaram um tempo para compartilhar conosco sua experiência no tema. Em especial, agradecemos aos autores e autoras que aceitaram colocar no papel suas reflexões e to-

param o desafio de traduzir o conhecimento de seus respectivos campos para uma audiência mais ampla.

Este livro é também fruto do trabalho de pesquisa que temos desenvolvido em nossas instituições. Nos últimos anos, contamos com o apoio da FAPESP, do Núcleo de Estudos da Violência (NEV/USP) e do Ibmec-RJ. Cabe aqui ressaltar a importância dos mecanismos públicos e privados de financiamento à pesquisa, sem os quais não teríamos como investir nessa empreitada.

Por fim, agradecemos à Fundação Konrad Adenauer (KAS) pela iniciativa de editar e financiar este livro. Nossos agradecimentos especiais à então representante da KAS no Brasil, Anja Czymmeck, por toda cordialidade e seriedade na condução das importantes atividades da fundação. Para a publicação deste livro, contamos com a valiosa colaboração de Luiz Gustavo Carlos, Coordenador de Projetos de Democracia e Estado de Direito, e de Reinaldo Themoteo, Coordenador Editorial. O trabalho e atenção dedicados por ambos foi fundamental para que o projeto se concretizasse.

Ao longo de nossas carreiras, a Fundação Konrad Adenauer tem sido uma parceira fundamental, dando suporte para nossa formação profissional e acadêmica. E não foi diferente quando apresentamos a ideia do livro. Muito obrigado!

Daniel Edler Duarte
Eleonora Mesquita Ceia

Lista de autores

Chiara Spadaccini de Teffé é Doutora e mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (uerj), tendo sido aprovada com distinção, louvor e recomendação para publicação. Graduada em Direito pela Universidade Federal do Rio de Janeiro (ufrj). Atualmente, é coordenadora de pesquisa e publicações da pós-graduação em Direito Digital do Instituto de Tecnologia e Sociedade do Rio (its Rio), em parceria com a uerj, e professora de Direito Civil e Direito Digital na faculdade de Direito do ibmec. Leciona em cursos específicos de pós-graduação e extensão do ceped-uerj, da puc-Rio, da emerj e do its Rio. Membro da Comissão de Proteção de Dados e Privacidade da oabrj. Membro da Comissão de Direito Civil do Conselho Seccional do Rio de Janeiro da oab (2022/2024). Membro do Fórum Permanente de Liberdade de Expressão, Liberdades Fundamentais e Democracia da emerj. Membro do Fórum permanente de inovações tecnológicas no Direito da emerj. Foi professora substituta de Direito Civil na ufrj. Associada ao Instituto Brasileiro de Estudos em Responsabilidade Civil (iberc). Atua como advogada em áreas do Direito Civil e do Direito Digital e como consultora em proteção de dados pessoais. Autora do livro *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*.

Cynthia Picolo Gonzaga de Azevedo é advogada, bacharela em Direito pela puc-Campinas e ll.M. em Direito Internacional Público pela Universidade de Leiden (Holanda). Especialista em Privacidade e Proteção de Dados e Inteligência Artificial (dpbr; Academy of European

Law; Vrije University Amsterdam). Atualmente, é diretora-presidente do Laboratório de Políticas Públicas e Internet (LAPIN), sendo responsável pelas áreas de pesquisa e políticas públicas nos eixos Governança de Dados, Desinformação, Inteligência Artificial e Vigilância.

Bárbara Simão é coordenadora da área de privacidade e vigilância no InternetLab. É mestre em direito e desenvolvimento pela Fundação Getúlio Vargas (FGV Direito SP). Graduada pela Faculdade de Direito da Universidade de São Paulo (FDUSP). Atuou como pesquisadora na área de direitos digitais do Instituto Brasileiro de Defesa do Consumidor (Idec).

Bianca Kremer é doutora em Direito pela PUC-Rio com período de pesquisadora visitante na universidade de Leiden – Holanda (bolsista Coimbra Group). É professora de graduação e pós-graduação em direito digital no IDP Brasília, e coordenadora de pesquisa no projeto IDP Privacy Lab: painel LGPD nos Tribunais. Professora visitante no Centro de Tecnologia e Sociedade da FGV Direito Rio (CTS – FGV). Atua nas áreas de direito digital, teoria do direito privado, pensamento afrodiaspórico e decolonialidade.

Daniel Edler Duarte é pesquisador de pós-doutorado FAPESP no Departamento de Sociologia da Universidade de São Paulo (FFLCH/USP) e no Núcleo de Estudos da Violência (NEV/USP). Anteriormente, foi pesquisador CAPES/Pró-Defesa na Escola de Guerra Naval (EGN). Completou o PhD em *Politics and International Studies* no *Department of War Studies*, King's College London (KCL). Daniel também foi professor e pesquisador assistente no Centro de Relações Internacionais da Fundação Getulio Vargas (CPDOC/FGV). Sua pesquisa atual aborda a produção e o uso de novas tecnologias de segurança, com foco na implementação de dispositivos de vigilância biométrica e no desenvolvimento de sistemas de policiamento preditivo.

Eleonora Mesquita Ceia é Doutora em Direito pela Faculdade de Economia e Ciências Jurídicas da Universidade de Saarland. É Professora Adjunta da Faculdade Nacional de Direito da Universidade Federal do Rio de Janeiro (UFRJ) e Professora do Curso de Graduação em Direito do Centro Universitário Ibmec-RJ. Sua pesquisa atual envolve o estudo crítico da forma federativa de Estado frente aos desafios postos por crises globais, com ênfase na Federação brasileira e seu viés cooperativo e municipalista.

Fernanda dos Santos Rodrigues Silva é doutoranda em Direito, Tecnociências e Interdisciplinaridade na Universidade Federal de Minas Gerais (UFMG). Possui Mestrado em Direitos na Sociedade em Rede, pela Universidade Federal de Santa Maria (UFSM), onde também obteve a sua graduação em Direito. Desenvolve pesquisas na área de direito e novas tecnologias, com foco em moderação de conteúdo, inteligência artificial e racismo algorítmico

Horrara Moreira é bacharela em direito pela Universidade Federal do Estado do Rio de Janeiro (UNIRIO). Membra do coletivo AqualtuneLab, consultora da Campanha Tire Meu Rosto da Sua Mira e Analista de Comunicação e Articuladora Social no projeto Defendendo o Brasil do Tecnoautoritarismo da Associação Data Privacy Brasil de Pesquisa. Possui capacitação em Privacidade e Proteção de Dados pelo Data Privacy Brasil e PUC-Rio, Mobilização e Engajamento pela Megafone Ativismo, *Human Centered Design* pela Acumen Academy e Ideo.org e em Práticas Colaborativas pelo Instituto Brasileiro de Práticas Colaborativas. Atua como educadora popular em direitos humanos desde 2015.

Pablo Nunes é doutor em Ciência Política pelo Instituto de Estudos Sociais e Políticos da Universidade do Estado do Rio de Janeiro (IESP-Uerj). É um dos coordenadores do Centro de Estudos de Segurança e

Cidadania (CESeC) onde desenvolve pesquisas na área de novas tecnologias na segurança pública, produção e análise de dados e avaliação de políticas públicas.

Rafaela Cavalcanti de Alcântara é bacharela em Direito pela Universidade Federal de Pernambuco (UFPE), com mestrado em Direitos Humanos pela Universidade Federal da Paraíba (UFPB). No mestrado, desenvolveu pesquisa de inspiração etnográfica, com foco em direito à moradia e à cidade. Atuou na equipe de Direitos Digitais da ARTIGO 19 Brasil e América Latina de 2019 a 2022, contexto no qual se somou à construção da Campanha #TireMeuRostoDaSuaMira. Como pesquisadora, vem analisando a relação entre tecnologia, vigilância, direito à cidade e gênero.

Raquel Rachid é doutoranda em Mudança Social e Participação Política pela EACH-USP; mestra em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie, bem como bacharela em Direito pela mesma universidade, com mobilidade pela Peking University (China); bacharela em História pela FFLCH-USP. Advogada, atualmente é pesquisadora do Laboratório de Políticas Públicas e Internet – LAPIN, do projeto "Impactos das Tecnologias Digitais nos Sistemas de Saúde" (ligado à Iniciativa Saúde Amanhã/Estratégia Fiocruz para a Agenda 2030) e do grupo de pesquisa "Crítica do Direito e Subjetividade Jurídica" (FADUSP).

Rodrigo Brandão é formado pela Universidade de São Paulo (USP), com bacharelado em Ciências Sociais (2008), especialização em Economia (2010) e mestrado em Ciência Política (2011). Desde 2020, é doutorando em Sociologia na mesma instituição, coordenador do Observatório da Inovação e Competitividade (pertencente ao Instituto de Estudos Avançados da USP) e pesquisador-bolsista do C4AI – *Center for Artificial Intelligence*. Anteriormente, atuou, entre outras organiza-

ções, na Fundação Fernando Henrique Cardoso, como coordenador -assistente da área de estudos e debates, e na Companhia Siderúrgica Nacional, como especialista em relações institucionais.

Sérgio Branco é cofundador e diretor do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Professor do Ibmec. Professor convidado da Universidade de Montreal. Autor dos livros «Memória e Esquecimento na Internet», "Direitos Autorais na Internet e o Uso de Obras Alheias", "O Domínio Público no Direito Autoral Brasileiro – Uma Obra em Domínio Público" e "O que é *Creative Commons* – Novos Modelos de Direito Autoral em um Mundo Mais Criativo". Especialista em propriedade intelectual pela Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio. Pós-graduado em cinema documentário pela FGV. Graduado em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Sócio de Rennó Penteado Sampaio Advogados.

Introdução

Daniel Edler Duarte
Eleonora Mesquita Ceia

Vivemos tempos de euforia e incerteza sobre os impactos de novas tecnologias digitais. Por um lado, desenvolvimentos recentes no campo da inteligência artificial (IA) produzem grandes transformações na indústria e no Estado, garantindo saltos de produtividade, maior eficiência na prestação de serviços e ganhos sensíveis nas áreas da saúde, educação e segurança (FRY, 2018; SMITH & BROWNE, 2020). Por outro, nossa integração com dispositivos de *internet das coisas* (IoT) (LUPTON, 2016), a implementação de projetos de "cidades inteligentes" (KITCHIN et al., 2017) e a consolidação de uma nova era do "capitalismo de vigilância" (ZUBOFF, 2021), em que dados pessoais alimentam sistemas algorítmicos que definem dietas de informação e mecanismos de manipulação de comportamento, levantam preocupações acerca do fim da privacidade, do aprofundamento das clivagens socioeconômicas e da consolidação de formas pervasivas de controle.

Esses processos têm sido acompanhados por pesquisas nos campos do direito e da sociologia que se debruçam sobre as múltiplas formas pelas quais tecnologias digitais e sistemas de informação passam a definir variados aspectos de nossa rotina. Práticas de monitoramento estão de tal modo difundidas em sociedades modernas que se torna cada vez mais difícil pensar em ações que não sejam monitoradas, rastreadas e classificadas. A todo instante, compras de mercado são registradas em programas de fidelidade que servem para a construção de perfis de consumo e análises de atividade econômica; pulseiras e relógios aferem ba-

timentos cardíacos e temperatura corporal, compondo bases de dados usadas na gestão de leitos hospitalares e na precificação de seguros de saúde; ônibus e carros particulares carregam sensores de GPS que informam sobre o fluxo do trânsito, auxiliando no trabalho de engenheiros de tráfego e atualizando aplicativos de transporte. Observando esses processos, David Lyon (2007, p. 25), diretor do Centro de Estudos de Vigilância da *Queen's University*, afirma que vivemos em *sociedades de vigilância*, nas quais a visibilidade é "ubíqua, constante e inescapável".

Escrito em diálogo com o amplo debate acerca dos efeitos sociais das inovações tecnológicas, esse livro busca refletir sobre um aspecto particular das transformações em curso: a disseminação, os usos e as formas de regulação de sistemas automatizados de reconhecimento facial.

Tecnologias biométricas são usadas para identificar indivíduos a partir de características fisiológicas, que podem ser mensuradas e autenticadas com base em atributos morfológicos (traços de aparência externa) ou análises biológicas (i.e., DNA). Tecnologias de reconhecimento facial (TRFs) são um tipo específico de sistema biométrico e podem ser implementadas com múltiplas funções, incluindo a simples detecção de rostos humanos em imagens, a classificação de rostos a partir de diferentes categorias (i.e., sexo, raça, idade) e a busca por marcadores de expressão e emoção (i.e., sorriso, felicidade, raiva). Embora esses usos tenham suas próprias trajetórias de desenvolvimento e suscitem diferentes controvérsias,[1] neste livro, nos debruçamos sobre o emprego de TRFs particularmente em dois processos: a autenticação de identidade, quando verificamos se a pessoa é realmente quem diz ser, por exemplo, ao tentar acessar um *smartphone* (comparação 1:1), e a identificação de indivíduos pela comparação de duas ou mais fontes de dados (comparação 1:N), o que ocorre, por exemplo, quando a polícia cruza imagens capturadas por câmeras de vídeo com galerias de fotos de suspeitos.

1 Para um debate sobre sistemas de reconhecimento de emoção, ver: BARRET et al. (2019); CRAWFORD (2021).

A busca por formas de identificação através da parametrização de atributos faciais tem uma longa história. Ainda no século XIX, a criminologia recorreu a saberes médicos para determinar marcadores biométricos que poderiam distinguir um indivíduo dos demais, além de desenvolver técnicas forenses (i.e, *bertillonage*) para compreender as supostas determinações corpóreas dos "fora da lei" (PAVLICH, 2009). Já nos anos 1960, pioneiros do campo da visão computacional aplicaram métodos ainda embrionários de aprendizado de máquina (*machine learning*) para interpretar imagens e identificar padrões faciais (CRAWFORD & PAGLEN, 2019; RAVIV, 2021). Essa tecnologia, no entanto, só começou a se disseminar a partir dos anos 1990, quando o avanço na capacidade de processamento e a disponibilização de amplas bases de dados para treinamento dos algoritmos levaram ao ganho de precisão e à redução de custos, permitindo o desenvolvimento de sistemas comercialmente viáveis.

A partir de então, diversas instituições passaram a implementar dispositivos capazes de fazer a verificação de identidade (1:1) a partir de bases reduzidas de dados (i.e., profissionais credenciados a acessar espaços seguros, como usinas nucleares ou zonas militares). Também datam desse período os primeiros experimentos em redes de videomonitoramento urbano (GRAY, 2003; NORRIS, 2003). No entanto, a identificação em tempo-real e em espaços abertos, onde há enorme concentração de pessoas, movimento e variações de luminosidade, além da demanda por respostas rápidas a partir do cruzamento automatizado com milhões de faces, ainda representava um desafio técnico. Portanto, foi apenas na última década, com a popularização das *redes neurais convolucionais* (CNN),[2] que TRFs deram um salto de qualidade e se popularizaram.

2 Como explica David Leslie (2020, p. 8), diretor do Instituto Alan Turing: "Quando uma imagem digital é apresentada a um algoritmo de visão computacional, o que ele, de fato, 'enxerga' é apenas uma matriz de valores de *pixels* (linhas e colunas de números indicando intensidade de cor e brilho)." Para identificar um rosto na matriz, o algoritmo precisa ter sido treinado para aprender os padrões numé-

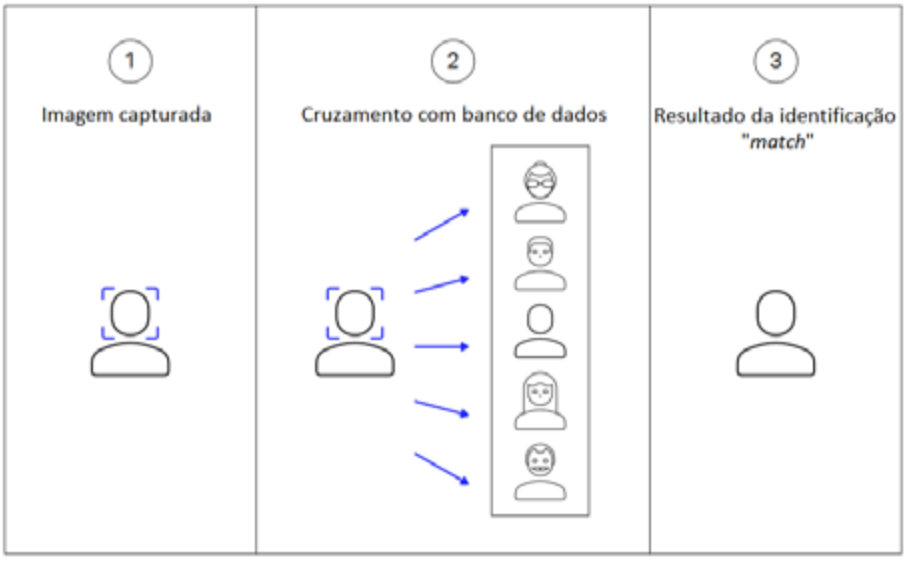
As TRFs atuais funcionam a partir de alguns passos específicos. Inicialmente, imagens são capturadas por instituições públicas ou privadas (i.e., forças policiais, departamentos de trânsito, agências de identificação civil, empresas privadas de segurança, bancos etc.). Em seguida, essas imagens são convertidas em códigos alfanuméricos que conferem unicidade aos dados, que passam então a integrar as bases com as quais serão feitas as análises. Na fase operacional, uma nova imagem é capturada e comparada com o arquivo para verificação de identidade (i.e., para acessar a conta do banco o aplicativo pede que o cliente tire uma nova foto do rosto que será cruzada com a base de dados). O resultado do sistema algorítmico não é uma resposta definitiva (sim ou não), mas um cálculo de probabilidade que afere a chance de que a nova imagem seja da pessoa cujo dado biométrico estava no arquivo.

Dependendo do contexto de implementação, as probabilidades usadas para a identificação variam, o que afeta a comodidade, a eficiência e a segurança do sistema. Por exemplo, dispositivos que buscam verificar se a pessoa que requer acesso ao aplicativo bancário é, de fato, o titular da conta precisam ter alto grau de certeza de que não se trata de uma fraude. No entanto, se o sistema tiver um limiar muito alto para a identificação, é possível que alguns clientes percam acesso ao aplicativo, o que pode gerar prejuízos e reclamações. Já os sistemas utilizados pelas forças de segurança, em geral, oferecem ao operador uma série de opções de "*match*" e porcentagens da probabilidade de cada comparação. Nesse caso, um limiar baixo vai gerar muitos "falsos positivos" – alertas de identificação para pessoas que não estão na base de busca –, mas um limiar muito alto fará o inverso, gerando "falso negativos" em abun-

ricos que representam a classe "rosto". No caso das CNNs, ocorre um processo chamado de aprendizado supervisionado, ou seja, o algoritmo identifica os padrões referentes aos rostos a partir da análise repetitiva de bases de dados pré-rotulados (i.e., milhões de exemplos de rostos humanos retirados de redes sociais). Para uma explicação mais detalhada sobre o funcionamento técnico de redes neurais, ver: Leslie (2020).

dância – o software falha em reconhecer uma pessoa procurada que se encontra na imagem. Há, portanto, um *trade-off* na definição do limiar que se resolve a partir do contexto de uso da ferramenta e, fundamentalmente, a partir das consequências do erro.

FIGURA 1. Como funciona a identificação por biometria facial?



Fonte: **RADIYA-DIXIT** (2022, p. 14)

Embora o debate público sobre o emprego de sistemas de reconhecimento facial esteja muito voltado para os riscos de discriminação no contexto da segurança pública, tema abordado em profundidade por diferentes capítulos deste livro, os exemplos acima já demostram que a identificação biométrica tem funções cada vez mais variadas. O controle de acesso a serviços digitais, como sistemas do governo ou aplicativos de celular, exige, com frequência, que indivíduos escaneiem seus rostos para autenticação de identidade. O trabalho de controle de fronteiras, antes intensivo em mão-de-obra de policiais ou agentes privados, passa pelo mesmo processo de automatização, com a instalação de totens ele-

trônicos em que passageiros tiram fotografias do rosto para comparação com documentos cadastrados (SERPRO, 2022). Mecanismo semelhante ocorre no monitoramento de catracas em sistemas de transporte público (EPTV, 2018), na identificação de torcedores em estádios esportivos (LAURENTIIS, 2023), no combate a cambistas em festivais de música (GRINBERG, 2019), na verificação de presença de alunos em escolas (TV BAHIA, 2022), no controle de ambientes de trabalho e na segurança do espaço doméstico (i.e., portarias eletrônicas).

Segundo projeções da indústria, esses múltiplos usos devem ainda se expandir nos próximos anos. Estimativas apontam um mercado global de tecnologias de reconhecimento facial de quase 13 bilhões de dólares em 2027, um salto de 297% em relação a 2019 (FORTUNE BUSINESS INSIGHTS, 2019). Esse crescimento é impulsionado por avanços na tecnologia, que diminui as barreiras técnicas para o uso, e por sua rápida disseminação no período da pandemia de COVID-19. De fato, um mapeamento de sistemas de inteligência artificial realizado por Raymond Perrault et al (2019), aponta que iniciativas de desenvolvimento de TRFs receberam, em 2019, 4.7 bilhões de dólares em investimentos, perdendo apenas para o setor de saúde e de carros autônomos.

O crescimento do mercado espelha o otimismo dos desenvolvedores em relação aos benefícios da tecnologia. Relatório do *Centre for Data Ethics and Innovation* (2020), órgão de pesquisa ligado ao governo do Reino Unido, lista algumas dessas vantagens em termos de segurança, eficiência e escala. No primeiro caso, ao substituir senhas de acesso, que podem ser roubadas ou esquecidas, TRFs aumentam a garantia de que apenas pessoas autorizadas podem fazer uso de serviços, como a requisição de auxílios financeiros do Estado, ou ter acesso a dados sensíveis, como históricos de saúde. Ainda neste campo, o uso de TRFs pelas forças policiais pode ajudar em investigações, substituindo métodos tradicionais de identificação de suspeitos a partir das impressões pouco confiáveis de vítimas e testemunhas. No contexto de centros urbanos com altas taxas de violência, o medo do crime tem se tornado o principal

aliado dos investimentos em tecnologias biométricas. Como analisado no segundo capítulo deste livro, empresas privadas e governantes alinham o discurso de que novos dispositivos de monitoramento são capazes de mitigar riscos de vitimização, diminuindo o perigo de circular pelas metrópoles brasileiras.

Em relação aos ganhos de eficiência, a capacidade de identificação automatizada permite não apenas deslocar a mão-de-obra para outras atividades, como promete trazer agilidade a diversos processos repetitivos na indústria e no setor de serviços. O relatório mencionado acima traz o exemplo de companhias aéreas obrigadas a verificar filas de passageiros antes do embarque. Estima-se que o uso de TRFs pode diminuir em até nove minutos a duração desse processo, aumentando o bem-estar de passageiros e abreviando o tempo do avião no solo. Deste modo, mais aviões podem usar o mesmo aeroporto, o que reduz ainda o custo médio de operação.

No que tange aos ganhos de escala, o exemplo mais óbvio vem também do monitoramento urbano. TRFs são mais aptas a tarefas de vigilância de amplos espaços, já que não sofrem com fadiga ou distrações e têm uma capacidade de análise muito superior ao olhar humano. Se até poucos anos, os centros de operações requeriam enormes equipes para observar as telas em busca de suspeitos, atualmente, as câmeras inteligentes são treinadas para reconhecer dinâmicas anormais ou pessoas de interesse. Ao identificar mochilas abandonadas em estações de metrô ou pessoas correndo em ruas comerciais, os sistemas de videomonitoramento disparam alertas para os operadores, que passam então a acompanhar o evento e avaliar a necessidade de intervenção.

Apesar do entusiasmo em torno de tecnologias de reconhecimento facial, movimentos sociais e organizações de direitos humanos, incluindo muitos dos autores e autoras deste livro, têm levantado debates sobre uma série de riscos associados à disseminação de dispositivos de vigilância, em geral, e aos métodos de análise biométrica, em particular. A vasta disponibilização de imagens nas redes sociais – usadas tanto para

treinar algoritmos, quanto para alimentar bases de dados – e a crescente implementação de sistemas de videomonitoramento, que operam à distância e sem o conhecimento ou consentimento explícito dos indivíduos filmados, representam sérias ameaças para a privacidade e a liberdade individual.

Como aponta Steven Feldstein (2019), pesquisador do *Carnegie Endowment for International Peace*, embora as novas tecnologias de IA também sejam empregadas por movimentos que resistem à expansão do poder repressivo de governos autocráticos, a escalada autoritária recente tem mostrado que as inovações neste campo contribuem para a corrosão democrática. Sistemas de IA são capazes de operacionalizar redes de vigilância mais amplas e intrusivas, criando um efeito inibidor sobre comportamentos indesejados que dispensa o exercício físico e violento do controle. Segundo Feldstein (2019, p. 42), "ao invés de confiar em densas infraestruturas de segurança para habilitar... a perseguição e a intimidação de oponentes em seu território, líderes autoritários têm usado IA para cultivar uma capacidade de repressão digital com baixos custos [políticos e econômicos]".

Além disso, uma falha de segurança que leve ao roubo de dados biométricos tem consequências potencialmente desastrosas e de difícil solução. Envelhecimento, mudanças de estilo (i.e., cabelos, barbas, maquiagem, tatuagens, *piercings*), novas cicatrizes ou sinais e mesmo cirurgias plásticas, podem interferir na aparência de um indivíduo, mas, na maioria dos casos, a face mantém atributos morfológicos básicos (i.e., formato do maxilar, distância dos olhos). Portanto, quando traços biométricos são parametrizados e armazenados, cria-se uma representação digital do corpo que passa a funcionar como código de acesso virtualmente imutável, o que não ocorre, por exemplo, com senhas alfanuméricas. Ou seja, no caso de um vazamento de dados, não é possível simplesmente pedir para os usuários de um sistema renovarem suas senhas.

Por fim, os próprios métodos de identificação biométrica apresentam limitações cujos efeitos são preocupantes. Em que pesem as me-

lhorias recentes de desempenho,[3] tecnologias de reconhecimento facial ainda enfrentam desafios quando são usadas em ambientes não controlados, especialmente quando se trata de indivíduos não-brancos. Joy Buolamwini e Timit Gebru (2018) apresentaram um importante relatório em que testaram as TRFs comercializadas pelas principais empresas do mercado (IBM, Microsoft, Face++) e apontaram que as falhas de identificação têm forte viés demográfico. Segundo as autoras, a análise em rostos de homens brancos é muito mais precisa do que em rostos de mulheres negras. Essa discrepância de precisão se dá pois o espectro de luminosidade usado pela maioria dos sistemas é ajustado para peles brancas, o que faz com que *pixels* de peles negras sejam vistos como indistinguíveis.[4] Outra dificuldade se revela nos padrões geométricos faciais. Quando os sistemas são treinados com rostos caucasianos, os modelos algorítmicos formulados carregaram parâmetros (i.e., distância dos olhos, formato da mandíbula, traços do nariz) que se adequam à amostra usada (DELGADO, 2022). No entanto, se estes parâmetros não são ajustados para rostos negros, podem gerar resultados flagrantemente racistas, como no caso do algoritmo do *Google Photos* que confundiu rostos de homens negros com gorilas (SIMONITE, 2018).

Além disso, apesar do entusiasmo de desenvolvedores privados, diversas pesquisas apontam que os índices de precisão ainda sofrem em condições ambientais ou técnicas adversas (LESLIE, 2020). Em resumo, diferenças de luz e sombra, vibrações ou sujeira nas câmeras, movimen-

3 A produção de câmeras com mais definição, maior capacidade de armazenamento e processamento de dados e algoritmos mais refinados, fez com que os sistemas disponíveis no mercado tenham atingido melhores níveis de precisão. Avaliação de 127 algoritmos conduzida pelo *National Institute for Standard and Technology* (NIST), dos Estados Unidos, apontou que, entre 2014 e 2018, "softwares de reconhecimento facial ficaram vinte vezes melhores em pesquisar uma base de dados para encontrar fotografias correspondentes" (NIST, 2018). Neste período, os índices de erros caíram, em média, de 4% para 0.2%.

4 Mais precisamente, os sistemas identificam pequenas variações/gradações em peles brancas, mas não em peles negras, o que atrapalha a identificação destes rostos.

tações frequentes no indivíduo filmado (i.e., rostos que mudam rapidamente de ângulo ou pessoas andando de forma não linear), chuva, névoa, maresia ou mesmo galerias de imagens muito vastas ou de baixa resolução podem interferir na capacidade de identificação, aumentando os índices de erro e tornando os sistemas menos eficazes.

Por todos os motivos descritos acima, notícias de erros de identificação são muito comuns. Em 2009, em um dos primeiros casos registrados de discriminação racial por TRFs, funcionários de uma loja nos Estados Unidos demostraram que câmeras da Hewlett-Packard (*HP MediaSmart*) com capacidade de identificar e seguir rostos nas imagens funcionavam conforme o esperado com uma funcionária branca, mas eram incapazes de reconhecer o rosto de seu colega negro (CHEN, 2009).[5] Em 2017, o sistema de desbloqueio do *Iphone* precisou ser revisto depois de alguns casos em que a identificação biométrica falhou em reconhecer o rosto de proprietários chineses (HAMILL, 2017). Dois anos depois, o sistema de análise de fotos empregado pelo governo do Reino Unido no combate à fraude em passaportes recusou a foto de um jovem negro por confundir seus lábios cerrados com uma boca aberta (GIBBONS, 2019). Em conjunto, esses casos levantaram o debate sobre o impacto de sistemas algorítmicos na reprodução do racismo. Discursos sobre a suposta neutralidade e objetividade da tecnologia escondem os múltiplos processos pelos quais sistemas de IA automatizam práticas de discriminação, um fenômeno que Tarcízio Silva (2021, p. 69) definiu como racismo algorítmico:

> o modo pelo qual a disposição de tecnologias e imaginários sociotécnicos em um mundo moldado pela supremacia branca realiza a ordenação algorítmica racializada de classificação social, recursos e violência em de-

5 O vídeo gravado pelos funcionários com a demonstração da discriminação racial pela câmera está disponível em: https://www.youtube-nocookie.com/embed/t4DT3tQqgRM (acesso em 27 de março de 2023)

> trimento de grupos minorizados. Tal ordenação pode ser vista como uma camada adicional do racismo estrutural, que, além do mais, molda o futuro e os horizontes de relações de poder, adicionando mais opacidade sobre a exploração e a opressão global.

Apesar de os desenvolvedores alegarem que muito tem sido feito para mitigar os casos de discriminação, aferir a precisão de sistemas de TRF não é tarefa simples. O primeiro problema é que a maioria dos algoritmos presentes no mercado são protegidos por regras de patentes para segredo comercial, o que dificulta a análise independente de seus resultados. Além disso, os próprios métodos para avaliar a precisão dependem dos atributos que se busca enfatizar, ou seja, a interpretação das métricas de desempenho muda com os diferentes contextos de uso. Como mencionado anteriormente, por se tratar de sistemas que funcionam por aferição probabilística, um "*match*" perfeito (100% de acurácia) entre a imagem capturada e aquela armazenada no banco de dados é indicação de fraude (exatamente a mesma imagem foi usada na verificação de identidade). Como destaca Daniel Edler (p. 76) em seu capítulo:

> mesmo 0.01% de erro pode representar um nível de falha com consequências sociais indesejáveis, seja pelo volume de rostos analisados todos os dias, seja por indicar uma total inoperância do sistema. No primeiro caso, podemos pensar nos usos correntes dessa tecnologia nas grandes cidades brasileiras. Se o dispositivo de vigilância capturar um milhão de rostos por dia (nas ruas, sistemas de transportes, entradas de espaços públicos etc.), uma taxa de erro de 0.01% indica que, em média, 100 pessoas sofrerão com abordagens equivocadas. No segundo caso, podemos pensar em um grande evento, como um festival de música, que chegue a 100 mil pessoas. Se dentro desse grupo existirem 10 homicidas procurados pela justiça criminal, o sistema de monitoramento pode não identificar ninguém e ainda assim afirmar que possui acurácia de 99.99%.

Apesar de todos os riscos listados acima, há ainda pouca regulação sobre a implementação de sistemas de reconhecimento facial no Brasil, incluindo regras de acesso e uso de bases de dados biométricos (ver capítulo 6). Normas específicas sobre como as imagens são armazenadas, para quais funções elas podem ser utilizadas, por quanto tempo as imagens capturadas pelos dispositivos de monitoramento podem ser guardadas e empregadas em investigações são ainda incertas e dependem dos interesses das múltiplas instituições públicas e privadas que fazem uso desses sistemas. Como costuma acontecer com inovações tecnológicas, empresas e órgãos públicos têm acelerado a instalação de dispositivos de monitoramento antes que legisladores sejam capazes de erigir um arcabouço legal robusto. Indo além, ao considerar o potencial inerente de TRFs para práticas de vigilância em massa, organizações da sociedade civil apontam que a única solução para garantir a liberdade individual seria o banimento destas tecnologias (ver capítulo 5). Esses debates normativos ganharam relevância nos últimos anos e muitos dos capítulos aqui publicados visam justamente a refletir sobre os problemas da legislação atual e apontar caminhos responsáveis e seguros para a implementação de sistemas de identificação biométrica.

Nesse sentido, este livro tem como objetivo apresentar o panorama atual dos debates em torno do desenvolvimento, uso e regulação de sistemas de reconhecimento facial no Brasil. Para tanto, reunimos capítulos de especialistas de diferentes áreas do conhecimento, de modo a cobrir as múltiplas práticas de gestão, governo e controle que foram impactadas pelas inovações recentes no campo da inteligência artificial aplicada às tecnologias de monitoramento biométrico. A proposta do livro não é trazer pesquisas empíricas inéditas, mas mapear, organizar e, fundamentalmente, pôr em diálogo abordagens sobre TRFs que se encontram ainda compartimentalizadas nos campos do direito, da sociologia e dos estudos de ciência e tecnologia. Nesse sentido, esperamos contribuir com uma abordagem interdisciplinar sobre o tema, o que pode ser útil para profissionais da área de segurança pública, jornalistas,

organizações da sociedade civil, estudantes e pesquisadores engajados nos temas do direito, tecnologia e sociedade.

De modo a abarcar os variados debates que cercam as TRFs, optamos por dividir a publicação em dois grupos temáticos. A primeira parte do livro traz um conjunto de capítulos que se debruçam sobre desenvolvimento, implementação e uso de sistemas de reconhecimento facial no Brasil.

O primeiro capítulo, de autoria de Pablo Nunes, coordenador do projeto Panóptico no âmbito do Centro de Estudos de Segurança e Cidadania (CESeC), traz um mapeamento do uso de sistemas de reconhecimento facial no Brasil. Nunes insere o debate sobre os efeitos da vigilância biométrica na discussão mais ampla sobre os mecanismos de controle social, destacando que a expansão do poder disciplinar do Estado tem sido acompanhada pelo aprofundamento da violência contra corpos negros.

No segundo capítulo, Daniel Edler, pesquisador do departamento de sociologia da Universidade de São Paulo (USP) e do Núcleo de Estudos da Violência (NEV/USP), traz uma análise acerca da disseminação de TRFs no campo da segurança pública. Nos últimos anos, diversos estados fizeram investimentos em dispositivos de vigilância que identificam cidadãos em espaços públicos e disparam alertas para a polícia sobre potenciais suspeitos. O trabalho de investigação também passou a ser auxiliado por sistemas integrados de imagens capazes de fazer pesquisas por pessoas específicas, o que contribui na produção de evidências para os inquéritos criminais. As promessas de redução da impunidade e da violência, no entanto, escondem alguns riscos. Erros na identificação biométrica de cidadãos têm levado à prisão de inocentes e aprofundam o caráter discriminatório da repressão policial contra grupos populacionais historicamente marginalizados. Além disso, a disseminação desses dispositivos na paisagem urbana cria uma capacidade inédita de monitoramento que pode contribuir com práticas autoritárias de controle social.

Já o terceiro capítulo, escrito por Bárbara Simão, coordenadora da área de privacidade e vigilância do InternetLab, aborda os usos de sistemas de reconhecimento facial pelo setor privado. A partir de dois estudos de caso – o uso da tecnologia por parte da ViaQuatro, concessionária da linha de metrô de São Paulo, e da ClearView, empresa norte-americana que busca acesso no mercado brasileiro para seu aplicativo que permite identificar pessoas a partir de fotos em redes sociais –, a autora debate os riscos específicos do processamento de dados biométricos por empresas privadas e apresenta algumas alternativas regulatórias que têm sido implementadas em outros países.

No último capítulo da primeira parte, Rodrigo Brandão, pesquisador do *Center for Artificial Intelligence* (C4AI) da Universidade de São Paulo (USP), apresenta alguns dos usos de sistemas de reconhecimento facial pelo setor público e discute recomendações para a mitigação dos problemas de discriminação listados acima. Para o autor, a administração pública brasileira ainda carece de mecanismos de avaliação dos sistemas implementados e de previsões legais para a responsabilização pelos erros.

Já na segunda parte do livro, nos aprofundamos nas controvérsias em torno das formas de regulação das tecnologias de reconhecimento facial, destacando não apenas os debates sobre práticas seguras e potenciais prejuízos, mas também as articulações em meio à sociedade civil em torno de projetos de lei que proíbam a implementação de TRFs em espaços públicos.

O quinto capítulo foi escrito de forma coletiva por Cynthia Picolo, Raquel Rachid, ambas pesquisadoras do Laboratório de Políticas Públicas e Internet (LAPIN), Horrara Moreira, da associação Data Privacy Brasil, e Rafaela Cavalcanti de Alcântara, então-assessora de direitos digitais da Artigo 19. Em seu texto, as autoras apresentam alguns dos motivos que levaram diversas instituições da sociedade de civil a se organizarem em torno da campanha *Tire Meu Rosto da Sua Mira*. O capítulo enfatiza que TRFs potencializam o racismo e a seletividade do sis-

tema penal e que as tentativas recentes de regulação têm sido ineficazes em bloquear as violações de direitos, em especial para grupos em situação de vulnerabilidade. Para as autoras, o banimento seria então a única solução ética. O capítulo traz ainda um pouco da memória institucional da campanha, apresentando os desafios para construção de uma rede com capilaridade em todo o país, além da articulação internacional para avançar no debate sobre os riscos de TRFs.

O capítulo seguinte, de Bianca Kremer, professora de direito digital do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP Brasília, e Fernanda dos Santos Rodrigues Silva, doutoranda em Direito, Tecnociências e Interdisciplinaridade na Universidade Federal de Minas Gerais (UFMG), levanta questões acerca do arcabouço legal vigente e aponta a necessidade de caminhar na formulação e aprovação de uma "LGPD penal" que garanta a segurança de dados pessoais sensíveis. As autoras debatem brevemente as propostas legislativas em curso e apontam os problemas da indefinição regulatória.

No sétimo capítulo, Eleonora Ceia, professora de direito do IBMEC/RJ e da UFRJ, e Chiara de Teffé, professora do IBMEC/RJ e Coordenadora de pesquisa e publicações da pós-graduação do ITS Rio, complementam o debate sobre jurisdição acerca da regulação de TRFs a partir de uma perspectiva federativa. As autoras analisam as principais controvérsias sobre tecnologias de reconhecimento facial para fins de segurança pública, a saber, os riscos de violação a direitos fundamentais e os potenciais conflitos de competência entre entes federativos na sua regulação.

Por fim, o capítulo de Sérgio Branco, diretor do Instituto Tecnologia e Sociedade (ITS), conclui a jornada proposta pelo livro com uma ampla análise das possíveis lições de marcos regulatórios desenvolvidos internacionalmente. Contando com a colaboração de Chiara de Teffé, o capítulo se debruça sobre o arcabouço legal em debate na União Europeia para pensar os limites que devem ser impostos no Brasil.

Desta forma, o livro contribui tanto para o debate público acerca do impacto de novas tecnologias de monitoramento e controle social,

quanto para a introdução às pesquisas no campo de estudos de vigilância. No contexto de digitalização da sociedade, uma preocupação central une todos os capítulos: temos que pensar em formas coletivas para assegurar o uso das tecnologias conforme os princípios democráticos da transparência, da descentralização do poder e dos direitos fundamentais.

Referências

BARRETT, L., **ADOLPHS**, R., **MARSELLA**, S., **MARTINEZ**, A. & **POLLAK**, S. "Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements". *Psychological Science in the Public Interest*, v. 20, no. 1, pp. 1–68, 2019.

BUOLAMWINI J. & **GEBRU** T. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification". *Proceedings of Machine Learning Research*, v. 81, pp. 1–15, 2018.

CDEI. "Facial Recognition Technology". Snapshot series, Centre for Data Ethics and Innovation. Londres, Maio, 2020. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/905267/Facial_Recognition_Technology_Snapshot_UPDATED.pdf

CHEN, B. "**HP** Investigates Claims of 'Racist' Computers". *Wired*, 22 de dezembro de 2009. Disponível em: https://www.wired.com/2009/12/hp-notebooks-racist/ (acesso em 23 de março de 2023)

CRAWFORD, K. & **PAGLEN**, T. *Excavating AI: The Politics of Training Sets for Machine Learning*. Disponível em: https://excavating.ai

CRAWFORD, K. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial*. New Haven, **CT**: Yale University Press, 2021.

DELGADO, A. (2022) "Race and statistics in facial recognition: Producing types, physical attributes, and genealogies". *Social Studies of Science*. Disponível em: https://doi.org/10.1177/0306312722112766

EPTV. "Ônibus de São Carlos passam a contar com sistema de biometria facial nas catracas". *G1.globo.com*, 23 de abril de 2018. Disponível em: https://g1.globo.com/sp/sao-carlos-regiao/noticia/onibus-de-sao-carlos-passam-a-contar-com-sistema-de-biometria-facial-nas-catracas.ghtml (acesso em 23 de março de 2023)

FELDSTEIN, S. "The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression". *Journal of Democracy*, v. 30, no. 1, pp. 40-52, 2019. https://doi.org/10.1353/jod.2019.0003

FORTUNE BUSINESS INSIGHTS. *Facial Recognition Market Size, Trends, Share (2030)*. Global Report, 2019. Disponível em: https://www.fortunebusinessinsights.com/industry-reports/facial-recognition-market-101061 (acesso em 23 de março de 2023)

FRY, H. *Hello World: How to be Human in the Age of the Machine*. Nova York: Doubleday, 2018.

GIBBONS, B. "Passport picture checker mistakes black man's lips for open mouth in astonishing error". *Birmingham Live*, 19 de setembro de 2019. Disponível em: https://www.birminghammail.co.uk/news/midlands-news/passport-picture-checker-mistakes-black-16945215 (acesso em 18 de março de 2023)

GRAY, M. "Urban Surveillance and Panopticism: will we recognize the facial recognition society?" *Surveillance & Society*, v. 1, no. 3, pp. 314-330, 2003 https://doi.org/10.24908/ss.v1i3.3343

GRINBERG, F. "Rock in Rio estreia sistema de câmeras de reconhecimento facial". *O Globo*, 28 de agosto de 2019. Disponível em: https://oglobo.globo.com/rio/rock-in-rio-estreia-sistema-de-cameras-de-reconhecimento-facial-23980877 (acesso em 23 de março de 2023)

HAMILL, J. "Chinese iPhone X owners claim Apple's Face ID facial recognition cannot tell them apart". *Metro*, 22 de dezembro de 2018. Disponível em: https://metro.co.uk/2017/12/22/iphone-x-racist-cant-tell-chinese-people-apart-apple-customers-claim-7178957/ (acesso em 18 de março de 2023)

KITCHIN, R., **LAURIAULT**, T. & **MCARDLE**, G. (Orgs.). *Data and the City*. Cambridge: Routledge, 2017.

LAURENTIIS, F. "Palmeiras faz primeiro teste de reconhecimento facial no Allianz Parque; veja os números". *ESPN*, 10 de janeiro de 2022. Disponível em: https://www.espn.com.br/futebol/palmeiras/artigo/_/id/11459909/palmeiras-faz-primeiro-teste-reconhecimento-facial-allianz-parque-veja-numeros (acesso em 23 de março de 2023)

LESLIE, D. *Understanding bias in facial recognition technologies: an explainer*. London: The Alan Turing Institute, 2020. Disponível em: https://doi.org/10.5281/zenodo.4050457

LUPTON, D. *The Quantified Self*. Londres: Polity Press, 2016.

LYON, D. *Surveillance Studies: An Overview*. Cambridge: Polity Press, 2007.

NIST. "NIST Evaluation Shows Advance in Face Recognition Software's Capabilities". *NIST*, 03 de novembro de 2018 Disponível em: https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities

NORRIS, C. "From personal to digital: **CCTV**, the panopticon, and the technological mediation of suspicion and social control". In: **LYON**, D. (org.). *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*. London and New York: Routledge, pp.249-281, 2003.

PAVLICH, G. "The subjects of criminal identification". *Punishment & Society*, v. 11, no. 2, pp. 171-190, 2009. https://doi.org/10.1177/1462474508101491

PERRAULT, R., **SHOHAM**, Y., **BRYNJOLFSSON**, E., **CLARK**, J., **ETCHEMENDY**, J., **GROSZ**, B., **LYONS**, T., **MANYIKA**, J., **MISHRA**, S. & **NIEBLES**, J. "The **AI** Index 2019 Annual Report". **AI** Index Steering Committee, Human-Centered **AI** Institute, Stanford University, Stanford (**CA**), 2019.

RADYIA-DIXIT, E. *A Sociotechnical Audit: Assessing Police Use of Facial Recognition*. Cambridge: Minderoo Centre for Technology and Democracy, 2022. https://doi.org/10.17863/CAM.89953

RAVIV, S. "The Secret History of Facial Recognition". *Wired*, 21 de janeiro de 2021. Disponível em: https://www.wired.com/story/secret-history-facial-recognition (acesso em 23 de março de 2023)

SERPRO. "Ponte aérea **SP-RJ** é a primeira do mundo com acesso biométrico do check -in ao embarque". *SERPRO*, 09 de agosto de 2022. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2022/ponte-aerea-rio-janeiro-sao-paulo-embarque-digital-definitivo (acesso em 23 de março de 2023)

SILVA, T. *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais*. São Paulo: Edições **SESC**, 2021.

SIMONITE, T. "When It Comes to Gorillas, Google Photos Remains Blind". *Wired*, 08 de novembro de 2018. Disponível em: https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind/ (acesso em 23 de março de 2023)

SMITH, B. & **BROWNE**, C. *Armas e Ferramentas: O Futuro e o Perigo da Era Digital*. Rio de Janeiro: Alta Books, 2020.

TV BAHIA. "Escola municipal de Mata de São João, na **BA**, usa reconhecimento facial para controlar presença de alunos". *G1.globo.com*, 07 de fevereiro de 2022. Disponível em: https://g1.globo.com/ba/bahia/noticia/2022/02/07/escola-municipal-de-cidade-da-ba-usa-reconhecimento-facial-para-controlar-presenca-de-alunos.ghtml (acesso em 23 de março de 2023)

ZUBOFF, S. *A Era do Capitalismo de Vigilância: A Luta por um Futuro Humano na Nova Fronteira do Poder*. São Paulo: Intrínseca, 2021.

PARTE I

Panorama dos usos de sistemas de reconhecimento facial no Brasil

Vigilância da cor: a tecnologia de reconhecimento facial e sua utilização no Brasil

Pablo Nunes

Resumo

As tecnologias de reconhecimento facial têm sido disseminadas no Brasil. O presente texto se propõe a apontar os efeitos perversos do uso dessas tecnologias, principalmente quando se trata de jovens negros. Destaca-se que essa tecnologia se insere em uma tradição de mecanismos de vigilância e controle de populações utilizados pelo Estado em sua própria consolidação e reprodução. Apesar de auxiliar na expansão do poder disciplinar do Estado, em terras brasileiras, o controle não será exercido sem violência quando o corpo negro é o alvo de vigilância. O texto está dividido em três partes: a primeira apresenta os desenvolvimentos sociotécnicos que levaram o reconhecimento facial ao destaque que ele possui hoje, a segunda analisa como essa tecnologia chega ao Brasil e quais efeitos já manifestados, e por fim, a terceira apresenta as tendências atuais vistas no país e os desafios que eles impõem.

Introdução

No carnaval de 2019, a imagem de um jovem negro vestido de melindrosa em um bloco em Salvador iria se tornar famosa. Não tanto pelo quê a câmera registrou naquela tarde de fevereiro, mas mais pela

própria câmera em si. Aquela imagem é o registro da primeira pessoa presa por reconhecimento facial no Brasil. A partir dali, o país passou a assistir de maneira veloz a multiplicação das câmeras com essa tecnologia pelo território nacional. De Roraima ao Rio Grande do Sul, o reconhecimento facial hoje é um dado da realidade brasileira. E seus efeitos perversos também já ficaram bem conhecidos por aqui.

O nascimento dessa tecnologia e sua utilização se insere em uma tradição das sociedades modernas de criar mecanismos de vigilância e controle de populações. Existe um extenso conjunto de estudos que se dedicam a entender esses mecanismos de vigilância utilizados pelo Estado em sua própria consolidação e reprodução. As câmeras de reconhecimento facial são um novo instrumento para esse controle e, não à toa, seu surgimento está atrelado ao ímpeto punitivista das nações modernas e ocidentais.

Apesar das tecnologias de reconhecimento facial auxiliarem na expansão do "poder disciplinar" do Estado (FOUCAULT, 1987), em terras brasileiras esse controle não será exercido sem violência quando o corpo a negro é o alvo de vigilância e controle. Em linha com o que Simone Browne (2015) defende, no Brasil, a vigilância não abre mão da violência e jovens negros reconhecidos por câmeras de reconhecimento facial ainda passarão pela violência e humilhação já bem conhecidas (RAMOS, 2022).

Isso porque, como diz Sueli Carneiro, a cor negra é a primeira coisa que chama atenção ao aparelho de vigilância e controle do Estado:

> A diversidade humana e a multiplicidade de identidades que atravessam os indivíduos, em suas diferentes características — profissão, gênero, classe etc. — desaparecem quando entra em jogo o fator negro. O negro chega antes da pessoa, o negro chega antes do indivíduo, o negro chega antes do profissional, o negro chega antes do gênero, o negro chega antes do título universitário, o negro chega antes da riqueza. Todas essas dimensões do indivíduo negro têm que ser resgatadas a posteriori, isto é, depois da averiguação, como convém aos suspeitos a priori. (CARNEIRO, 2023:144)

Este texto está dividido em três partes. Na primeira apresentarei brevemente os desenvolvimentos sociotécnicos que levaram o reconhecimento facial ao destaque que ele possui hoje, tanto seu desenvolvimento técnico, quanto sua massificação por meio de estratégias de mercado. Em seguida, analisaremos como essa tecnologia chega ao Brasil e, principalmente, que efeitos de seu uso já são visíveis em vários campos. Por fim, concluo brevemente apresentando as tendências atuais vistas no país e os desafios que eles impõem.

Desenvolvimento sócio-técnico e contexto internacional

A utilização da face como forma de identificação de pessoas não é algo tão recente. Desde os estudos de frenologia e mensuração de crânios, elementos do rosto humano servem como base para estudiosos definirem o que é uma característica "normal" de um humano e, consequentemente, o que é "desvio". Para os propósitos deste texto, proponho retrocedermos apenas até a década de 1960, quando as primeiras pesquisas produziram resultados na área de reconhecimento facial por meio de computadores.

No ano de 1966, Woodrow Bledsoe publicou os achados de seu modelo para identificar rostos humanos por meio da computação. Seu projeto utilizou um conjunto de fotografias de suspeitos produzido pela polícia, o que convencionamos chamar no Brasil de "álbum de suspeitos", como a lista de "alvos" do seu software. A partir do número de correlações positivas em relação ao total de correlações, Bledsoe calculou a razão de acerto do seu software como indicador de sucesso do seu programa.

Além de ser o que pode ser chamado de "pai fundador" dos algoritmos de reconhecimento facial modernos, o que chama atenção na pesquisa de Bledsoe são duas condições que escapam a mera taxa de acerto ou a construção dos parâmetros do software. Em primeiro lugar, sua pesquisa foi financiada por uma agência de inteligência do governo dos Estados Unidos, mostrando o interesse estatal de usar os achados de

pesquisa para usos de vigilância e militares. Mais à frente veremos que esse interesse de setores militares não se resumiria ao financiamento da pesquisa de Bledsoe.

Em segundo lugar, chama atenção o banco de dados utilizado para o treinamento e a avaliação do software. Os "álbuns de suspeitos" são bancos de dados produzidos pelas agências policiais que, em sua maioria, carecem de padrões mínimos de proteção de dados dos indivíduos bem como na qualidade do dado em si. Além disso, esses bancos ajudam a cristalizar a imagem de quem os agentes policiais entendem como "suspeitos". Esse tipo de expediente tem sido cada vez mais condenado no Brasil, tendo sido foco de trabalho do Conselho Nacional de Justiça que produziu normativas para lidar com essa realidade (CONSELHO NACIONAL DE JUSTIÇA, 2022).

Anos mais tarde, ainda nos EUA, novos estudos foram realizados no ramo da biometria facial que tornaram viável a adoção dessa tecnologia comercialmente. Em 1996, o Departamento de Defesa dos EUA e o *National Institute of Standards and Technology* (NIST) criaram o banco de dados chamado FERET (*The Facial Recognition Technology Dataset*) investindo mais de seis milhões de dólares. O banco de dados foi criado para prover informação necessária para que pesquisadores da área pudessem desenvolver novas tecnologias de reconhecimento facial. O investimento significativo feito pelo governo induziu o rápido desenvolvimento desse campo de estudo.

O sucesso do FERET fez com que várias implementações comerciais de algoritmos de reconhecimento facial surgissem pelos idos dos anos 2000, o que provocou o NIST a produzir um teste para avaliar essas soluções de biometria facial. A criação do *Facial Recognition Vendor Test* (FRVT) se coaduna com a preocupação que até hoje persegue as tecnologias de biometria facial: a sua grande maioria simplesmente não passa por avaliações sérias e transparentes de sua eficiência, e são raros os exemplos de softwares treinados fora dos ambientes controlados dos laboratórios que apresentam padrões aceitáveis de acurácia.

A partir da criação do FVRT, a NIST publica regularmente relatórios de avaliação de acurácia de diversos softwares de reconhecimento facial. A cada publicação um novo recorde de acurácia é registrado, tendo o mais novo relatório apontando o software Idemia com 99,88% de acurácia no teste realizado com 12 milhões de faces (NIST, 2023). Acurácia, em termos gerais, é a medida utilizada para avaliar o quão eficiente o software é em correlacionar corretamente a mesma face e de apontar quando as faces comparadas não pertencem a mesma pessoa. Chamamos esses casos de "positivo verdadeiro" e "negativo verdadeiro", respectivamente. O que esses resultados de acurácia escondem é que por maiores que sejam os níveis alcançados, nunca um algoritmo de reconhecimento facial acertará 100% das vezes (ver introdução). Isso significa dizer que o software da Idemia com 99,88% de acurácia ainda irá cometer erros com 398.280 cidadãos americanos que correspondem a 0,12% da população dos EUA. Isso é aceitável?

Nem mesmo o desenvolvimento de bancos de dados que apresentam registros de faces em contextos mais próximos do que ocorrem no dia a dia (baixa luminosidade, ângulo, maquiagem etc.), pode resolver a questão da acurácia. A criação do *Labeled Faces in the Wild* (LfW) foi inspirada em bancos de dados construídos mediante raspagem de dados disponíveis na internet, em um tempo em que o direito à privacidade não era tão presente nessas discussões como atualmente. A criação de bancos de dados com a coleta de imagens pelo Google Image Search (CAO et al., 2018) e Flickr (MERLER et al., 20019), por exemplo, representam um perigo claro aos direitos digitais das pessoas.

Apesar de o tema da privacidade de dados ser hoje cada vez mais forte, ainda existem empresas e softwares que utilizam dados raspados de sites públicos na internet sem o consentimento do usuário, como a ClearView AI. A empresa ficou famosa após descobrirem que a mesma coleta fotografias disponíveis online e alimenta um banco com bilhões de faces. Esses bancos são vendidos para empresas e também para agências policiais, levando a casos de prisões equivocadas (WIRED, 2023) e mal uso por parte de policiais (JOHNSON, 2023; JAYNES, 2020).

Um banco de dados massivo como da ClearView aliado aos últimos desenvolvimentos na área de *Deep Learning*[1] nos trouxe aos dias atuais em que o reconhecimento facial passou a estar presente em nossas vidas de maneira massiva, seja em autenticação de aplicativos de bancos, seja através da vigilância por parte das polícias.

Apesar das peças de propaganda que colocam o reconhecimento facial como eficiente, objetivo e que produz erros mínimos, a verdade é que diversos casos de erros foram registrados ao longo desses anos. Os erros ocorridos são frutos da miopia com que algoritmos de reconhecimento facial enxergam pessoas negras. Segundo a pesquisa "*Gender Shades*", conduzida por Joy Buolamwini e Timnit Gebru (2018), algoritmos de reconhecimento facial baseados em *machine learning* podem discriminar pessoas baseado em gênero e raça. Os resultados mostraram que a taxa de erros para mulheres negras chegou a 34,7%, enquanto o erro máximo para homens brancos foi de 0,8%.

Vários casos de erros cometidos por reconhecimento facial ocorreram nos últimos anos. Robert Williams estava em seu trabalho quando recebeu uma ligação do departamento de polícia solicitando sua presença na delegacia para ser preso (HILL, 2020a) . Ao chegar na delegacia ele foi algemado e os policiais não disseram o porquê dele estar sendo preso. Robert foi identificado erroneamente pelo sistema de reconhecimento facial e passou por horas tensas enquanto esteve detido. Em um caso semelhante, Nijeer Parks foi acusado erroneamente de ter furtado doces de uma loja e de ter acertado um policial com um carro (HILL, 2020b). Ele passou dez dias na prisão. Os erros produzidos pelo reconhecimento facial impuseram uma questão para o desenvolvimento dessa tecnologia.

1 *Deep Learning* ou aprendizagem profunda é uma área do *Machine Learning*, ou, aprendizado de máquina. É baseado em um conjunto de algoritmos que procuram realizar suas tarefas através de várias camadas de processamento, cada vez mais profundas (ver capítulo 4).

O que tem ocorrido nos últimos anos é um movimento crescente de impor limites e até mesmo banir esse tipo de tecnologia nos espaços públicos ou, especificamente, para as agências policiais (ver capítulo 5). Essa mudança de cenário que se intensifica a partir de 2019 tem relação com os casos de maior repercussão internacional de uso de algoritmos de reconhecimento facial.

A ação violenta e abrangente da China contra a minoria islâmica Uigur tomou as manchetes em 2019. Mais de 500.000 faces de indivíduos uigures foram escaneadas em apenas um mês de uso da inteligência artificial na região de Xinjiang (MOZUR, 2019). No ano seguinte, a morte de George Floyd detonaria uma série de protestos massivos nos EUA e no mundo. Em resposta às manifestações, agências policiais fortaleceram seu sistema de vigilância, principalmente nos pontos onde foram registradas aglomerações de manifestantes, como a Anistia Internacional (2022) documentou.

Os casos serviram para dar corpo a uma série de movimentações pelo banimento do reconhecimento facial. A campanha "*Ban Facial Recognition*", capitaneada pela *Fight for the Future* e assinada por centenas de organizações, mapeou algumas dezenas de cidades americanas que já baniram o uso de reconhecimento facial por suas polícias (FIGHT FOR THE FUTURE, [s.d.]). Além dos EUA, a Justiça da Argentina proibiu recentemente o uso de reconhecimento facial após prisões indevidas (JUSTIÇA, 2022), a Itália baniu o reconhecimento facial exceto para fins de segurança pública (ITALY, 2022), e o atual governo da Alemanha se posicionou pelo banimento do reconhecimento facial e da vigilância em massa (NOYAN, 2021). Apesar do banimento do reconhecimento facial seguir avançando no cenário internacional, incluindo a União Europeia (PEETS et al, 2021), a tecnologia está em todo lugar (SIMONITE, 2021).

O movimento pelo banimento tem sido desafiado por uma postura agressiva das grandes empresas de tecnologia em campanhas publicitárias, financiamento de agências governamentais, doações de tecnologia e casos de usos que colocam os setores progressistas em situação desconfortável.

Gostaria de destacar esse último ponto, pois acredito que seja o cenário de maior disputa entre as grandes empresas de tecnologia e ativistas pelos direitos humanos. A invasão do Capitólio, em janeiro de 2021, colocou boa parte dos defensores do banimento do reconhecimento facial em uma situação sensível. Afinal de contas, reacionários e extremistas invadiram o Congresso americano para impedir a diplomação do presidente eleito, Joe Biden, em um movimento sem precedentes na história americana e que, de maneira muito clara, desafiava a democracia daquele país. "Democracia" e seu fortalecimento fazem parte central das preocupações e linhas de ação de uma parcela significativa dos movimentos sociais e coletivos. O CEO da Clearview à época disse que seu software de reconhecimento facial foi utilizado por policiais para identificar os invasores – eles registraram um aumento de 26% no uso do software no dia posterior à invasão (LYONS, 2021). Como então se opor a tecnologia quando policiais e alguns ativistas passaram a utilizar softwares de reconhecimento facial para identificar os invasores do Capitólio?

Essa não seria a primeira nem a última vez que o reconhecimento facial seria utilizado com a anuência de setores progressistas. O que temos visto ao longo dos anos é que a maioria desses projetos se inicia com dois objetivos básicos: identificar pessoas procuradas pela justiça e encontrar pessoas desaparecidas, notadamente, crianças. O fato de o reconhecimento facial ser vendido como um auxílio na busca de crianças desaparecidas acaba por desarticular setores que se oporiam em um primeiro momento. Nesse sentido, o reconhecimento facial seria como uma vigilância do "cuidado" ao tomar conta daqueles que são inocentes e desprotegidos (O'NEILL et al, 2022). Uma das questões mais complicadas nesse uso é que o rosto das crianças muda rapidamente em poucos meses, o que é reconhecido como um desafio técnico para o uso de reconhecimento facial. A despeito desses limites, a indústria segue usando a inocência das crianças, e o que essa inocência suscita nos adultos, para seguir legitimando e expandindo seus negócios com tecnologias de vigilância (ibidem).

Em um caso mais recente, a ClearView AI tem propagandeado seus esforços para auxiliar na identificação de mortos no contexto da guerra da Rússia contra a Ucrânia (HAGERTY, 2023). A defesa da soberania ucraniana é quase um consenso internacional e os supostos esforços da Clearview em colaborar para que familiares e amigos possam saber se o seu familiar ou amigo foi morto durante um ataque acaba criando uma imagem de que o reconhecimento facial está no lado "dos mocinhos".

Independente da opinião se é necessário ou não responsabilizar criminalmente os que invadiram o Capitólio, do possível benefício de se encontrar crianças desaparecidas, ou de religar parentes e amigos com entes mortos na guerra, todos esses usos estão mais para "dádivas" indigestas do que qualquer outra coisa. São "trojans"[2], benesses doadas para a sociedade pelas grandes empresas, mas que escondem por trás todos os riscos e vieses que a tecnologia possui. O fato de a Clearview AI estar atuando na guerra da Ucrânia gratuitamente para identificar mortos é apenas a forma que a empresa encontrou de deixar fora dos holofotes o uso de sua tecnologia que realmente gera lucros para a empresa. Aceitando esse Cavalo de Tróia a sociedade acaba incorporando de maneira irrefletida a tecnologia e seus perigos.

O Reconhecimento facial ganha o Brasil

No Brasil, a história do reconhecimento facial na segurança pública é mais recente. Durante os grandes eventos que mobilizaram todo o país durante os anos 2010, foram experimentadas diversas tecnologias e arquiteturas de vigilância voltadas para a segurança desses eventos. Em dez anos, o Brasil recebeu as Olimpíadas e a Copa do Mundo, os principais eventos esportivos do mundo; também foi sede da Jornada

2 *Trojans* ou Cavalos de Tróia são *malwares* que enganam o usuário sobre sua verdadeira intenção, incluir vírus e transformar o computador em um disseminador de malwares.

Mundial da Juventude, série de atividades realizadas pela igreja católica que mobilizou mais de 3 milhões de católicos de todo mundo (JORNADA, 2021), incluindo o próprio Papa. Esses são apenas os maiores e mais expressivos exemplos dos eventos que marcaram essa década no Brasil.

Receber esse número grande de pessoas no país, incluindo chefes de Estado e de governo, além dos principais atletas de várias modalidades, impôs aos diversos governos uma preocupação em relação à segurança pública. Esse que é um tema central no Brasil, também poderia ser a grande pedra no sapato.

Na esteira dessas preocupações, os Centros Integrados de Comando e Controle (CICCs) foram propostos como uma forma de reunir as principais agências ligadas à segurança pública, mas também Defesa Civil, bombeiros etc., em um espaço de troca e de pronta resposta a possíveis ocorrências[3]. Sua integração se dava a nível local, no estado, mas também a nível nacional, já que muitos estados receberam jogos da Copa e de seus campeonatos preparatórios. Essa "coordenação como técnica de governo" (CARDOSO; HIRATA, 2016) foi uma marca dos anos 2010 na área de segurança pública e provocou uma série de mudanças de tendências nas agências policiais brasileiras[4].

Nesse contexto, alguns estados testaram tecnologias de reconhecimento facial dentro dos CICCs. A tecnologia foi usada nos jogos preparatórios para a Copa, nos principais estádios brasileiros (FILHO/ CALIL, 2012) e, apesar do uso disseminado pelo país, há pouca informação sobre os efeitos do uso dessas tecnologias durante os jogos e, principalmente, como as agências policiais trataram da ferramenta. O que sabe-

3 Até 2014, ano da Copa do Mundo, foram criados 12 CICCs. Para saber mais sobre as agências que integram os CICCs e seu modelo de operação, ver: MARTINS, 2023.

4 Seja pela manutenção da coordenação enquanto cerne da política pública de segurança, seja pela adoção cada vez mais frequente de novas tecnologias com a justificativa de melhoria na eficiência, os CICCs têm papel importante nas tendências que assistimos nos últimos anos.

mos é que, apesar da propaganda da época, boa parte dos CICCs deixou de usar reconhecimento facial em sua rotina. Aliás, muitos dos Centros simplesmente viram seus orçamentos enxugarem de maneira a impossibilitar sua plena operação, cenário em que muitos CICCs se encontram até hoje (BACELAR; TEIXEIRA; ARAÚJO, 2018).

De certa forma, a tecnologia de reconhecimento facial para segurança pública hibernou após o final dos grandes eventos e a subsequente crise fiscal que atingiu o país em cheio a partir de 2015 só ajudou a desmobilizar os projetos. Simultaneamente, o país enfrentou o pior momento em termos de mortes violentas, chegando ao patamar de mais de 60 mil mortes registradas em 2017 (INSTITUTO DE PESQUISA ECONÔMICA APLICADA; FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2019).

Essa sensação de aumento da violência e da insegurança foi um dos muitos fatores mobilizados pela extrema-direita nas eleições de 2018. Sempre presente no cenário político brasileiro, ora mais discreta, ora mais vocal, a extrema-direita encontrou em Jair Bolsonaro seu candidato à presidência e uma centena de candidatos a deputados estaduais e federais. A campanha de 2018 foi marcada por promessas de expurgo dos adversários políticos (RIBEIRO, 2018)[5], por desejos de que bombas pudessem ser lançadas em favelas do Rio de Janeiro (WITZEL, 2019)[6] e também pela reeleição do governador da Bahia que viu inerte durante o seu primeiro mandato a letalidade policial passar dos mil mortos por ano (MENDONÇA, 2022)[7].

Junto a eleição de governadores e presidente aliados a uma pauta punitivista e inclinados a aceitar a violação de direitos como política pública, houve um aumento importante do número de parlamentares

5 Em comício no Acre, Bolsonaro disse "Vamos fuzilar a petralhada".

6 Em campanha ao Palácio Guanabara, Wilson Witzel disse que "se fosse com autorização da ONU, em outros lugares do mundo, nós tínhamos autorização para mandar um míssil naquele local e explodir aquelas pessoas".

7 Durante a gestão Rui Costa, a Bahia entrou para o seleto grupo de estados brasileiros a registrar mais de mil mortes cometidas por policiais anualmente.

eleitos sob o mesmo manto. A legislatura iniciada em 2019 foi marcada também pela primeira viagem internacional de parlamentares e o destino foi a China. Posto de maneira clara pelas matérias à época, os parlamentares foram ao país asiático para importar novas tecnologias, principalmente as de reconhecimento facial (REBELLO, 2019).

A partir de então, vários projetos de uso de câmeras com reconhecimento facial iriam se espalhar pelo Brasil. Bahia e o Rio de Janeiro foram os estados onde esses projetos tomaram uma maior relevância dado o tamanho das unidades federativas, seus problemas crônicos com a violência e por serem projetos capitaneados pelos estados e não pequenas iniciativas feitas por municípios.

A Bahia se destacou pela estrutura que dava as bases para o projeto de uso de câmeras. Aproveitando a estrutura de vigilância construída desde a Copa do Mundo com os CICCs, a Bahia pôde rapidamente incluir o sistema de reconhecimento facial ao seu conjunto de ferramentas de vigilância. A estrutura por trás do projeto, aliada ao comprometimento pessoal do governador em fazer daquela tecnologia um "case de sucesso" de sua gestão, permitiu que o projeto baiano se consolidasse mais rapidamente e fincasse raízes mais profundas na gestão pública. Não à toa ele é o mais antigo projeto de reconhecimento facial ainda em operação no Brasil e está atualmente expandindo a sua cobertura para o interior do estado. E, pela última contagem, já são 746 os presos por meio de reconhecimento facial no estado (RECONHECIMENTO, 2023).

No Rio de Janeiro, foi escolhido o bairro de Copacabana para o projeto-piloto realizado em 2019. Foram duas fases, a primeira durou dez dias com um número menor de câmeras e ficou localizada apenas no bairro de Copacabana. Já a segunda fase expandiu a quantidade de câmeras naquele bairro e ainda ampliou a cobertura para os arredores do Maracanã e do aeroporto. Diferente da Bahia onde o governador foi o grande patrocinador da tecnologia, no Rio de Janeiro a iniciativa foi tímida e localizada, fruto de uma parceria com a empresa Oi, que cedeu as câmeras e o software para a Polícia Militar "sem custo" (NUNES; SILVA; OLIVEIRA, 2022).

Em ambos os estados, foram registrados casos de erros no reconhecimento facial. O primeiro deles é expressivo não só dos problemas inerentes a tecnologia em si e sua cegueira em relação a pessoas racializadas, mas também demonstra como os perigos no uso de novas tecnologias podem vir de diferentes fontes. Durante a primeira fase do projeto-piloto, uma mulher foi reconhecida erroneamente pelo software. Além das consequências individuais para a pessoa detida para averiguação, o fato é que, na verdade, a pessoa procurada já estava presa há anos. Ou seja, o banco de dados estava desatualizado. E não só isso: os gestores do projeto-piloto sabiam que o banco não poderia ser utilizado, mas decidiram fazê-lo mesmo assim (NUNES; SILVA; OLIVEIRA, 2022).

Em Salvador, enquanto estava a caminho de uma consulta médica com sua mãe, um jovem foi abordado por um policial que apontou uma arma para a sua cabeça. Nada poderia justificar essa utilização da arma de fogo durante uma abordagem: o jovem não oferecia nenhum risco à segurança do policial e nem a terceiros. Segundo o relato da mãe do jovem que possui deficiência mental, o policial apontou a arma para a cabeça do seu filho enquanto ele estava de costas em uma padaria onde tomavam café (PALMA; PACHECO, 2020). Depois desse encontro violento com a polícia, o jovem não conseguiu sair às ruas novamente por certo tempo.

Esses casos marcaram o ano de 2019, quando a tecnologia de reconhecimento facial ganhou força no Brasil. Durante esse ano, mapeamos os casos de prisões com o uso dessa tecnologia. Foram 184 pessoas presas em seis estados. A grande maioria dos casos em que foi possível recolher informações sobre a cor/raça do preso, 90% deles eram negros. E presos, em sua maioria, por crimes sem violência, como furtos e tráfico de pequenas quantidades de drogas (NUNES, 2023).

Unindo a vontade da extrema-direita de implantar no país um estado de vigilância massiva e os investimentos financeiros, tanto do poder público, quanto de empresas privadas, registramos a partir de 2019 um aumento expressivo no número de câmeras com tecnologias de reco-

nhecimento facial no Brasil. Os investimentos públicos, seja por meio de emendas parlamentares, seja pela destinação de parcelas importantes do Fundo Nacional de Segurança Pública (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2019)[8], possibilitaram que diversas cidades e estados tivessem a primeira experiência com a tecnologia. Aliado ao movimento governamental, empresas passaram a oferecer testes gratuitos ou empréstimos de aparelhos e softwares com o intuito de criar um mercado consumidor.

O movimento político e de mercado encontrou pouca resistência de setores progressistas no Brasil. A mistificação com que alguns setores ainda tratam tecnologias baseadas em Inteligência Artificial fez com que a chegada do reconhecimento facial no país fosse celebrada por muitos daqueles que defendem e lutam pela igualdade e pela garantia de direitos.

Isso porque, para esses setores, o racismo que estrutura a polícia e o sistema de justiça criminal poderia ser superado, uma vez que o operador do sistema deixa de decidir quem ele irá abordar ou aplicar maiores penas e a decisão passa para as mãos de tecnologias "isentas e objetivas". Dar a um algoritmo "isento" a responsabilidade de selecionar, por exemplo, quem será abordado seria a resposta final ao problema secular do perfilamento racial.

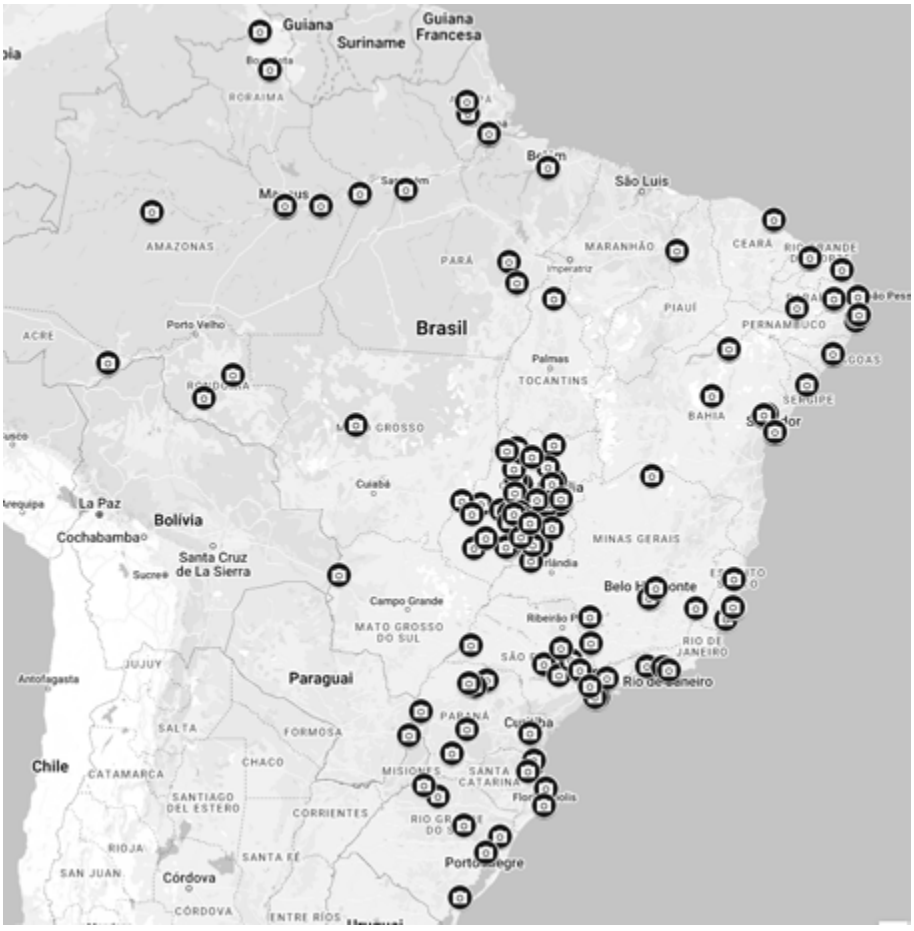
O véu da isenção e da objetividade com que são cobertas as novas tecnologias já foi muito bem desvelado por diversos autores[9]. No entanto, ele segue sendo um dado facilitador para o avanço de novas tecnologias baseadas em Inteligência Artificial, principalmente as aplicadas à segurança pública.

8 Em 2019, o então Ministro da Justiça, Sérgio Moro, assinou a portaria nº 793 que reservou parte do Fundo Nacional de Segurança Pública para o financiamento de câmeras de reconhecimento facial.

9 Para uma aproximação sobre o tema a partir de uma leitura racial, ver KREMER, 2021 e SILVA, Tarcízio, 2022.

O resultado pode ser demonstrado pelo número de cidades e estados brasileiros que já tiveram contato ou seguem utilizando tecnologias de reconhecimento facial. Dados coletados até o final de 2022 mostram que a quase totalidade das 27 Unidades Federativas já utilizaram reconhecimento facial na segurança pública.

FIGURA 1. Mapeamento do uso de tecnologias de reconhecimento facial pelas forças de segurança



Fonte: NUNES, 2023.

O avanço desenfreado dessa tecnologia no Brasil não foi acompanhado, como visto pelos exemplos do Rio de Janeiro e da Bahia, da estruturação de uma política pública de segurança onde a tecnologia seria apenas uma ferramenta. Nem houve preocupação com a construção de procedimentos operacionais para estruturar o uso diário da tecnologia. Tampouco a população sujeita ao reconhecimento facial foi amplamente informada sobre o processamento de suas imagens a partir de câmeras instaladas em espaços públicos.

Essas são algumas simples recomendações elaboradas pela Associação Internacional de Chefes de Polícia (IACP, na sigla em inglês) em conjunto com o Instituto de Sistemas Integrados de Informação da Justiça (IJIS, na sigla em inglês), organizações compostas por policiais (LAW ENFORCEMENT IMAGING TECHNOLOGY TASK FORCE, 2019). A organização de direitos digitais Lapin concluiu em seu relatório que nenhuma das experiências de uso de reconhecimento facial por polícias brasileiras estudadas cumpria todos os quatro critérios simples: a existência de regulação da tecnologia; boas práticas; controle dos erros de acurácia; e a defesa dos direitos dos titulares (REIS et al, 2021).

A recomendação de publicizar a eficiência das tecnologias de reconhecimento facial deveria ser algo essencial para a aquisição e o uso dessas tecnologias. Sabemos pela experiência internacional que o uso de algoritmos de reconhecimento facial pelas polícias produz erros que podem chegar a 80% (BREWSTER, 2019). No entanto, no Brasil, não existe uma agência policial ou uma secretaria de segurança pública que registre e divulgue o número de pessoas identificadas pelo algoritmo e o número de indivíduos que realmente estavam na lista de procurados.

A verdade é que as instituições de segurança pública brasileiras não se moldaram completamente à democracia. No país ainda vigora a ideia de que segurança pública é assunto apenas de agentes policiais, afastando a sociedade civil e a população em geral das políticas públicas de segurança. Não é à toa que a única área do Estado que não foi modificada pela Constituição de 1988 seja a Segurança Pública. Governadores

seguem sendo donos de pequenos exércitos particulares ou, de outro lado, temos polícias tão empoderadas que submetem seus governadores a chantagens.

Esse cenário leva a uma fragmentação que se reflete na produção de dados sobre crime e violência no país. Não existe hoje no Brasil uma estatística produzida pelo estado do número total de homicídios registrados no país. Nem de crimes contra o patrimônio, estupros, pessoas desaparecidas e abordagens policiais. Cada estado produz (ou não) os dados da forma como bem entendem e os divulgam ao sabor da vontade política. Segundo pesquisa recente realizada pela Associação Brasileira de Jornalismo Investigativo, menos da metade das 27 Polícias Militares atendem a critérios básicos de transparência e produção de dados (ABRAJI, 2023).

É nesse contexto de baixa transparência estatal que as tecnologias de reconhecimento facial têm avançado. Sem saber quantas dessas pessoas reconhecidas erroneamente pelos sistemas, não conseguimos avaliar se a política de utilização de reconhecimento facial é eficiente ou não. Estamos falando de pessoas que têm tido seus direitos violados, mas também estamos falando sobre mau uso do dinheiro público e desorientação do policiamento cotidiano.

Algumas cidades que estão recebendo câmeras nem ao menos conseguem prover a maioria da população saneamento básico adequado. É o caso de Seabra, município do interior da Bahia que cobre apenas 4.03% da população com saneamento básico adequado (NUNES; LIMA; CRUZ, 2023).

Apesar de não termos os números, nada nos permite dizer que a tecnologia de reconhecimento facial utilizada no Brasil produza uma taxa de erros inferior ao registrado em outros países. Sendo assim, é razoável imaginar que essas tecnologias têm produzido efeitos de desorganização para as polícias que as utilizam. Uma vez que a tecnologia erra muito e que a cada alerta um ou dois policiais precisam abordar a pessoa reconhecida, podemos imaginar que, na maior parte do tempo, os

policiais estejam averiguando pessoas que não iriam abordar se não fosse o reconhecimento facial. Além disso, sem boas práticas e regulação, os policiais da ponta acabam criando formas próprias para lidar com a tecnologia, ampliando ainda mais as possibilidades de erros e violações.

Todo esse cenário aponta para um contexto preocupante para a segurança pública no Brasil. Mas nada é mais grave do que governos comprando tecnologias falhas a custos milionários enquanto os reais problemas de segurança pública seguem sem políticas para superá-los. É curioso notar que estados que hoje se destacam pela letalidade policial[10] sejam os mesmos com desenvolvimento de projetos de reconhecimento facial (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2022). Não é à toa.

Reconhecimento facial significa abordagem policial e fortalecimento do punitivismo. Em um país que cada vez mais assume a violência enquanto uma forma de resolver conflitos, reforça-se a ideia de que para jovens negros as únicas saídas que o Estado oferece são a cadeia ou a morte. O relato da mãe do jovem abordado violentamente por policiais em Salvador nos ajuda a enxergar essa relação:

> Dois meses depois [do filho ser abordado violentamente por conta do reconhecimento facial], aconteceu com o filho de uma amiga minha, e eles mataram o menino de 15 anos. Não foi reconhecimento facial, mas foi uma abordagem da polícia, chegaram já atirando. Ele correu com medo, os colegas conseguiram se esconder, mas ele não e mataram ele com vários tiros na nuca. Minha amiga hoje chora, acabou a vida dela porque ele era filho único, enquanto eu dou graças a Deus por não ter acontecido nada com meu filho (PALMA; PACHECO, 2020).

10 Rio de Janeiro e Bahia são os únicos dois estados da federação que registraram nos últimos anos mais de mil mortes decorrentes de intervenções policiais, segundo o Anuário Brasileiro de Segurança Pública.

Tendências e frentes de ação

Enquanto a compra de câmeras de reconhecimento facial avança, um fosso cada vez maior se abre no caminho para uma sociedade mais justa e que enxergue seus cidadãos em sua completude. A morosidade em avançarmos no Brasil em direção a uma regulação mínima ou, no melhor cenário, o banimento se baseia, na minha opinião, em três aspectos:

O primeiro deles é a própria natureza do Estado brasileiro e como ele exerce controle, vigilância e punição. O fato de termos uma das maiores populações carcerárias do mundo, o país com o maior número de pessoas mortas violentamente todos os anos, não afasta de alguns setores da sociedade a ideia de que para lidar com crime os caminhos são cadeia ou morte. Obviamente que isso só é possível enquanto há a destituição da população alvo majoritária da punição, os negros, de qualquer traço de humanidade, de qualquer direito.

Em segundo lugar, há interesses financeiros que se articulam para a manutenção e expansão dessa arquitetura de vigilância no Brasil, no nível local e no nível global. O processo de "municipalização do reconhecimento facial" que temos assistido em alguns estados se dá por relações suspeitas entre políticos e pequenas empresas que surgem um ano e fecham as portas assim que vencem a licitação para fornecer a tecnologia (NUNES, LIMA, RODRIGUES, 2023). No nível federal, deputados têm criado através de emendas uma base de apoio importante para sua pauta de segurança pública em seus estados (ibidem). E é importante notar que essa tecnologia também tem sido usada como ferramenta na guerra geopolítica entre EUA e China, tendo o último país investido massivamente nos últimos anos em estados do nordeste brasileiro[11].

11 Fonte: https://www1.folha.uol.com.br/mundo/2019/08/nordeste-vira-palco-de-guerra-fria-tecnologica-entre-eua-e-china shtml. Acesso em 30 mar 2023.

Por fim, o aspecto da transparência impõe desafios importantes para compreendermos os verdadeiros efeitos do uso do reconhecimento facial no Brasil. Isso se reflete na dificuldade que existe em criarmos uma taxa de erros, um diagnóstico, do uso dessas tecnologias por policiais em um cenário habitual de policiamento. Boa parte dos estados que utilizaram ou ainda utilizam essas tecnologias dizem não recolher essa informação, ou dizem que ela é sigilosa. Outra dificuldade é encontrarmos pessoas afetadas pelo uso das câmeras. Sabemos que nem sempre os policiais dizem que a abordagem foi fruto de um alarme do sistema de inteligência artificial e, por isso, não temos mais histórias como as ocorridas com o jovem baiano abordado violentamente em 2019. A falta de controles mínimos, de regulação e de transparência afasta a instituição policial da responsabilização, algo que tem sido a marca das polícias por décadas.

Nada mais importante do que colocar no centro do debate quais são as verdadeiras prioridades para a segurança pública dos estados brasileiros. Enquanto vemos as mortes cometidas por policiais galoparem na Bahia e no Rio, os governadores investem em tecnologias caras, enviesadas e ineficientes quando alguns locais mal têm iluminação pública adequada, inclusive para o reconhecimento facial funcionar minimamente. Enquanto isso, pessoas negras seguem sendo violadas. E essas violações são tratadas como "efeitos colaterais para um bem maior". Não caminharemos para uma sociedade realmente democrática e justa se as violações de direitos da população negra continuarem a ser vistas como "efeitos colaterais".

Referências

ABRAJI. Mapa de Acesso a Informações Públicas 2023. Avaliação de transparência ativa e passiva das Polícias Militares. 2023.

AMNESTY INTERNATIONAL. Inside the NYPD's Surveillance Machine. 2022. Disponível em: https://banthescan.amnesty.org/decode/ Acesso em 2 fev 2023.

BACELAR, Carina; **TEIXEIRA**, Fábio; **ARAÚJO**, Vera. Quartel-general das Forças Armadas no Rio sofre com falta de verbas. Jornal O Globo. 4 mar. 2018. Disponível em: https://oglobo.globo.com/rio/quartel-general-das-forcas-armadas-no-rio-sofre-com-falta-de-verbas-22454328. Acesso em 30 mar. 2023.

BREWSTER, Thomas. London Police Facial Recognition 'Fails 80% Of The Time And Must Stop Now'. Forbes. 4 jul 2019. Disponível em: https://www.forbes.com/sites/thomasbrewster/2019/07/04/london-police-facial-recognition-fails-80-of-the-time-and-must-stop-now/?sh=6d5fa9aebf95. Acesso em 23 mar. 2023.

BROWNE, Simone. Dark Matters : On the Surveillance of Blackness. Duke University Press 2015.

BUOLAMWINI, Joy; **GEBRU**, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: Conference on fairness, accountability and transparency. **PMLR**, 2018. p. 77-91.

CAO, Q.; **SHEN**, L.; **XIE**, W.; **PARKHI**, O. M.;and **ZISSERMAN**, A. Vggface2: A dataset for recognising faces across pose and age. In 2018 13th **IEEE** International Conference on Automatic Face & Gesture Recognition (**FG** 2018), 67–74. **IEEE**.

CARDOSO, Bruno; **HIRATA**, Daniel. "Coordenação como técnica de governo". Horizontes Antropológicos, Porto Alegre, ano 22, n. 46, p. 97-130, jul./dez. 2016 http://dx.doi.org/10.1590/S0104-71832016000200004

CARNEIRO, Sueli. Dispositivo de racialidade: A construção do outro como não ser como fundamento do ser. Rio de Janeiro: Ed. Zahar, 2023.

CONSELHO NACIONAL DE JUSTIÇA. Grupo de Trabalho: Reconhecimento de Pessoas. Brasília: **CNJ**, 2022. Disponível em:https://www.cnj.jus.br/wp-content/uploads/2022/12/relatorio-final-gt-sobre-o-reconhecimento-de-pessoas-conselho-nacional-de-jusica.pdf> Acesso em 30 mar. 2023.

FIGHT FOR THE FUTURE. Ban facial recognition. [s.d.]. Disponível em: https://www.banfacialrecognition.com/map/. Acesso em 2 de fev. 2023.

FILHO, Herculano Barreto; **CALIL**, Lucas. Reconhecimento facial em câmeras irá identificar torcedores em estádios. Jornal Extra. 25 ago. 2012. Disponível em: https://extra.globo.com/casos-de-policia/reconhecimento-facial-em-cameras-ira-identificar-torcedores-em-estadios-5896012.html. Acesso em 3 fev. 2023.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, Anuário Brasileiro de Segurança Pública 2022. São Paulo. 2022. Disponível em: https://forumseguranca.org.br/anuario-brasileiro-seguranca-publica/. Acesso em 17 mar. 2023.

FOUCAULT, M. Vigiar e Punir: história da violência nas prisões. Petrópolis: Editora Vozes, 1987.

HAGERTY, Alexa. In Ukraine, Identifying the Dead Comes at a Human Rights Cost. Wired. 22 fev. 2023. Disponível em: https://www.wired.com/story/russia-ukraine-facial-recognition-technology-death-military/. Acesso 2 fev. 2023.

HILL, Kashmir. Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match. Nova Iorque. 29 dec. 2020b. Disponível em: https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html. Acesso em 28 jan 2023.

HILL, Kashmir. Wrongfully Accused by an Algorithm. New York Times. Nova Iorque. 24 jun. 2020a. Disponível em: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html. Acesso em 28 jan 2023.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA; FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. "Atlas da violência 2019". Brasília: Rio de Janeiro: São Paulo: Instituto de Pesquisa Econômica Aplicada; Fórum Brasileiro de Segurança Pública. 2019

ITALY outlaws facial recognition tech, except to fight crime. Reuters. 14 nov 2022. Disponível em: https://www.reuters.com/technology/italy-outlaws-facial-recognition-tech-except-fight-crime-2022-11-14/. Acesso em 2 fev. 2023.

JAYNES, A. The end of anonymity? Facial recognition app used by police raises serious concerns, say privacy advocates. *CBC Radio*, 21 de janeiro de 2020. Disponível em: https://www.cbc.ca/radio/thecurrent/the-current-for-jan-21-2020-1.5434328/the-end-of-anonymity-facial-recognition-app-used-by-police-raises-serious-concerns-say-privacy-advocates-1.5435278 Acesso em 01 jan. 2023.

JOHNSON, K. Face Recognition Software Led to His Arrest. It Was Dead Wrong. *Wired*, 28 de fevereiro de 2023. Disponível em: https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/ Acesso em 01 mar. 2023

JOHNSON, Khari. Face recognition software led to his arrest. It was dead wrong. **WIRED**. Disponível em: https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/. Acesso em: 1 jan. 2023.

JORNADA Mundial da Juventude. Globo. 28 out. 2021. Disponivel em: https://memoriaglobo.globo.com/jornalismo/coberturas/jornada-mundial-da-juventude/noticia/jornada-mundial-da-juventude.ghtml. Acesso em 3 fev. 2023.

JUSTIÇA argentina proíbe reconhecimento facial após prisões indevidas. Convergência Digital. 8 set. 2022. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Justica-argentina-proibe-reconhecimento-facial-apos-prisoes-indevidas-61384.html. Acesso em 2 fev. 2023

KREMER, Bianca. *Direito e tecnologia em perspectiva amefricana : autonomia, algoritmos e vieses raciais*. Tese (doutorado)–Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Direito, 2021.

LAW ENFORCEMENT IMAGING TECHNOLOGY TASK FORCE. Law Enforcement: Facial Recognition use case catalog. 2019. Disponível em: https://www.theiacp.org/resources/document/law-enforcement-facial-recognition-use-case-catalog. Acesso em: 24 mar. 2023.

LYONS, Kim. Use of Clearview AI facial recognition tech spiked as law enforcement seeks to identify Capitol mob. The Verge. 10 jan 2021. Disponível em: https://www.theverge.com/2021/1/10/22223349/clearview-ai-facial-recognition-law-enforcement-capitol-rioters. Acesso em 2 fev. 2023.

MARTINS, Vitor. CICC – Centro Integrado de Comando e Controle. WikiFavelas. 2023. Disponível em: https://wikifavelas.com.br/index.php/CICC_-_Centro_Integrado_de_Comando_e_Controle. Acesso em 3 fev. 2023.

MENDONÇA, Jeniffer. Por que a violência policial explodiu na Bahia mesmo com 15 anos de PT no poder. Ponte Jornalismo. 10 mar. 2022. Disponível em: https://ponte.org/por-que-o-governo-da-bahia-nao-reduziu-a-violencia-policial-mesmo-com-15-anos-de-pt-no-poder/. Acesso em 2 fev. 2023.

MERLER, M.; RATHA, N.; FERIS, R. S.; SMITH, J. R. Diversity in Faces. arXiv preprints arXiv:1901.10436. 2019

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. PORTARIA Nº 793, DE 24 DE OUTUBRO DE 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575. Acesso em 20 mar. 2023.

MOZUR, Paul. One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. 14 abr. 2019. Disponível em: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html. Acesso em 2 fev 2023Fonte:

NOYAN, Oliver. New German government to ban facial recognition and mass surveillance. Euractiv. 26 nov 2021. Disponível em: https://www.euractiv.com/section/data-protection/news/new-german-government-to-ban-facial-recognition-and-mass-surveillance/. Acesso 2 fev. 2023.

NUNES, Pablo. Coleção Panorama: Reconhecimento Facial. Rio de Janeiro: CESeC, 2023 (no prelo).

NUNES, Pablo; **LIMA**, Thallita Gabriele Lopes; **CRUZ**, Thais Gonçalves. **O SERTÃO VAI VIRAR MAR**: Expansão do reconhecimento facial na Bahia. Rio de Janeiro: **CESeC**, 2023 (no prelo).

NUNES, Pablo; **LIMA**, Thallita Gabriele Lopes; **RODRIGUES**, Yasmin. **DAS PLANÍCIES AO PLANALTO**: como Goiás influenciou a expansão do reconhecimento facial na segurança pública brasileira. Rio de Janeiro: **CESeC**, 2023 (no prelo).

NUNES, Pablo; **SILVA**, Mariah Rafaela; **OLIVEIRA**, Samuel R. Um Rio de olhos seletivos [livro eletrônico]: uso de reconhecimento facial pela polícia fluminense. Rio de Janeiro: **CESeC**, 2022.

O'**NEILL**, Christopher et al. The two faces of the child in facial recognition industry discourse: biometric capture between innocence and recalcitrance. Information, Communication & Society, v. 25, n. 6, p. 752-767, 2022. Disponível em: https://doi.org/10.1080/1369118X.2022.2044501. Acesso em 2 fev. 2023.

PALMA, Amanda; **PACHECO**, Clarissa. 'O policial já foi com a arma na cabeça dele', diz mãe de rapaz confundido por reconhecimento facial. Correio. 5 jan 2020. Disponível em: https://www.metro1.com.br/noticias/cidade/85609,o-policial-ja-foi-com-a-arma-na-cabeca-dele-diz-mae-de-jovem-confundido-por-reconhecimento-facial. Acesso em 17 mar. 2023

PEETS, Lisa et al. European Parliament Votes in Favor of Banning the Use of Facial Recognition in Law Enforcement. Insider Privacy. 12 out 2021. Disponível em: https://www.insideprivacy.com/artificial-intelligence/european-parliament-votes-in-favor-of-banning-the-use-of-facial-recognition-in-law-enforcement. Acesso em 1 fev. 2023.

RAMOS, Silvia. Negro Trauma: Racismo e abordagem policial no Rio de Janeiro. Rio de Janeiro: **CESeC**, 2022.

REBELLO, Aiuri. Bancada do **PSL** vai à China importar sistema que reconhece rosto de cidadãos. **UOL**. 16 jan 2019. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2019/01/16/bancada-do-psl-vai-a-china-para-importar-tecnicas-de-reconhecimento-facial.html. Acesso em 6 fev. 2023.

RECONHECIMENTO captura dois homens que não pagavam pensão. **SSP-BA**. 24 mar. 2023. Disponível em: https://www.ssp.ba.gov.br/2023/03/13556/Reconhecimento-captura-dois-homens-que-nao-pagavam-pensao.html. Acesso em 24 mar. 2023

REIS, Carolina; **ALMEIDA**, Eduarda; **DA SILVA**; Felipe; **DOURADO**, Fernando. Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil. Brasília: Laboratório de Políticas Públicas e Internet, 2021.

RIBEIRO, Janaína. Set/2018: "Vamos fuzilar a petralhada", diz Bolsonaro em campanha no Acre. Exame. 3 set. 2018. Disponível em: https://exame.com/brasil/vamos-fuzilar-a-petralhada-diz-bolsonaro-em-campanha-no-acre/. Acesso em 3 fev. 2023

SILVA, Tarcízio. Racismo algorítmico: inteligência artificial e discriminação nas redes digitais. Edições Sesc **SP**, 2022.

SIMONITE, Tom. Face Recognition Is Being Banned—but It's Still Everywhere. 22 dez 2021. Wired. Disponível em: https://www.wired.com/story/face-recognition-banned-but-everywhere/. Acesso em 28 jan. 2023.

WITZEL diz que 'em outros lugares do mundo', poderia ter autorização para jogar míssil em bandidos da Cidade de Deus. G1. 14 jun 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/06/14/em-discurso-witzel-fala-em-jogar-missil-em-traficantes-na-cidade-de-deus.ghtml. Acesso em 3 de fev. 2023

Biometria facial e segurança pública: Práticas contemporâneas de vigilância policial

Daniel Edler Duarte[1]

Resumo

Tecnologias de reconhecimento facial têm transformado práticas policiais no Brasil. Nos últimos anos, diversos estados fizeram investimentos em dispositivos de vigilância que identificam cidadãos em espaços públicos e disparam alertas para a polícia sobre potenciais suspeitos. O trabalho de investigação também passou a ser auxiliado por sistemas integrados de imagens capazes de fazer pesquisas por pessoas específicas, o que contribui na produção de evidências para os inquéritos criminais. As promessas de redução da impunidade e da violência, no entanto, escondem alguns riscos inerentes ao uso dessas tecnologias no contexto da segurança pública. Erros na identificação biométrica de cidadãos têm levado à prisão de inocentes e aprofundam o caráter discriminatório da repressão policial contra grupos populacionais historicamente marginalizados. Além disso, a disseminação desses dispositivos na paisagem urbana cria uma capacidade inédita de monitoramento que, sem regulação ou transparência, pode contribuir com práticas autoritárias de controle social. Este capítulo tem como objetivo apresentar o pano-

1 A pesquisa para este capítulo foi financiada pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP). Processo No. 2020/05628-1.

rama do uso de tecnologias de reconhecimento facial pelas forças de segurança no Brasil e refletir sobre seus potenciais prejuízos.

Introdução

Tecnologias de reconhecimento facial (TRFs) são cada vez mais comuns em meio à panóplia de equipamentos de vigilância à disposição das instituições policiais. Com os avanços em capacidade de processamento computacional e o barateamento das câmeras e dos softwares de análise biométrica disponíveis no mercado, forças de segurança mundo afora adquiriram sistemas para extrair dados sobre circulação e comportamento de indivíduos, facilitando o trabalho de identificação de suspeitos e auxiliando a rotina de policiamento ostensivo. Na prática, patrulhas ganharam aplicativos de verificação de identidade a serem utilizados durante abordagens e as câmeras de monitoramento passaram a realizar a identificação biométrica em tempo-real, cruzando as imagens registradas com bases de dados mantidas pelos sistemas de justiça criminal.

Até pouco tempo, as bases de imagens eram fragmentadas (em muitos casos, fitas específicas para as diferentes câmeras, que se mantinham estáticas e gravavam vídeos de baixa qualidade) e raramente eram vistas (gravações precisavam ser feitas em cima de imagens antigas e só eram recuperadas com ordens judiciais após os eventos criminais). A criação de centros de operação com *videowalls* que transmitem simultaneamente imagens de diferentes espaços públicos permitiu a integração das bases de dados, mas não resolveu alguns problemas centrais: trata-se de uma prática de vigilância intensiva em mão de obra (requer diversos profissionais destacados apenas para a observação das telas) e pouco eficiente, já que o foco nas imagens se perde em poucos minutos (SMITH, 2012).

Ao transformar os vídeos em dados estruturados que podem ser integrados e classificados, as TRFs prometem superar essas limitações. Por exemplo, se antes para a investigação de um crime era necessário des-

tacar equipes inteiras para coletar fitas e observar as milhares de horas de vídeo de diferentes câmeras, atualmente há softwares que permitem selecionar dinâmicas ou indivíduos de especial interesse, reduzindo em muito o material que precisa ser de fato analisado. No caso do monitoramento em tempo-real, os softwares também são capazes de disparar alertas para pessoas ou dinâmicas consideradas suspeitas, dispensando a necessidade do olhar contínuo dos operadores. Como aponta Jay Stanley (2019, p. 3), analista de privacidade e tecnologia da *American Civil Liberties Union* (ACLU), "por trás dos 'olhos' estúpidos das câmeras [...], nos monitoram 'cérebros' cada vez mais inteligentes".

No Brasil, as TRFs têm se disseminado em um contexto específico de segurança pública que conjuga três fatores estruturantes: a persistência de altos índices de violência, o aprofundamento da retórica punitivista e a aposta em novas tecnologias como vetor de reformas gerenciais nas polícias.

Mesmo com a queda recente na curva de homicídios, o Brasil ainda é um dos países mais violentos do mundo. Dados do Fórum Brasileiro de Segurança Pública (FBSP) apontam que 47.508 pessoas foram assassinadas em 2022 (FBSP, 2023). Elemento central para entender o enorme número de homicídios na sociedade brasileira é destacar o perfil das vítimas. Essas são, em geral, homens (91.3% das mortes violentas em 2021), negros (77.9%) e jovens (58.2% das vítimas têm entre 18 e 34 anos) (FBSP, 2022). O local de moradia também influencia nas estatísticas, que apresentam forte concentração nas periferias de grandes cidades, especialmente do Nordeste. Na prática, enquanto um morador branco dos bairros ricos de São Paulo enfrenta um risco de vitimização próximo dos patamares de países europeus, as chances de um jovem negro morador da periferia de Salvador ser assassinado são semelhantes às de baixas em cenários de guerra. O trágico panorama da violência urbana é resultado de uma série de variáveis, entre elas a dinâmica das disputas territoriais entre diferentes grupos do crime organizado, a deterioração de condições socioeconômicas (i.e., aumento do desempre-

go e altos padrões de desigualdade), e a facilidade de acesso a armas de fogo (CERQUEIRA, 2014). No entanto, as políticas públicas nessa área têm dado especial atenção à atuação policial e sua capacidade repressiva, o que nos leva para o segundo fator.

As crescentes taxas de encarceramento no país — padrão verificado desde os anos 1990 e que culminou, em 2021, com mais de 820 mil pessoas em situação de privação de liberdade (SISDEPEN, 2022) —, têm sido impulsionadas pela disseminação de um "populismo penal" marcado pela manipulação do medo do crime por políticos conservadores que se elegem com plataformas de "tolerância zero" (PRATT, 2007). Como resultado dessa "virada punitiva", David Garland (2001, p. 13) aponta que "as vozes dominantes das políticas criminais não são mais as dos especialistas ou mesmo dos profissionais do campo. [...] A importância da pesquisa e do conhecimento criminológico foi rebaixada e em seu lugar está a deferência à voz da 'experiência', do 'senso comum' e do que 'todo mundo sabe'". No bojo desse processo, testemunhamos a substituição do ideal de justiça corretiva, que depositava na prisão o objetivo de ressocialização, por práticas punitivistas caracterizadas por maior coerção, pelo moralismo e por leis que primam pela lógica da retaliação e da vingança do mal cometido. A literatura da sociologia da violência se debruça com frequência sobre esse fenômeno e, em geral, identifica suas raízes na convergência de alguns elementos mais específicos, entre eles: a deterioração do estado de bem-estar social, incluindo políticas previdenciárias robustas;[2] a fragmentação do tecido social, o que abre espaço para um individualismo exacerbado em que a competição (ou a concorrência) rege os padrões de interação; e a disseminação de uma percepção de insegurança entre as elites que guar-

2 O resultado dessa retração é o surgimento do que Loïc Wacquant (2003, p. 55) chama de "estado centauro", com uma cabeça liberal para a elite e um corpo autoritário para o resto.

da pouca correlação com as variações nos índices criminais (GARLAND, 2001; WACQUANT, 2003).

Por fim, o investimento em novas tecnologias de vigilância também deve ser entendido dentro do contexto mais amplo das iniciativas de reformas nas polícias no período de preparação para os megaeventos esportivos. Em todo o país, buscou-se implementar uma mudança de paradigma na atuação das forças de segurança que, entre outros aspectos, passou pela adoção de sistemas integrados de comando e controle e modelos empresariais de gestão. Nos últimos anos, diversos estados adotaram indicadores de desempenho que têm como meta premiar e disseminar boas-práticas, aumentando a eficiência e a eficácia da polícia (CARDOSO, 2019). Ao longo desse processo, os sistemas de videomonitoramento foram vistos como aliados que promoveriam a melhoria nos serviços de despachos, a construção de consciência situacional durante operações, a dissuasão da ação criminal sem a necessidade de ampliar o número de patrulhas e, finalmente, a produção de evidências que contribuiriam para aprimorar a qualidade dos inquéritos policiais. No contexto de modernização da gestão pública, as tecnologias de reconhecimento facial permitiriam ao Estado "fazer mais com menos".

Levantamento do Instituto Igarapé (2019) aponta que, entre 2011 e 2019, ao menos 48 cidades, distribuídas em 16 estados, implementaram sistemas de reconhecimento facial, incluindo iniciativas de segurança pública. Desde então, as TRFs se disseminaram ainda mais, deixando de ser privilégio de grandes centros urbanos e se tornando parte da infraestrutura de segurança mesmo em zonas rurais (ver capítulo 1). No entanto, essa rápida expansão tem gerado controvérsias. Por um lado, muitos agentes de segurança e desenvolvedores privados argumentam que o uso da biometria facial contribui para políticas de redução da criminalidade e manutenção da ordem. Por outro, organizações da sociedade civil lembram que estas tecnologias apresentam vieses, aprofundam a discriminação e promovem a escalada do controle social autoritário (SILVA & VARON, 2021; REIS et al., 2021; NUNES, et al., 2022). Nesse sentido,

seu uso acarreta graves riscos para a sociedade, especialmente quando não há regulação específica, objetivos bem delimitados e mecanismos de auditoria dos sistemas.

Ainda faltam estudos mais detalhados sobre os efeitos das TRFs na segurança pública no Brasil, de modo que grande parte das análises guarda forte caráter especulativo. Enquanto as polícias se mostram refratárias a avaliações independentes de impacto, diversas instituições têm denunciado casos de erros nos sistemas que levaram à prisão de inocentes (ACCESS NOW, 2021). De uma forma geral, críticos apontam que as câmeras com TRF não contribuem de forma decisiva para manutenção da ordem, violam direitos dos cidadãos e ainda geram custos desnecessários para a polícia, já que recursos escassos são empenhados em operações pouco efetivas. Diante dessas críticas, foram lançadas campanhas pelo banimento do uso de TRFs no país e diversos projetos de lei já foram apresentados para restringir seu uso (ver capítulos 5 e 6).

Esse capítulo tem como objetivo apresentar um panorama do uso de sistemas de reconhecimento facial pelas forças de segurança no Brasil, destacando os principais elementos que sustentam os altos investimentos nessa tecnologia, e abordar os riscos que esse processo representa para a privacidade e os direitos humanos.

Os usos de sistemas de reconhecimento facial pelas forças de segurança brasileiras

Tecnologias de reconhecimento facial têm sido usadas há algumas décadas como chaves biométricas para acessar espaços virtuais (i.e., contas de bancos e sites protegidos) ou físicos (i.e., zonas militares, usinas nucleares e outras infraestruturas críticas) (GRAY, 2003). Apesar do enorme interesse por identificadores pessoais, o uso se mantinha restrito pelas limitações técnicas das ferramentas disponíveis. Devido à baixa qualidade da captura do vídeo e do processamento da imagem para cruzar com as informações armazenadas nas bases de dados, era necessário

que o indivíduo a ser identificado estivesse em um ambiente com farta iluminação, se posicionasse em frente à câmera por alguns segundos e que o sistema se limitasse à autenticação (1:1) (ver introdução). Além disso, mesmo nesses casos, pequenas mudanças, como corte de cabelo e pelos faciais, envelhecimento, maquiagem, ganho ou perda de peso e adereços (i.e., óculos, chapéu) podiam impossibilitar a identificação.

Nos últimos anos, esse cenário mudou radicalmente. Os enormes ganhos de precisão analítica ajudaram a formar uma indústria global com estimativas de faturamento de 9.6 bilhões de dólares (AHMAD et al., 2020). Boa parte desse faturamento se deve à profusão de contratos públicos para monitoramento urbano. Atualmente, TRFs são capazes de cruzar bases de dados de milhões de faces com imagens capturadas em condições bastante desfavoráveis (com baixa iluminação, chuva etc.), apontando resultados de identificação (1:N) em poucos segundos. As TRFs se disseminaram de tal modo, que se tornaram parte "banal" da infraestrutura urbana (GOOLD et al., 2013).

No Brasil, os sistemas de TRF são usados para desbloqueio de *smartphones* e acesso a contas bancárias; como filtros em aplicativos de fotos e recursos de interação em redes sociais; em vitrines de lojas para identificar potenciais consumidores; como permissão de embarque em aeroportos e desbloqueio de catracas no transporte público (ver capítulo 1). Impulsionados pelo discurso agilidade e precisão, estes dispositivos ganharam especial destaque no campo da segurança pública (EDLER, 2021).

A Lei Geral de Proteção de Dados (LGPD), em vigor desde 2020, prevê maior controle para o processamento de "dados pessoais sensíveis", entre eles, as características biométricas dos indivíduos. No entanto, o uso desses sistemas por parte das polícias está em um limbo jurídico (ver capítulo 6). Em seu artigo 4º, a LGPD prevê que atividades de investigação criminal, uso repressivo por parte das polícias militares e mesmo questões ligadas à defesa nacional e segurança do Estado, seriam regulados por lei complementar, a "LGPD penal" (ver capítulo 6). Enquanto esta lei não é aprovada, não há regulação clara sobre os limi-

tes dos usos de TRFs por forças de segurança. E é nesse cenário de incerteza que diversos estados têm investido na tecnologia.

Em 2019, a Polícia Militar do Rio de Janeiro (PMERJ) implementou um sistema de videomonitoramento com reconhecimento facial no bairro de Copacabana e em áreas próximas ao estádio do Maracanã. O sistema era capaz de fazer cruzamentos entre listas de procurados mantidas pelo Conselho Nacional de Justiça (CNJ) (i.e., indivíduos com mandados de prisão em aberto) e imagens capturadas em espaços públicos. Em uma primeira fase de testes, foram instaladas 34 câmeras que capturaram cerca de três milhões de rostos e detectaram oito mil indivíduos suspeitos, mas apenas dez pessoas foram abordadas e levadas à delegacia (SILVA, 2019).[3] Relatório do projeto Panóptico, do Centro de Estudos de Segurança e Cidadania (CESeC), apontou que o software utilizado pela PMERJ produziu grande quantidade de "falsos positivos" (ver introdução). Ao avaliar o emprego do sistema durante uma partida de futebol, por exemplo, o relatório revelou que 63% dos indivíduos abordados pela polícia não eram as pessoas indicadas pelo programa de verificação biométrica (NUNES et al., 2022). Ainda assim, os números foram motivo de celebração do então comandante-geral da PMERJ, coronel Rogério Lacerda: "é a modernidade, enfim, chegando. [...] A ferramenta é fantástica. Já passou da época de a PM se modernizar" (LACERDA *apud* O GLOBO, 2019).

A polícia militar previa outros períodos de testes, mas críticas da sociedade civil, a falta de recursos e o início da pandemia de COVID-19 levaram ao adiamento do cronograma. A partir de 2022, no entanto, as TRFs voltaram à pauta do governo do estado com o anúncio da instalação de 22 câmeras no Jacarezinho, favela da zona norte do Rio de Janeiro, no marco do programa "Cidade Integrada" (COELHO, 2022).

3 Na segunda fase de testes, entre agosto e novembro do mesmo ano, os alertas do sistema de vigilância levaram à 357 prisões (dados obtidos pelo autor junto à PMERJ).

Recentemente, o governador Claudio Castro anunciou ainda o investimento de R$ 500 milhões ao longo de quatro anos para a instalação de câmeras (incluindo tecnologias de reconhecimento facial) em viaturas, delegacias e demais repartições públicas. Nas palavras do Castro, "a tecnologia é uma aliada do policial e de toda a sociedade. Estamos dando um salto tecnológico na segurança pública do nosso estado, mudando uma cultura nas polícias, e tenho muito orgulho desse avanço. Esse é o caminho: o futuro é tecnológico, não tenho dúvida disso" (CASTRO apud ARAÚJO, 2023).

Além das iniciativas centralizadas pelo governo do estado, as TRFs se disseminaram através de projetos específicos de diferentes prefeituras. Em 2019, o Centro Integrado de Operações (Ciop) de Petrópolis investiu na instalação de 56 câmeras com TRF, principalmente em áreas turísticas e ruas com concentração de comércio (PETRÓPOLIS, 2019). No mesmo ano, a prefeitura de Niterói optou por equipar seu Centro Integrado de Segurança Pública (CISP) com 70 "câmeras inteligentes". O então prefeito Rodrigo Neves apontou que o software capaz de identificar rostos e placas de carro foi peça central no programa municipal de redução da violência (GOULART, 2019). Já em 2022, 19 municípios da região metropolitana se juntaram para criar o Centro Integrado de Comando e Controle da Baixada Fluminense (CISPBAF). Com um custo aproximado de R$ 70 milhões, o centro conta com 320 câmeras e integra forças policiais, bombeiros, defesa civil, SAMU e guardas municipais com o objetivo de acelerar o tempo de resposta para incidentes e implementar um cerco eletrônico de videomonitoramento (CAXIAS, 2023).

Na Bahia, câmeras de monitoramento equipadas com sistemas de reconhecimento facial começaram a ser implementadas no final de 2018. Os dispositivos foram incialmente instalados apenas em áreas turísticas de Salvador, mas se expandiram para todo o estado a partir de 2021, quando o governo firmou contratos de mais de R$ 900 milhões com empresas privadas para a integração de 4095 câmeras à rede de vigilância (FALCÃO, 2021). Em janeiro de 2023, o governo do estado come-

morou os resultados do "maior investimento já realizado na Segurança Pública na Bahia" (BAHIA, 2023). Em pouco mais de quatro anos, 600 pessoas foram presas a partir da identificação facial, sendo 222 suspeitos com mandado de prisão em aberto por assalto, 113 procurados por homicídios, 106 por tráfico de drogas e 20 por estupro de vulnerável. Apenas no carnaval de 2023, 77 foragidos da polícia foram identificados nos circuitos dos trios elétricos que ocuparam as ruas da capital (FANTÁSTICO, 2023). Na Bahia, essa tecnologia tem se difundido ainda para municípios pequenos e com baixos índices de criminalidade, além de zonas rurais, onde há baixa concentração de pessoas para o monitoramento em tempo-real.

Em São Paulo, o governo do estado inaugurou em 2020 o Laboratório de Identificação Biométrica – Facial e Digital. O laboratório teve custo aproximado de R$ 5 milhões e conta com cerca de 30 milhões de registros biométricos. Ao integrar câmeras, bancos de dados e registros geolocalizados de ocorrências, o laboratório promete "maior celeridade, confiabilidade e capacidade de processamento na produção de provas técnicas, dando mais agilidade a diversas investigações conduzidas pela Polícia Civil" (GOVERNO DE SÃO PAULO, 2020). Câmeras já estão em operação no metrô, em catracas de ônibus e em parques públicos, mas a expectativa é que o processo de expansão se acelere nos próximos anos.

A prefeitura da capital anunciou no final de 2022 o projeto *Smart Sampa*, com investimentos de R$ 140 milhões para a instalação de 20 mil câmeras.[4] O projeto prevê que imagens de drones, câmeras corporais e

4 O edital público para a instalação da infraestrutura e a contratação do serviço de integração e gestão das bases de dados previa ainda que o sistema deveria alertar as autoridades para pessoas suspeitas de "vadiagem", o que levantou críticas sobre a produção de perfis de suspeição criminal voltados para a repressão de moradores de rua Após as denúncias de organizações da sociedade civil, o edital foi suspenso. A prefeitura informou que reformularia o projeto para retirar referências à "vadiagem" e "cor" de forma a evitar os riscos de injustiças contra populações marginalizadas (MENGUE, 2022b).

câmeras de patrulhas móveis sejam integradas e passem por uma análise automatizada de identificação de suspeitos, o que promete transformar a rotina dos policiais na capital paulista:

> Atualmente, um guarda civil ou militar tem acesso a imagens de procurados em aparelhos nas viaturas. Caso aborde um suspeito, faz a checagem para verificar se é a mesma pessoa. Com a nova tecnologia, o próprio sistema vai analisar o banco de dados e cruzá-lo com imagens de pessoas na rua para emitir um alerta (FREITAS, 2022).

O setor privado também contribui em muito para a capilaridade do sistema de videomonitoramento de São Paulo. A Associação Brasileira de Empresas de Sistemas Eletrônicos de Segurança (Abese) afirma que a indústria fatura no Brasil R$ 9.2 bilhões por ano, grande parte desse valor referente à cidade de São Paulo, que conta com cerca 2.4 milhões de câmeras privadas (PAGNA, 2022). Essa infraestrutura de vigilância foi impulsionada nos últimos anos por programas como o *City Câmeras* e o *Detecta*, que visaram a integração do parque privado de câmeras com as salas de operação da polícia, além do uso de softwares de análise de vídeo para identificação de criminosos (PERON & ALVAREZ, 2021).

Os casos do Rio de Janeiro, da Bahia e de São Paulo servem para ilustrar um processo que tem dimensão nacional. Embora não haja um levantamento consolidado de todas as forças de segurança que fazem uso de TRFs, ainda em 2019, entidades da sociedade civil listavam prisões que partiram do reconhecimento facial no Ceará, na Paraíba, em Santa Catarina, em Minas Gerais, no Espírito Santo e no Distrito Federal (NUNES, 2019) (para um levantamento atualizado, ver capítulo 1).

A rápida expansão das TRFs entre as polícias brasileiras foi estimulada por uma série de fatores, que passam pela disseminação do uso de tecnologias digitais de uma forma geral, o que reduziu a resistência entre os agentes, e pelas melhorias nos próprios sistemas de identificação biométrica, que contam com mais bases de dados, algoritmos mais pre-

cisos e custos menores. Destaco aqui, no entanto, dois pontos centrais: o incentivo institucional por parte do governo federal e as demandas por formas mais eficazes e supostamente objetivas de controle social que partem de dentro das instituições policiais, mas também da sociedade civil.

O uso de TRFs em atividades de patrulhamento rotineiro e investigação policial ganhou mais atenção da administração federal após a publicação da portaria nº 793/2019 do Ministério da Justiça e Segurança Pública que regulamenta formas de incentivo financeiro para ações de "enfrentamento à criminalidade violenta" (BRASIL, 2019). A portaria prevê que recursos do Fundo Nacional de Segurança Pública devam ser destinados à disseminação de dispositivos de inteligência artificial, incluindo "o fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial" (BRASIL, 2019). Nessa mesma direção, a Polícia Federal (PF) implementou, em 2021, o sistema ABIS (Solução Automatizada de Identificação Biométrica). Este visa a unificação das bases de dados biométricos das secretarias de segurança de todo o país, podendo chegar ao armazenamento de registros faciais de até 200 milhões de pessoas. Para a PF, a construção de uma base biométrica nacional serve para organizar e integrar dados antes dispersos e coletados de forma pouco sistemática, o que auxiliaria na resolução de crimes, mas também na identificação de pessoas desaparecidas (POLÍCIA FEDERAL, 2021). Além disso, deputados federais passaram a designar emendas parlamentares para o investimento nessa tecnologia em seus estados. O delegado Waldir, deputado por Goiás, por exemplo, disponibilizou cerca de 30 milhões de reais do orçamento público federal para que cidades com menos de 4 mil habitantes e quase sem ocorrência de crimes violentos comprassem câmeras com reconhecimento facial (REBELLO, 2023).

Em termos de ganhos de eficácia e objetividade das políticas de controle da criminalidade, as TRFs são apresentadas como mecanismos para a redução de erros e injustiças cometidos através de identificação de

suspeitos pelo "faro policial" ou pelo reconhecimento fotográfico nas delegacias. Em outras palavras, entusiastas do uso de TRFs no âmbito da segurança pública não negam que estas são capazes de cometer erros, levando a abordagem de pessoas inocentes, mas apontam que os algoritmos têm desempenho muito superior ao olhar clínico de policiais, vítimas e testemunhas quando se trata de identificar suspeitos.

Diversas pesquisas apontam que o racismo é elemento definidor da seletividade penal no Brasil, onde negros têm maior chance de serem abordados, presos e mortos pela polícia (SINHORETTO et al., 2022). A discriminação racial está na base da construção dos perfis de risco que orientam as práticas de repressão, de modo que o "elemento suspeito" não difere do perfil de vítimas de homicídios apresentado acima. Essa constatação tem alimentado demandas por mudanças no processo de formação policial (incluindo, por exemplo, disciplinas de direitos humanos), mas também por novas estratégias de patrulhamento e novas tecnologias que possam reduzir a discricionariedade dos policiais e aumentar a supervisão sobre suas ações. Nessa perspectiva, ao direcionar as abordagens apenas para indivíduos com mandados de prisão em aberto, as TRFs diminuiriam os casos de abuso da polícia contra jovens negros.

O mesmo ocorreria com a substituição do reconhecimento de suspeitos nas delegacias por algoritmos de identificação biométrica. Os números comprovam que a prática de reconhecimento fotográfico tem sérios problemas. Em muitos casos, o inquérito policial é incapaz de levantar um conjunto de provas para sustentar pedidos de condenação e acaba se pautando exclusivamente no reconhecimento feito por vítimas ou testemunhas a partir de catálogos fotográficos. No entanto, preocupa a falibilidade desse método, que não tem regras claras para a construção das bases de dados (são usadas, por exemplo, fotos de redes sociais), que cataloga imagens de baixa qualidade e, em geral, que não segue as normas para o reconhecimento definidas no código penal (CASTRO, 2022). Entre 2012 e 2020, apenas no Rio de Janeiro, 73 pessoas inocentes foram

presas após erros de identificação fotográfica. Estas passaram, em média, 9 meses no cárcere (em alguns casos, inocentes passaram mais de dois anos presos) (FANTÁSTICO, 2021).

Indo além, se há críticas de que o reconhecimento algorítmico carrega vieses contra pessoas negras, os atuais sistemas de identificação podem ser ainda piores. Levantamento do Conselho Nacional de Defensores Públicos (CONDEGE) aponta que 83% dos casos de erros de identificação nas delegacias ocorrem com suspeitos negros (FANTÁSTICO, 2021). Entre outros problemas, a profusão de falsos positivos se dá pois muitos dos catálogos de suspeitos são alimentados com fotos de pessoas que passaram pelo sistema de justiça, mas acabaram inocentadas. A mera presença no catálogo aumenta as chances de uma nova prisão (há casos de jovens negros que foram presos nove vezes de forma equivocada), mesmo sem qualquer fundamento legal para a suspeição.

Observando esse cenário, o professor da Faculdade de Direito da USP, Floriano de Azevedo Marques Neto, por exemplo, aponta que as críticas às TRFs partem fundamentalmente de "ludistas", ou aqueles que se colocam de forma contrária a qualquer inovação no campo da segurança pública sem antes avaliar seu impacto e pesar os potenciais benefícios (NETO apud MENGUE, 2022a). Nessa perspectiva, os algoritmos não são apenas mais eficientes e tecnicamente superiores às análises realizadas por humanos, mas oferecem ferramentas de tomada de decisão que não dependem da discricionariedade individual. O pressuposto é que as câmeras veem sem inferência ou interpretação, de modo que a vigilância se despiria de qualquer normatividade e preconceito (PEREIRA & RAETZSCH, 2022).

Para os entusiastas, portanto, trata-se de uma tecnologia que não apenas reduz a violência, mas que ainda contribui para dirimir o histórico problema da discriminação racial na atividade policial. Assim, a sociedade e as autoridades deveriam se concentrar no aprimoramento técnico dos sistemas e dos procedimentos de uso por parte das polícias.

Racismo algorítmico e os riscos do vigilantismo

Em que pesem os argumentos listados acima, instituições voltadas para a proteção de direitos digitais e privacidade têm levantado preocupações acerca da implementação de TRFs no campo da segurança pública. Pesquisadores e ativistas argumentam que o uso dessa tecnologia, em geral, extrapola os objetivos legítimos de controle do crime. Há evidências, por exemplo, de protestos pacíficos sendo monitorados ou de operadores fazendo uso dos sistemas de videomonitoramento para atender a interesses pessoais (CARDOSO, 2015; GUARIGLIA, 2020). Além disso, a falta de avaliações de desempenho faz com as TRFs funcionem como ferramentas que discriminam contra negros e pessoas trans, seja pelos erros de identificação, seja pela escolha dos espaços em que as câmeras são instaladas. Por fim, os mecanismos externos de controle e supervisão são praticamente inexistentes. Ou seja, quando as forças de segurança implementam TRFs, é muito difícil para entidades da sociedade civil ou mesmo para outros órgãos do Estado entender a forma como os sistemas são usados e responsabilizar os culpados por seus potenciais prejuízos. Nessa seção, vou me debruçar especificamente sobre dois riscos inerentes ao uso de TRFs pelas forças de segurança: o "racismo algorítmico" e o "vigilantismo" (ou tecnoautoritarismo) (SILVA, 2021; VENTURINI et al., 2022).

O impacto de TRFs na automatização do racismo na prática policial

Kade Crockford (2020), especialista em tecnologias de vigilância da ACLU, argumenta que a identificação por biometria facial é uma "tecnologia distópica" para a população negra por dois motivos: os sistemas são enviesados, levando a uma taxa desigual de erros entre diferentes grupos populacionais, e as bases de dados com as quais são feitos os cruzamentos tem uma sobrerrepresentação de indivíduos negros.

As denúncias acerca dos erros cometidos por TRFs contra negros ganharam destaque após a publicação de um estudo de Joy Buolamwini e Timnit Gebru (2018). Segundo as autoras, os serviços de reconhecimento facial oferecidos pelas principais empresas do mercado, incluindo IBM, Microsoft e Face++, apresentavam erros de identificação que chegavam a 1% em casos de homens brancos, 12% em casos de homens negros e 35% em casos de mulheres negras. Após essa constatação, algumas empresas adotaram moratórias para a comercialização de seus produtos. Essas, no entanto, começam a ser suspensas com o argumento de que as TRFs têm se aperfeiçoado com o tempo. Nessa perspectiva, a produção de câmeras com mais definição, capacidade de armazenamento e processamento de dados faz com que os sistemas disponíveis no mercado tenham atingido melhores níveis de precisão, o que tornaria as críticas de Buolamwini & Gebru (2018) um problema do passado.

É importante, contudo, ponderar os argumentos sobre os avanços tecnológicos. Mesmo que os sistemas de identificação biométrica tenham melhorado, eles nunca chegarão a 100% de precisão. Trata-se de uma tecnologia que funciona por aferição probabilística, ou seja, um "*match*" perfeito entre a imagem capturada na rua e aquela armazenada no banco de dados é indicação de fraude (exatamente a mesma imagem foi usada na verificação de identidade). Além disso, mesmo 0.01% de erro pode representar um nível de falha com consequências sociais indesejáveis, seja pelo volume de rostos analisados todos os dias, seja por indicar uma total inoperância do sistema. No primeiro caso, podemos pensar nos usos correntes dessa tecnologia nas grandes cidades brasileiras. Se o dispositivo de vigilância capturar um milhão de rostos por dia (nas ruas, sistemas de transportes, entradas de espaços públicos etc.), uma taxa de erro de 0.01% indica que, em média, 100 pessoas sofrerão com abordagens equivocadas. No segundo caso, podemos pensar em um grande evento, como um festival de música, que chegue a 100 mil pessoas. Se dentro desse grupo existirem 10 homicidas procurados pela justiça criminal, o sistema de monitoramento pode

não identificar ninguém e ainda assim afirmar que possui acurácia de 99.99%.

O segundo ponto levantado por Crockford (2020) também merece atenção. Muitos departamentos de polícia constroem bancos de dados a partir de fotografias da face (*mugshots*) dos indivíduos abordados ou presos em flagrante (antes de qualquer julgamento), o que tende a levar à reprodução do padrão discriminatório do policiamento nas bases de dados. Como apontado anteriormente, há vasta evidência de que negros são presos em uma proporção maior que brancos pelos mesmos crimes (SINHORETTO et al., 2022). Por exemplo, as taxas de uso de maconha por populações negras e brancas é semelhante nos Estados Unidos, mas negros têm quatro vezes mais chances que brancos de serem presos por posse dessa droga (ACLU, 2020). Mesmo que os indivíduos sejam posteriormente liberados ou inocentados essas detenções acarretam no registro da ocorrência e no arquivamento da foto, que pode ser usada posteriormente na identificação de suspeitos. Há, portanto, o risco de vigilância desproporcional da população negra, exacerbando o racismo das políticas de segurança pública.

No Brasil, algumas instituições policiais se defendem dessa acusação afirmando que utilizam o banco de imagens do CNJ, no qual constam somente mandados de prisão em aberto. No entanto, os próprios policiais confirmam que essa base de dados tem problemas estruturais. Além de muitas fotos serem de baixa qualidade (o que diminui a precisão da identificação), são recorrentes os casos de erros de registro. Esse problema acarretou, por exemplo, na detenção de uma mulher no Rio de Janeiro em 2019. O sistema alertou que ela seria uma foragida da justiça, mas quando as informações foram checadas, verificou-se que a pessoa procurada já estava presa e que seu registro era mantido no banco do CNJ por um equívoco da justiça (ALBUQUERQUE, 2019).

De fato, os números apontam que TRFs tendem a reproduzir o viés racial do policiamento. Entre março e outubro de 2019, o primeiro ano de uso mais disseminado dessa tecnologia pelas forças de se-

gurança, dados da Rede de Observatórios de Segurança apontam que 151 pessoas foram detidas após a identificação biométrica automatizada. Destas, 90.5% eram negras (NUNES, 2019). Frente a esse cenário, Thiago Amparo (2020) reflete que: "Permitir ou não reconhecimento facial e, se sim, como fazê-lo está intrinsecamente ligado a uma outra questão: sobre quais ombros recai o estado policial? Informação é poder e, como todo poder, pode ser racializado e deve ser controlado".

Os riscos do vigilantismo

A Coalizão Direitos na Rede (2019, 2020), grupo que reúne mais de 50 organizações engajadas no debate sobre direitos digitais, tem sido ativa em denunciar os efeitos discriminatórios das TRFs e contextualizar sua disseminação em meio à ascensão do "tecnoautoritarismo".[5] Essas críticas ecoam posicionamentos anteriores de organizações da sociedade civil ao redor do mundo. Em 2019, por exemplo, 80 entidades assinaram uma carta em que pediam o banimento do uso de TRFs com o seguinte argumento:

> Reconhecimento facial é uma tecnologia especialmente invasiva e desumanizante que torna possível, cedo ou tarde, a vigilância constante do espaço público. Ela cria uma sociedade em que todos são suspeitos. Ela transforma nossos rostos em aparelhos de rastreio, ao invés de signos de personalidade, eventualmente reduzindo-os a objeto técnicos. [Em resumo], ela habilita um controle invisível (APC, 2019).

5 Segundo a Data Privacy Brasil e a LAUT (2021), *tecnoautoritarismo* pode ser definido como os "processos de expansão do poder estatal, por meio do uso de tecnologias de comunicação da informação de ponta, com o objetivo de incrementar as capacidades de vigilância e controle sobre a população, mediante violação de direitos individuais ou ampliação importante dos riscos de violação a direitos fundamentais. Práticas tecnoautoritárias ajudam a corroer por dentro os pilares de sustentação da democracia, criando estruturas aptas a aumentar a vigilância, repressão e supressão de exercícios de direitos".

O videomonitoramento tradicional já registra fluxos nos grandes centros urbanos, mas sistemas biométricos fazem com que todas as movimentações, hábitos e interações de um indivíduo possam ser documentadas e catalogadas sem qualquer esforço operacional. Não é necessário seguir um suspeito para flagrar atividades ilegais. Basta fazer uma pesquisa em um banco de dados para ter acesso a todas as imagens em que determinado indivíduo aparece. E esses registros não são possíveis apenas para alvos de investigação, mas estão disponíveis para absolutamente todos os cidadãos. Em questão de segundos, a polícia pode descobrir, por exemplo, todas as vezes em que uma pessoa foi a um bar, visitou amigos, chegou atrasada no trabalho, frequentou uma casa de prostituição, fumou na calçada, participou reuniões dos alcóolicos anônimos ou traiu seu parceiro conjugal. Ou seja, a vigilância biométrica carrega um potencial de controle ubíquo que pode transformar a natureza das interações sociais e constranger comportamentos individuais, sejam esses ilegais ou não.

Além disso, toda câmera com programas analíticos se torna um dispositivo de monitoramento ativo, avaliando o conteúdo das imagens em tempo-real em busca de padrões ou indivíduos que possam ser de interesse da polícia. Está em desenvolvimento portanto, uma nova infraestrutura de controle que não apenas expande as práticas anteriores, mas traz mudanças qualitativas. Se o sistema algorítmico julgar que há algum indício de anormalidade, alertas são disparados para as forças policiais, que vão avaliar a cena e decidir sobre a necessidade de intervenção. Esse cenário pode ser lido por um profissional do campo da segurança pública como um importante avanço, conferindo enormes ganhos de eficiência ao trabalho de investigação, diminuindo a impunidade e fazendo justiça para as vítimas. No entanto, essa capacidade de vigilância massiva e pervasiva tem potencial de eliminar a privacidade e impedir a concretização de direitos civis e políticos. Já seria um problema entregar essa tecnologia nas mãos de instituições transparentes e auditáveis. Mas quando falamos do sistema de justiça criminal, os riscos são ainda maiores.

As formas de repressão implementadas na China, em geral, são o exemplo levantado para ilustrar os possíveis abusos cometidos através de sistemas de TRFs por governos autoritários (MOZUR, 2019). No entanto, os problemas não se resumem à opressão com fins políticos. Diversas pesquisas indicam que quando os profissionais de segurança têm acesso às câmeras e bases de dados, essas ferramentas são usadas para interesses pessoais. Há casos de sistemas sendo direcionados para observar mulheres de biquini nas praias, para seguir cônjuges e identificar possíveis casos de adultério ou para verificar se os filhos falam a verdade quando afirmam que saem da escola direto para casa (SMITH, 2012; CARDOSO, 2014). Há evidências ainda de que grupos do crime organizado conseguem acesso aos sistemas de videomonitoramento da polícia para acompanhar a rotina de suas futuras vítimas (MARINATTO, 2023). Quando Edward Snowden abriu os arquivos da NSA, verificou-se que a massa de dados coletados não estava relacionada aos alvos da agência, como suspeitos de terrorismo. Muitas pessoas comuns foram vigiadas por terem alguma relação com os operadores. Os arquivos revelados por Snowden "contam histórias de amor e corações partidos, de relações sexuais ilícitas, de crises mentais, de conversões políticas e religiosas, de ansiedades financeiras e esperanças frustradas" (GELLMAN et al., 2014).

Como definem Woodrow Hartzog & Evan Selinger (2018), as forças policiais propagandeiam os aspectos positivos que realmente existem nos dispositivos de reconhecimento facial, mas a sociedade não pode ignorar que se trata de:

> Uma ferramenta irresistível de opressão e uma máquina de destruição total de privacidade perfeitamente adequada para governos que exercem controle autoritário sem precedentes... A mera existência de sistemas de reconhecimento facial, que são, em geral, invisíveis, causa danos para as liberdades civis, pois as pessoas vão agir de formas diferentes se suspeitarem que estão sendo vigiadas.

Conclusão

A introdução das TRFs na rotina policial tem levado a transformações significativas no trabalho de vigilância, o que, como vimos nesse capítulo, suscita enormes controvérsias. Há receios de que vieses nos erros de identificação biométrica contribuam para a automatização do racismo nas práticas de controle social. Além disso, o potencial de vigilância ubíqua representa um risco para a democracia e os direitos políticos. O alerta de Philip Agre (2003) há duas décadas permanece válido, TRFs "funcionam bem o suficiente para serem perigosas, e mal o suficiente para também serem perigosas".

No Brasil, a ausência de lei específica sobre o uso de marcadores biométricos para fins de segurança pública e defesa nacional contribui para um cenário de incerteza e aumenta as preocupações acerca de abusos. O limbo jurídico e a indefinição sobre regras e limites para o uso de TRFs são especialmente problemáticos por três motivos.

Em primeiro lugar, faltam padrões claros para coleta, armazenamento e processamento de dados pelas forças policiais. Estão em operação múltiplos sistemas de reconhecimento facial que se valem de diferentes bases, são empregados em diferentes funções e que raramente assumem modelos de avaliação e *accountability*. A falta de padrões claros para a implementação prejudica quem busca delimitar boas-práticas (i.e., como mitigar falsos positivos? Como desenvolver procedimentos operacionais para abordagens?), mas também impõe obstáculos para a troca de informações entre as instituições nacionais e parceiros estrangeiros (LEMOS et al, 2021).

Além disso, devido à ausência de lei específica, são fracas as diretrizes para a produção e implementação desses sistemas por parte das empresas que firmam contratos com as forças públicas. Não há regras gerais para verificação de precisão, não há determinações sobre a transparência dos algoritmos e mecanismos externos de controle. Do mesmo modo, também não há um regramento claro sobre a segurança dos da-

dos armazenados pelas instituições policiais, mas manuseados por parceiros privados. Quais são os limites para o compartilhamento? Como garantir que esses dados não serão usados para finalidades não previstas na LGPD?

Por fim, também não estão claros os limites que a privacidade impõe à vigilância biométrica. Os indivíduos têm direito de saber que seus dados estão sendo capturados? Há possibilidade de recusar esse olhar intrusivo? É possível saber quais dados estão armazenados? Como um cidadão pode apontar erros e exigir mudanças nos dados (como nos casos da base do CNJ)? Como se proteger de sistemas discriminatórios? Quando são presos a partir da identificação biométrica, os indivíduos e seus advogados devem ser informados disso? Podem ter acesso ao (ou contestar o) resultado do reconhecimento facial? Se muitas instituições policiais não identificam a discriminação racial como problema recorrente em suas operações, como esperar que elas atentem para a forma como esses sistemas amplificam o problema?

Os discursos acerca de soluções tecnológicas para a segurança pública são muito atrativos em uma sociedade marcada por altos índices de violência. No entanto, a promessa de uma justiça automática e absoluta esconde os múltiplos riscos inerentes às TRFs. A vigilância biométrica anuncia o fim da impunidade, mas aponta também para o fim do anonimato e da privacidade. Em última análise, caminhamos para substituição da presunção de inocência, que censura atividades de vigilância indiscriminadas, por uma lógica de controle ubíquo e preventivo. Como a ex-secretária de interior do Reino Unido, Amber Rudd (apud SLAUGHTER & HARE,2018), define, não somos mais inocentes, mas "pessoas [ainda] não-condenadas".

Referências

ACCESS NOW. *Surveillance Tech in Latin America: Made Abroad, Deployed at Home*. New York: Access Now, 2021.

ACLU. *A Tale of Two Countries: Racially Targeted Arrests in the Era of Marijuana Reform*. **ACLU** Research Report, 2020.

AGRE, P. "Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places", 2003. Disponível em: https://pages.gseis.ucla.edu/faculty/agre/bar-code.html (acesso em 14 de março de 2023)

ALBUQUERQUE, A. "Em fase de testes, reconhecimento facial no Rio falha no 2º dia". *Folha de São Paulo*, 17 de julho de 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/07/em-fase-de-testes-reconhecimento-facial-no-rio-falha-no-20-dia.shtml (acesso em 21 de março de 2023)

AMPARO, T. "Polícia algorítmica". *Folha de São Paulo*, 27 de janeiro de 2020. Disponível em: https://www1.folha.uol.com.br/colunas/thiago-amparo/2020/01/policia-algoritmica.shtml (acesso em 13 de março de 2023)

APC. *Joint letter: Ban security and surveillance facial recognition*, 2019. Disponível em: https://www.apc.org/en/pubs/joint-letter-ban-security-and-surveillance-facial-recognition

ARAÚJO, V. "Carros da **PM** terão câmeras para identificar suspeitos na rua". *O Globo*, 13 de março de 2023. Disponível em: https://oglobo.globo.com/rio/noticia/2023/03/carros-da-pm-terao-cameras-para-identificar-suspeitos-na-rua.ghtml (acesso em 13 de março de 2023)

BAHIA. "Reconhecimento Facial chega a marca de 600 foragidos localizados e presos". *Governo do Estado da Bahia*, 25 de janeiro de 2023. Disponível em: https://www.bahia.ba.gov.br/2023/01/noticias/seguranca/reconhecimento-facial-chega-a-marca-de-600-foragidos-localizados-e-presos/ (acesso em 02 de março de 2023)

BRASIL. Portaria nº 793, de 25 de outubro de 2019. *Ministério da Justiça e da Segurança Pública.* Diário Oficial da União, Brasília, **DF**, edição 208, seção 1, p.55. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575 (acesso em 20 de março de 2023)

BUOLAMWINI, J. & **GEBRU**, T. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification". *Proceedings of Machine Learning Research*, no. 81, pp. 1-15, 2018.

CARDOSO, B. "A lógica gerencial-militarizada e a segurança pública no Rio de Janeiro: O **CICC-RJ** e as tecnologias de (re)construção do Estado. *Dilemas*, v. 12, especial 3, pp. 53-74, 2019.

CARDOSO, B. *Todos os Olhos: Videovigilâncias, Voyeurismo e (re)produção Imagética*. Rio de Janeiro: Editora **UFRJ**, 2015.

CASTRO, C. "Polícia do RJ impõe inferno judicial a negros inocentes incluídos em álbum de suspeitos". *The Intercept*, 4 de abril de 2022. Disponível em: https://theintercept.com/2022/04/04/negros-inocentes-album-de-suspeitos-rj/ (acesso em 16 de março de 2023)

CAXIAS. "Centro Integrado de Comando e Controle da Baixada Fluminense é aposta para melhorar índices de segurança". *Extra*, 27 de janeiro de 2023. Disponível em: https://extra.globo.com/noticias/centro-integrado-de-comando-controle-da-baixada-fluminense-aposta-para-melhorar-indices-de-seguranca-25651081.html (acesso em 16 de março de 2023)

CERQUEIRA, D. "Causas e consequências do crime no Brasil". Tese de doutorado, Departamento de Economia. Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro, 2014.

COALIZÃO DIREITOS NA REDE. *Open letter from Brazilian civil society on the occasion of the 15th edition of the United Nations Internet Governance Forum*, 2020. Disponível em: https://direitosnarede.org.br/2020/11/17/open-letter-from-brazilian-civil-society-on-the-occasion-of-the-15th-edition-of-the-united-nations-internet-governance-forum/

COALIZÃO DIREITOS NA REDE. *Open letter from representatives of Brazilian civil society facing threats to the democratic, free and open internet in Brazil*, 2019. Disponível em: https://direitosnarede.org.br/2019/11/27/igf-2019-open-letter/

COELHO, H. "Cidade Integrada: estudo estima custo de projeto de câmeras no entorno do Jacarezinho em R$ 164 mil mensais". *G1.Globo.com*, 29 de março de 2022. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2022/03/29/cidade-integrada-estudo-estima-custo-projeto-cameras-entorno-jacarezinho.ghtml (acesso em 13 de março de 2023)

CROCKFORD, K. "How is Face Recognition Surveillance Technology Racist?" *ACLU*, 16 de junho de 2020. Disponível em: https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist (acesso em 20 de março de 2023)

DATA PRIVACY BRAZIL & LAUT. Retrospectiva Tecnoautoritarismo — 2020, 2021. Disponível em: https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/

EDLER, D. "Sistemas de reconhecimento facial e seus usos no campo da segurança pública no Brasil". *Cadernos Adenauer*, v. 22, no. 4, pp. 27-48, 2021.

FALCÃO, C. "Lentes Racistas". *The Intercept*, 20 de setembro de 2021. Disponível em: https://theintercept.com/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/ (acesso em 02 de março de 2023)

FANTÁSTICO. "Câmeras de reconhecimento facial flagraram e prenderam 77 foragidos da Justiça no carnaval da Bahia". *Fantástico*, 26 de fevereiro de 2023. Disponível em: https://globoplay.globo.com/v/11402252/ (acesso em 02 de março de 2023)

FANTÁSTICO. "Exclusivo: 83% dos presos injustamente por reconhecimento fotográfico no Brasil são negros". *G1.globo.com*, 21 de fevereiro de 2021. Disponível em: https://g1.globo.com/fantastico/noticia/2021/02/21/exclusivo-83percent-dos-presos-injustamente-por-reconhecimento-fotografico-no-brasil-sao-negros.ghtml (acesso em 10 de março de 2023)

FBSP. *A frágil redução das mortes violentas intencionais no Brasil.* São Paulo: Fórum Brasileiro de Segurança Pública, 2022.

FBSP. *Anuário Brasileiro de Segurança Pública*. São Paulo: Fórum Brasileiro de Segurança Pública, 2023.

FREITAS, H. "Câmeras de reconhecimento facial se multiplicam em São Paulo". *VEJA*, 08 de dezembro de 2022. Disponível em: https://vejasp.abril.com.br/cidades/cameras-reconhecimento-facial-sp/ (acesso em 02 de março de 2023)

GARLAND, D. *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford: Oxford University Press, 2001.

GELLMAN, B., **TATE**, J. & **SOLTANI**, A, "In NSA-intercepted data, those not target far outnumber the foreigners who are". *The Washington Post*, 5 de julho de 2014. Disponível em: https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html (acesso em 21 de março de 2023)

GOOLD, B., **LOADER**, I. & **THUMALA**, A. "The Banality of Security: The Curious Case of Surveillance Cameras". *British Journal of Criminology*, v. 53, no. 6, pp. 977-996, 2013.

GOULART, G. "Câmeras com inteligência artificial fazem índices de criminalidade despencarem em Niterói". *O Globo*, 23 de outubro de 2019. Disponível em: https://oglobo.globo.com/rio/cameras-com-inteligencia-artificial-fazem-indices-de-criminalidade-despencarem-em-niteroi-1-24036335 (acesso em 16 de março de 2023)

GRAY, M. "Urban Surveillance and Panopticism: will we recognize the facial recognition society?" *Surveillance & Society*, v. 1, no. 3, pp. 314-330, 2003.

GUARIGLIA, M. "High Tech Police Surveillance of Protests and Activism". *Electronic Frontier Foundation*, 25 de dezembro de 2020. Disponível em: https://www.eff.org/deeplinks/2020/12/high-tech-police-surveillance-protests-and-activism-year-review-2020 (acesso em 20 de março de 2023)

HARTZOG, W. & **SELINGER**, E. "Facial Recognition Is the Perfect Tool for Oppression". *Medium*, 02 de agosto de 2018 Disponível em: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 (acesso em 21 de março de 2023)

INSTITUTO IGARAPÉ *Reconhecimento facial no Brasil*. Rio de Janeiro, 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/ (acesso em 15 de março de 2023)

LEMOS, A., **FERNANDES**, E., **MEDEIROS**, J., **GUEDES**, P. & **SILVA**, P. *Comentários ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública: Tecnologia de Reconhecimento Facial*. Rio de Janeiro, **ITS**, 2021.

MARINATTO, L. "Membros de facção que planejavam ataque contra Moro tinham acesso a sistema de monitoramento do governo de **SP**, diz **PF**". *O Globo*, 23 de março de 2023. Disponível em: https://oglobo.globo.com/politica/noticia/2023/03/membros-de-faccao-que-planejavam-ataque-contra-moro-tinham-acesso-a-sistema-de-monitoramento-do-governo-de-sp-diz-pf.ghtml (acesso em 13 de março de 2023)

MENGUE, P. "Reconhecimento facial é criticado e até proibido no exterior; veja argumentos a favor e contra". *O Estado de São Paulo*, 01 de setembro de 2022a. Disponível em: https://www.estadao.com.br/brasil/reconhecimento-facial-e-criticado-e-ate-proibido-no-exterior-veja-argumentos-favoraveis-e-contra/ (acesso em 13 de março de 2023)

MENGUE, P. "Reconhecimento facial: após críticas, cidade de **SP** suspende temporariamente programa com câmeras". *O Estado de São Paulo*, 03 de dezembro de 2022b. Disponível em: https://www.estadao.com.br/sao-paulo/reconhecimento-facial-apos-criticas-cidade-de-sp-suspende-temporariamente-programa-com-cameras/ (acesso em 13 de março de 2023)

MOZUR, P. "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority". *The New York Times*, 14 de abril de 2019. Disponível em: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html (acesso em 20 de março de 2023)

NUNES, P. "Exclusivo: levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros". *The Intercept*, 21 de novembro de 2019. Disponível em: https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/ (acesso em 16 de março de 2023)

NUNES, P.; **SILVA**, M. & **OLIVEIRA**, S. *Um Rio de olhos seletivos: uso de reconhecimento facial pela polícia fluminense*. Rio de Janeiro: **CESeC**, 2022.

PAGNAN, R. "Torres de segurança usam inteligência artificial para alertar crimes em **SP**". *Folha de São Paulo*, 01 e junho de 2022. Disponível em: https://www1.folha.uol.com.br/mercado/2022/06/startup-de-seguranca-privada-abre-mercado-em-sp-com-alertas-de-moto-na-calcada-a-bike-na-contramao.shtml (acesso em 02 de março de 2023)

PEREIRA, G. & **RAETZSCH**, C. "From Banal Surveillance to Function Creep: Automated License Plate Recognition (**ALPR**) in Denmark". *Surveillance & Society*, v. 20, no. 3, pp. 265-280, 2022.

PERON, A; **ALVAREZ**, M. "O Governo da Segurança: Modelos Securitários Transnacionais e Tecnologias de Vigilância na Cidade de São Paulo". *Lua Nova*, v. 114, pp. 175-212, 2021.

PETRÓPOLIS (2019) "Petrópolis inicia uso de câmera com reconhecimento facial". *Prefeitura de Petrópolis*, 02 de outubro de 2019. Disponível em: https://www.petropolis.rj.gov.br/pmp/index.php/imprensa/noticias/item/14478-petr%C3%B3polis-inicia-uso-de-c%C3%A2mera-com-reconhecimento-facial.html (acesso em 16 de março de 2023)

POLÍCIA FEDERAL. "Polícia Federal implementa nova Solução Automatizada de Identificação Biométrica". *Gov.br*, 30 de junho de 2021. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica (acesso em 16 de março de 2023)

PRATT, J. *Penal populism* Londres: Routledge, 2007.

REBELLO, A. "O Mecenas". *The Intercept Brasil*, 05 de abril de 2023. Disponível em: https://www.intercept.com.br/2023/04/05/delegado-waldir-torrou-r-30-milhoes-em-reconhecimento-facial-para-cidades-que-sequer-tem-saneamento-em-goias/ (acesso em 05 de abril de 2023)

REIS, C., **ALMEIDA**, E., **DOURADO**, F. & **SILVA**, F. "Vigilância automatizada: uso de reconhecimento facial pela Administração Pública no Brasil". *LAPIN*, 2021. Disponível em: https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/ (acesso em 03 de março de 2023)

SILVA, M. & **VARON**, J. *Reconhecimento facial no setor público e identidades trans: Tecnopolíticas de controle e ameaça à diversidade de gênero em suas interseccionalidades de raça, classe e território*. São Paulo: Coding Rights, 2021.

SILVA, T. *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais*. São Paulo: Edições **SESC**, 2021.

SINHORETTO, J., **CEDRO**, A. & **MACEDO**, H. "New Technologies and Racism in Ostensive Policing in São Paulo". *Dilemas: Revista de Estudos de Conflito e Controle Social*, v. 15, no. 3, pp. 803-826, 2022.

SISDEPEN. "Segundo Levantamento do Depen, as vagas no sistema penitenciário aumentaram 7,4%, enquanto a população prisional permaneceu estável, sem aumento significativo". *Ministério da Justiça e Segurança Pública*, 04 de novembro de 2022. Disponível em: https://www.gov.br/depen/pt-br/assuntos/noticias/segundo-levantamento-do-depen-as-vagas-no-sistema-penitenciario-aumentaram-7-4-enquanto-a-populacao-prisional-permaneceu-estavel-sem-aumento-significativo (acesso em 14 de março de 2023)

SLAUGHTER, A.M. & **HARE**, S. "Our Bodies or Ourselves". *Project Sydicate*, 23 de julho de 2018. Disponível em: https://www.project-syndicate.org/commentary/dangers-of-biometric-data-by-anne-marie-slaughter-and-stephanie-hare-2018-07 (acesso em 22 de março de 2023)

SMITH, G. "Surveillance Work(ers)". In: Ball, K; Haggerty, K; and Lyon, D. (eds.) *Routledge Handbook of Surveillance Studies*. Abingdon, Oxon: Routledge, pp. 107-115, 2012.

STANLEY, J. "The Dawn of Robot Surveillance: **AI**, Video Analytics, and Privacy". *American Civil Liberties Union*, 2019.

VENTURINI, A. C.; **ANSEL**, P.; **BARRETO**, M.S.; **OLIVEIRA**, Y.M.; **ROSA**, A. S. *Vigilância & vigilantismo: conceitos, legislação brasileira e organizações atuantes*. São Paulo. Centro de Análise da Liberdade e do Autoritarismo (**LAUT**), 2022.

WACQUANT, L. *Punir os pobres: a nova gestão da miséria nos Estados Unidos*. Rio de Janeiro: Revan, 2003.

O uso do reconhecimento facial pelo setor privado: alternativas regulatórias em debate

Bárbara Simão

Resumo

Este capítulo tem o objetivo de sistematizar o debate quanto à regulação do reconhecimento facial no setor privado e localizar o contexto brasileiro no cenário global de discussão sobre o tema. São abordados, em um primeiro momento, os usos mais frequentes do reconhecimento facial pelo setor privado, assim como dois casos de contestação da tecnologia: o caso ViaQuatro, no metrô de São Paulo, e o caso Clearview AI. Em um segundo momento, o capítulo volta-se para o atual estado de propostas regulatórias para o uso do reconhecimento facial, examinando discussões hoje existentes nos EUA, União Europeia e Brasil. Percebe-se que as perspectivas regulatórias variam desde a possibilidade de autorregulação do mercado, até a possibilidade de medidas mais duras, como a vedação a determinados usos da tecnologia. A discussão sobre os usos em âmbito privado da tecnologia aparece de maneira mais residual em projetos de lei específicos sobre o tema. Destaca-se, também, intersecção importante da discussão sobre o reconhecimento facial com a regulação de sistemas de inteligência artificial, em que tem ganhado tração uma abordagem regulatória baseada no risco desses sistemas.

Introdução

O setor privado possui papel indissociável do âmbito do desenvolvimento e aplicação de tecnologias de reconhecimento facial. Empresas têm sido grandes responsáveis pelo investimento em pesquisa para aprimoramento de ferramentas de aprendizagem de máquina que aumentem a capacidade técnica da tecnologia. É, também, por meio da aplicação comercial que o uso do reconhecimento facial tem se expandido pelas mais diferentes vertentes, seja para fins de *marketing* e classificação de grupos de usuários interessados por uma propaganda, seja para fins de segurança e prevenção a fraudes no âmbito de sistemas internos de um aplicativo.

Pesquisas de mercado mostram que a renda gerada pelo mercado de reconhecimento facial, nos EUA, foi de U$3 a U$5 bilhões de dólares entre 2016 e 2019. Para os próximos anos, a expectativa do setor é que o crescimento dobre até 2024, com renda projetada entre U$7 e U$10 bilhões (LAMBERT, 2021, p. 57). Trata-se, assim, de uma tecnologia em rápida expansão e que acumula investimentos. As razões para tanto, ao menos econômicas, relacionam-se ao aumento de eficácia e diminuição do custo da tecnologia, o que fez com que mais interessados fossem capazes de adquiri-la. O setor financeiro também ampliou o uso do reconhecimento facial após normas regulatórias editadas pela União Europeia para sistemas de pagamentos, que exigem critérios de autenticação mais fortes (Idem, 2021, p. 58).

As possibilidades são diversas e o rápido avanço e expansão da tecnologia também têm levantado preocupação. Desde que passou a ser disseminada por sistemas operacionais de celular, aplicativos, lojas físicas e espaços públicos, grupos da sociedade civil têm questionado a aplicação do reconhecimento facial por conta de seus possíveis riscos e impactos negativos sobre a população, em especial sobre grupos historicamente minorizados como pessoas negras, mulheres e LGBTQIA+ (ver capítulos 1 e 5).

Diante desse cenário, o debate sobre a regulamentação do uso do reconhecimento facial torna-se premente. Autoridades do sul ao norte global têm questionado a aplicação da tecnologia e até decidido contrariamente ao uso em determinados contextos, como em ambientes escolares ou para fins de segurança pública e persecução penal. Algumas soluções provisórias, como imposição de moratória ao uso desses sistemas, também têm aparecido e permeado o debate público. Neste prisma, há propostas que vão desde a autorregulação do mercado até pedidos de banimento da tecnologia (ver capítulos 5 e 6).

Este capítulo possui, então, o objetivo de sistematizar as atuais contribuições desse debate e localizar o contexto brasileiro no cenário global de discussão sobre o tema. Para tanto, serão abordados, em um primeiro momento, os usos mais frequentes do reconhecimento facial pelo setor privado, assim como as disputas e questionamentos feitos em torno de sua utilização. Serão narrados dois casos de contestação da tecnologia: o caso ViaQuatro, de utilização de sistema de reconhecimento de emoções pela concessionária da linha amarela do metrô de São Paulo, e o caso Clearview AI, em que se contestou a empresa responsável pelo desenvolvimento de aplicativo capaz de localizar pessoas com base em seus registros de imagem. Em um segundo momento, o artigo irá voltar-se para o atual estado de propostas regulatórias para o uso do reconhecimento facial, examinando discussões hoje existentes nos EUA e União Europeia, buscando localizar também o atual contexto brasileiro nesse debate.

Usos e disputas relacionadas a aplicações privadas do reconhecimento facial

Definida como uma forma de inteligência artificial que envolve a identificação automatizada de um rosto, avaliando a distribuição de seus atributos espaciais e geométricos (LI; JAIN, 2011), pode-se dizer que o reconhecimento facial possui, em geral, três macro objetivos: categorizar, verificar ou identificar uma pessoa (SIMÃO; FRAGOSO; ROBERTO,

2020). No primeiro caso, o que se pretende pela ferramenta é que ela seja capaz de atribuir características a um rosto, sejam elas demográficas (por exemplo, afirmar se a pessoa em questão é do gênero feminino, masculino, ou sua idade), sejam elas comportamentais (tais como o reconhecimento de emoções expressadas pela pessoa – se triste, feliz ou com raiva, dentre outras possibilidades), ou sejam até mesmo de condições físicas (como a atribuição de temperatura corporal e mensuração de frequência de batimentos cardíacos).

Indo além, o reconhecimento facial também possibilita a verificação ou identificação de uma pessoa. Isto é, verificar se alguém é realmente quem afirma ser (por meio da comparação entre imagem registrada no banco de dados e imagem que se busca verificar) ou identificar quem é uma pessoa dentre as muitas que podem passar em frente à ferramenta (por meio da comparação entre a imagem em tempo real e bancos de dados com fotos de diversas pessoas) (ver introdução).

No âmbito privado, o reconhecimento de emoções e a atribuição de características demográficas têm sido frequentemente utilizados para fins de *marketing* e perfilamento de consumidores, isto é, para verificação de suas reações diante de uma propaganda ou de um produto. A Hering, por exemplo, anunciou tecnologia do tipo em loja conceito da marca, que identificava se uma pessoa ficava "satisfeita" com a roupa que era sugerida a ela (GUIMARÃES, 2023). Outros usos desse tipo de tecnologia se aplicam para a determinação de padrões de comportamento – algumas empresas, inclusive, afirmam conseguir detectar "comportamentos suspeitos". É o caso, por exemplo, da empresa britânica WeSee,[1] que afirma ser capaz de detectar comportamentos suspeitos de indivíduos por meio da leitura dos sinais faciais de um indivíduo, afirmando até mesmo a possibilidade de alertar ameaças terroristas (DANIEL, 2018).

O discurso relativo à segurança, de fato, permeia o uso de grande parte dessas iniciativas. O reconhecimento facial tem sido implementa-

1 Ver: https://www.wesee.com/#app. Acesso em 13. Mar. 2023.

do para prevenção a fraudes e acessos indevidos em sistemas ou dispositivos eletrônicos, como aplicativos de bancos ou sistemas financeiros. Redes sociais também têm se utilizado da ferramenta para identificação de pessoas marcadas em uma foto. Em escolas, o reconhecimento facial também tem sido utilizado para verificação de presença de alunos e, de acordo com gestores públicos, otimização da gestão escolar (TAVARES et al., 2023). Há também usos do reconhecimento facial com propósitos relacionados à saúde, que se tornaram mais recorrentes ao longo da pandemia de Covid-19: é o caso de câmeras que verificavam a adequada utilização de máscaras em um ambiente (YAN, 2020).

Considerando-se as possibilidades de uso, o reconhecimento facial hoje possui implicações potenciais sobre o exercício de direitos. Caso seja mal utilizada, essa tecnologia pode alimentar práticas de vigilância, bem como viabilizar práticas abusivas, discriminação e invasão de privacidade. Nesse sentido, uma importante dimensão do risco do reconhecimento facial diz respeito ao seu uso discriminatório. Sendo tais sistemas baseados em algoritmos de *machine learning* – capazes de identificar padrões em bases de dados – quaisquer problemas ou tendências nos dados usados para treinar o sistema serão reproduzidos em seus resultados. Estudos têm mostrado que a taxa de erro dessas ferramentas é sistematicamente maior para mulheres negras em comparação a outros grupos, por exemplo (BUOLAMWINI; GEBRU, 2018). Além disso, a tecnologia de reconhecimento facial utilizada para reconhecer emoções ainda possui outros problemas de acurácia. Como será visto adiante, seu funcionamento é baseado em fundamentos científicos contestados, muitas vezes falhando em fornecer resultados precisos.

A dificuldade em se obter resultados confiáveis por parte da tecnologia pode apresentar um risco caso tais sistemas sejam utilizados como critérios de acesso de usuários ao exercício de direitos. Consequentemente, levanta preocupação a interação entre as empresas privadas desenvolvedoras desses sistemas e o poder público, seja no caso de uma aplicação desenvolvida diretamente no âmbito da prestação de

um serviço público, seja no caso de pedidos de acesso a dados por parte de autoridades policiais em uma investigação criminal. Nesses casos, falsos positivos também podem levar a buscas e prisões ilegais, violando direitos fundamentais dos cidadãos (ver capítulos 1 e 2).

Diante da expansão da tecnologia e das controvérsias relacionadas a seu uso, organizações de defesa de direitos humanos e consumeristas passaram a questionar a utilização do sistema em alguns casos. Uma discussão sobre a regulamentação do reconhecimento facial também se iniciou ao redor do mundo, com campanhas da sociedade civil e iniciativas de banimento ou moratória da tecnologia por parte do poder público de determinadas cidades e estados. Nas próximas seções, serão descritos alguns desses casos de disputa em relação ao reconhecimento facial, descrevendo-se as controvérsias em jogo e o atual estado da discussão regulatória sobre o tema.

O caso ViaQuatro e a controvérsia sobre a inferência de características demográficas e emoções

Em 2018, a ViaQuatro – concessionária da linha amarela do metrô de São Paulo – anunciou a instalação de "portas interativas digitais", desenvolvidas pela empresa AdMobilize, nas plataformas de acesso aos trens das estações, capazes de reconhecerem a quantidade de pessoas que olhariam para a tela e de identificarem suas reações emocionais, gênero e faixa etária. De acordo com a empresa, a tecnologia possibilitaria a produção de relatórios estatísticos sobre as pessoas que frequentavam as dependências do metrô, afirmando se elas estariam com aparência feliz, insatisfeita, surpresa ou neutra.

O anúncio chamou a atenção do Instituto Brasileiro de Defesa do Consumidor (Idec), que, em agosto do mesmo ano, ingressou com Ação Civil Pública questionando a adoção da tecnologia. O Instituto questionou o uso do reconhecimento facial sem informação ou consentimento, alegando tratar-se de pesquisa de opinião compulsória, o que

seria prática abusiva de acordo com o Código de Defesa do Consumidor e do Código de Defesa dos Usuários de Serviços Públicos.[2] A ação citou, também, violação à Lei Geral de Proteção de Dados (LGPD), que havia acabado de ser aprovada no Congresso quando a ação foi proposta, embora ainda não estivesse em vigor à época. A empresa alegou, em sua defesa, não realizar reconhecimento facial, mas detecção facial, afirmando que os dados estariam anonimizados desde a origem e que, portanto, não haveria coleta de dados pessoais ou violação de direitos consumeristas ou à privacidade no caso.

A ação relacionada à ViaQuatro foi o primeiro grande caso sobre o uso de reconhecimento facial no Brasil, e chama atenção por suas particularidades. Primeiro, pela parceria público-privada envolvida na aquisição da tecnologia e implicações quanto ao uso de reconhecimento facial em espaços públicos, mesmo que não direcionados ao fim de segurança pública ou persecução penal. Segundo, pelo embate em torno das possibilidades e limites éticos (e técnicos) do reconhecimento de emoções: poderia o reconhecimento de emoções ser considerado reconhecimento facial? Há embasamento científico que dê respaldo à atividade? Em que o reconhecimento de emoções se diferenciaria da detecção facial? Quais seriam os impactos e riscos próprios à atividade?

Diversos pareceres dedicados ao exame dessas questões foram anexados à ação: de um lado, a ViaQuatro apresentava laudos afirmando que o sistema não geraria riscos à privacidade e reforçando que ele não poderia ser considerado, de fato, reconhecimento facial; de outro, o Idec reafirmava o argumento de que o reconhecimento de emoções seria um tipo de reconhecimento facial, e que, de toda maneira, ainda se trataria de prática abusiva por violação ao princípio da informação, predominante nas relações de consumo. O Instituto Alana ingressou na ação como *Amicus Curiae*, argumentando violação aos direitos de crianças e

2 Ver: MEDEIROS, H. Idec entra com ação judicial contra ViaQuatro por coleta indevida de dados. **Mobile Time**, 31 ago. 2018.

adolescentes.[3] Já o Instituto de Referência em Internet e Sociedade (Iris) colaborou com parecer técnico em que se debruçou sobre a questão da possibilidade de anonimização dos dados (TEOFILO et al., 2019).

Em parecer apresentado ao caso, a organização americana Access Now criticou a premissa da tecnologia do reconhecimento de emoções alegando que não haveria lastro científico para tanto. Ademais, a inferência de gênero também seria problemática, assumindo uma concepção binária de gênero com base na detecção de certas características físicas, como tamanho da mandíbula, maçãs do rosto e testa, que seriam associadas a um gênero masculino ou feminino. Tal concepção sugeriria que determinadas características físicas seriam correspondentes a identidades de gênero específicas, o que reforçaria discriminação contra pessoas trans e não binárias.

De fato, a possibilidade de uma tecnologia ser capaz ou não de reconhecer uma emoção humana é objeto de controvérsia pela literatura científica especializada. A maior parte do desenvolvimento de tecnologias de reconhecimento de emoções fundamenta-se na "teoria das emoções básicas", desenvolvida nos anos 1960 pelo psicólogo Paul Ekman, que defendeu que todos os seres humanos exibiriam o mesmo conjunto de seis emoções universais: medo, raiva, alegria, tristeza, desgosto e surpresa. Uma categoria emocional poderia ser inferida de um conjunto típico de movimentos faciais – um "protótipo". O estado de raiva, por exemplo, poderia ser afirmado por um protótipo que incluiria a sobrancelha franzida, os olhos arregalados e os olhos apertados. Esta seria uma configuração facial "ideal" que traduziria o estado emocional da raiva, tal qual uma impressão digital poderia ser utilizada para reconhecer uma pessoa (BARRETT *et al.*, 2019).

3 Ver: INSTITUTO Alana é contrário à coleta de dados biométricos de crianças. **Migalhas**, 24 maio 2019. Disponível em: <https://www.migalhas.com.br/quentes/303068/instituto-alana-e-contrario-a-coleta-de-dados-biometricos-de-criancas-pela-viaquatro>. Acesso em 22 de fevereiro de 2023.

Outra corrente científica, no entanto, contesta essa visão alegando que expressões de uma mesma categoria emocional podem variar substancialmente entre diferentes pessoas, culturas e situações. Em revisão sistemática de literatura, Barrett *et al* (2019) encontraram poucas evidências que dessem apoio à teoria das emoções básicas, alegando que a maior parte dos resultados positivos nesse sentido ocorriam quando o participante do estudo era orientado a se portar de acordo com uma emoção indicada ou com um cenário descrito, o que desafiaria a possibilidade de classificação diante de emoções verdadeiramente espontâneas. De acordo com o estudo, "uma descrição mais precisa (...) seria que a tecnologia detecta movimentos faciais, não expressões emocionais" (BARRETT *et al.*, 2019, p. 47). Em entrevista recente, o próprio Paul Ekman alegou que técnicas atuais de inferência de emoções carecem de respaldo científico e que "simplesmente medir a face não demonstra se a interpretação sobre ela está correta ou incorreta" (*apud* MURGIA, 2021).

Sendo assim, o reconhecimento que tem o objetivo de inferir emoções ou categorizar pessoas a partir de suas características físicas é permeado por controvérsias que partem desde a premissa científica das ferramentas, até os efeitos possivelmente discriminatórios das inferências feitas quanto a gênero, raça, idade, dentre outras possíveis categorias. Nesse sentido, há estudos que demonstram vieses discriminatórios da tecnologia com relação a pessoas negras – Lauren Rhue (2018) evidenciou que homens negros eram sistematicamente considerados como mais "raivosos" por tecnologias de inferência de emoções, em comparação a homens brancos.

O caso ViaQuatro ainda segue em andamento. Hoje, encontra-se em sede de recurso, após decisão de 1ª instância que concedeu ganho de causa ao Idec e condenou a empresa ao pagamento de danos coletivos no valor de R$100 mil.[4]

4 Até a data de finalização do artigo, em março de 2023.

O caso Clearview AI: raspagem de dados e cooperação com autoridades de investigação

Em janeiro de 2020, o jornal *The New York Times* publicou reportagem em que descreve as atividades da Clearview AI, empresa que desenvolveu um aplicativo de reconhecimento facial capaz de, a partir da foto de uma pessoa, indicar outras fotos públicas daquela pessoa, bem como indicação dos locais onde essas fotos foram publicadas. De acordo com a empresa, um banco de dados com mais de três bilhões de imagens teria sido construído a partir da extração de dados de sites como Facebook, Youtube, entre outros.

Chamou atenção, também, a interação da empresa com delegacias policiais. Elas estariam se utilizando dos seus serviços, sem escrutínio público, para a identificação e resolução de casos de furtos, roubos de identidade, fraudes com cartões de crédito, homicídios e exploração sexual infantil. De acordo com a empresa, mais de 600 delegacias em todo o mundo teriam se utilizado de seus serviços quando a reportagem foi divulgada.

A prática levantou preocupações com relação à privacidade dos indivíduos e gerou questionamentos sobre a legalidade das operações da empresa. Em primeiro lugar, em relação aos métodos de coleta de dados empregados pela empresa. As imagens utilizadas para o treinamento do software da Clearview AI foram obtidas de forma automatizada, sem que houvesse o consentimento prévio dos indivíduos retratados nas fotografias. Outro ponto é referente à precisão da tecnologia e à interação com órgãos de investigação criminal, questionando-se o fato de que o uso da tecnologia de reconhecimento facial poderia resultar em prisões falsas e condenações injustas.

Em resposta à controvérsia, a empresa foi denunciada e investigada em diversas jurisdições. Autoridades de proteção de dados da Itália, França, Austrália, Canadá, Alemanha e Reino Unido multaram a em-

presa por violação à legislação.[5] Todas as autoridades relataram violação aos princípios de legalidade e transparência, afirmando que a empresa não possuiria base legal válida para o tratamento de dados sensíveis, nem razão que justificasse a coleta de dados biométricos sem consentimento ou garantia de informação aos usuários. Também se criticou a ausência de prazos para retenção dos dados, bem como a ausência de procedimentos em prática para a resposta a direitos de titulares de dados, como possibilidade de acesso às informações disponíveis e solicitação de exclusão.

Nos Estados Unidos, apesar da falta de legislação federal sobre o tema, a empresa enfrentou ação proposta pela União Americana pelas Liberdades Civis (ACLU), com base na Lei de Privacidade de Informações Biométricas de Illinois (BIPA). O processo alegava que a Clearview AI coletou e armazenou ilegalmente dados biométricos de residentes do estado sem o seu consentimento. Em maio de 2022, a empresa firmou acordo para excluir todos os dados biométricos de residentes de Illinois que havia coletado, exceto os dados pertencentes às agências policiais. A empresa também concordou em parar de coletar dados biométricos de residentes de Illinois, a menos que obtenha seu consentimento ou haja um mandado ou ordem judicial. Além disso, a Clearview AI concordou em pagar US$ 1 milhão aos autores do processo (ACLU, 2022).

Além das respostas que vieram ao nível de decisões administrativas e judiciais, o caso Clearview AI ressaltou o debate quanto à necessidade de regulamentação do reconhecimento facial e quanto aos limites e possibilidades dos mecanismos de raspagem de dados utilizados para alimentar ferramentas de inteligência artificial. Além disso, reforçou a discussão sobre o uso de ferramentas desse tipo por órgãos de investigação criminal. O resultado desse debate se manifesta em todo o mundo,

5 Para mais, ver: MCCALLUM, Shiona. Clearview AI fined in UK for illegally storing facial images. **BBC.** Londres, 23 de maio de 2022. Disponível em: <https://www.bbc.com/news/technology-61550776>. Acesso em 31 de maio de 23.

onde diversos projetos de lei visam regulamentar o uso dessa tecnologia, incluindo propostas de proibição total da sua utilização no setor público. Na próxima seção deste artigo, serão examinadas as principais propostas hoje para regulamentação da tecnologia, tanto em âmbito internacional como nacional.

Regras e diretrizes de uso do reconhecimento facial: as propostas em jogo

Os casos narrados acima demonstram como o reconhecimento facial tem sido questionado por vias contenciosas, sejam elas judiciais ou administrativas. Nesse contexto global, somam-se também campanhas de organizações da sociedade civil com o objetivo de coibir a utilização da tecnologia pelo poder público. No Brasil, vale mencionar a campanha "Tire meu rosto da sua mira", da Coalizão Direitos na Rede, que pede a vedação ao uso de reconhecimento facial para fins de segurança pública no país (ver capítulo 5).[6]

Diante da ausência de respostas normativas para o reconhecimento facial, diversas propostas de regulamentação têm surgido em diferentes países. Entre as medidas estão a limitação do acesso a informações coletadas pelo reconhecimento facial, a necessidade de consentimento prévio para o uso dessa tecnologia e a proibição de sua utilização em determinados contextos. Para Bioni e Luciano, há uma espécie de pêndulo de alternativas: em um polo do debate, estão propostas de autorregulação do mercado, centralizadas em diretrizes éticas; no outro polo, propostas de banimento da tecnologia; e, no centro, a proposta de um sistema de corregulação balizado no princípio da precaução, em que ações de mitigação de risco deveriam ser propostas anteriormente à operação da tecnologia (BIONI; LUCIANO, 2019, p. 207–231). Ademais, o reconhecimento facial é o caso específico no bojo de um problema maior, que abrange

6 Ver: https://tiremeurostodasuamira.org.br/. Acesso em 2. Abr. 2023.

não apenas essa, mas quaisquer tecnologias capazes de tomar decisões automatizadas.

Buscando entender a situação atual dessas propostas, as próximas seções deste artigo se dedicarão a destrinchar como países da União Europeia e os Estados Unidos têm enfrentado a questão, em seguida partindo para uma análise sobre o cenário brasileiro e projetos de lei atualmente em discussão no Congresso Nacional.

O cenário europeu e norte-americano: abordagem centralizada nos riscos

Na Europa, a discussão sobre a regulação do reconhecimento facial tem se intensificado nos últimos anos, especialmente considerando a proposta de um marco legal de inteligência artificial pela Comissão Europeia, o *Artificial Intelligence Act*.[7] A redação atual do texto restringe o uso de reconhecimento facial por forças policiais, a menos quando seja utilizado para o combate de crimes graves – sendo apontados, como exemplo, o crime de terrorismo ou de sequestro. O Comitê Supervisor de Proteção de Dados Europeu (EDPS, na sigla em inglês), no entanto, pede que a legislação vá além e inclua abordagem mais rigorosa quanto ao reconhecimento de características humanas em espaços públicos (European Data Protection Supervisor, 2021).

Recomendações e diretrizes nessa direção já foram emitidas por outros órgãos da União Europeia. Em outubro de 2021, o Parlamento

7 O *AI Act* foi proposto pela Comissão Europeia em abril de 2021. Seu objetivo seria o de abordar os riscos associados ao uso da IA e estabelecer regras claras para o desenvolvimento e uso da tecnologia em diferentes níveis de risco. A proposta classifica os riscos em quatro diferentes níveis: risco inaceitável, alto risco, risco limitado e risco mínimo. Ver: Comissão Europeia. Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain EU legislative acts. Abril de 2021. Disponível em: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. Acesso em: 25 mar. 2023.

Europeu publicou decisão não vinculante em que sugere a proibição permanente do uso de análise e reconhecimento automatizado de características humanas em espaços públicos, assim como uma moratória na implantação de sistemas de reconhecimento facial para segurança pública, até que padrões técnicos possam ser considerados totalmente compatíveis com direitos fundamentais (ver capítulo 8). Ademais, expressou preocupação com o uso de bancos de dados privados de reconhecimento facial por autoridades policiais e serviços de inteligência, como o Clearview AI, e solicitou a proibição desse tipo de uso. Por fim, o Conselho da Europa emitiu diretrizes que recomendam a proibição de tecnologias de reconhecimento facial quando utilizadas para determinar características pessoais, como cor da pele, crença religiosa, idade, saúde ou status social.

Chamam atenção também decisões de autoridades de proteção de dados a esse respeito. A Comissão Nacional de Informática e Liberdade (CNIL), autoridade francesa, tem demonstrado preocupação com a tecnologia de reconhecimento facial desde, no mínimo, 2019, quando se opôs à proposta de experimentação de reconhecimento facial em dois colégios na França. A medida visava reduzir o tempo de entrada de estudantes e evitar intrusos nas escolas. No entanto, a CNIL considerou que o dispositivo seria desproporcional e desnecessário, já que a segurança poderia ser garantida por meios menos invasivos, como um controle por meio de cartões (CNIL, 2019).

Nos Estados Unidos, o uso de reconhecimento facial é atualmente regulamentado a nível estadual e municipal. Cidades como San Francisco, Boston e Portland, adotaram leis locais que proíbem ou restringem o uso de tecnologia de reconhecimento facial por forças policiais (J.E.F., 2019). Em nível federal, a *Federal Trade Commission* (FTC)[8] publicou relatório com recomendações e boas práticas não vinculantes para usos comer-

8 Nos EUA, a *Federal Trade Commission* é a agência responsável por salvaguardar os interesses dos consumidores e da defesa da concorrência.

ciais do reconhecimento facial. No caso da tecnologia capaz de inferir características demográficas, o órgão encoraja que exista interação direta do usuário capaz de solicitar o consentimento antes da coleta e processamento de sua imagem (Federal Trade Commission, 2012).

No Congresso, tem-se debatido a necessidade de uma legislação mais ampla para regular o uso de tecnologia pelo governo. Nesse sentido, está em discussão o projeto de *Facial Recognition Act* (Lei do Reconhecimento Facial), proposto por deputados norte-americanos, que proibiria o uso de reconhecimento facial para identificar manifestantes pacíficos ou investigar delitos de menor gravidade. A proposição também exige maior transparência e avaliações anuais do uso da tecnologia pelas forças policiais (IAPP, 2022). Outro projeto em discussão no senado dos EUA é o *Stopping Unlawful Negative Machine Impacts through National Evaluation Act*[9]. Apresentado em dezembro de 2022, o projeto busca reforçar que as leis de direitos civis se aplicam tanto a decisões habilitadas por IA quanto a decisões feitas por humanos, além de autorizar o *National Institute of Standards and Technology* (NIST) a estabelecer "avaliações tecnológicas" para ajudar a indústria a encontrar inovações que reduzam a discriminação algorítmica. Não se trata, todavia, de um projeto que visa regular a tecnologia, mas incentivar a cooperação entre indústria e órgãos públicos na solução de problemas (PORTMAN..., 2022).

Vemos, assim, que as propostas hoje em discussão na Europa e nos EUA têm, em geral, foco no uso do reconhecimento facial em espaços ou serviços públicos, com especial atenção para a segurança pública e o acesso a dados por autoridades de investigação. São frequentes proposições que visam coibir a utilização de bancos de dados privados por órgãos públicos – o que nasce, provavelmente, em resposta às denúncias do Clearview AI. Chamam atenção também recomendações de que tec-

9 Lei da "Avaliação nacional para parar os impactos negativos ilegais de máquinas", em português.

nologias capazes de inferir características – como raça, gênero e emoções – não sejam utilizadas.

Já propostas direcionadas ao setor privado tendem a ser discutidas principalmente no âmbito de projetos de leis mais abrangentes, relativas ao uso de quaisquer tecnologias de decisão automatizada ou inteligência artificial. Observa-se, nessa abordagem, dinâmicas de regulação baseadas no risco oferecido pela tecnologia: quanto maior o risco, maior a necessidade de cautela e de salvaguardas capazes de estabelecer anteparos à sua utilização, como a elaboração de relatórios de impacto prévios à operação, bem como mecanismos de explicabilidade do funcionamento dos algoritmos e transparência ativa. Tecnologias com risco considerado inaceitável, ao menos na proposta europeia, deveriam ser interditas de antemão (MAHLER, 2021). O desafio, diante da ausência de respostas prontas ou fáceis de serem desenhadas, residiria no julgamento quanto à gradação do risco e das medidas adequadas a mitigá-lo.

O cenário brasileiro

No Brasil, embora haja um debate avançado no âmbito da sociedade civil a esse respeito, não há lei que regulamente o uso do reconhecimento facial, seja em âmbito privado ou público. Aos dados biométricos aplicam-se as disposições referentes aos dados sensíveis na Lei Geral de Proteção de Dados. Isto é, de que devem ser coletados mediante enquadramento em uma das bases legais previstas no Art. 11 da Lei: consentimento específico e destacado, cumprimento de obrigação legal ou regulatória, execução de políticas públicas, realização de estudos por órgão de pesquisa, exercício regular de direitos, proteção da vida ou da incolumidade física do titular ou de terceiro, tutela da saúde, e, por fim, prevenção à fraude. Esta última merece atenção, uma vez que, *a priori*, permite a coleta do dado sem consentimento na ocasião de empresas que solicitam o reconhecimento facial para verificação da pessoa com o propósito de evitar fraudes, algo que tem se tornado prática recorrente no mercado.

Ademais, há previsão geral de elaboração de relatório de impacto à proteção de dados, que poderá ser solicitado a qualquer tempo pela Autoridade Nacional de Proteção de Dados. A regra, no entanto, abarca quaisquer atividades de tratamento de dados, não havendo especificação quanto a práticas específicas ao menos no nível da legislação. Em âmbito regulatório, não há também decisão ou norma da ANPD que regulamente o uso do reconhecimento facial.

Projetos de lei sobre reconhecimento facial

Em levantamento de propostas legislativas feitas no Congresso Nacional em fevereiro de 2023,[10] foram encontrados 24 resultados no site da Câmara dos Deputados e 3 resultados no site do Senado Federal. A maioria das propostas aborda o reconhecimento facial no âmbito da criação ou atualização de bancos de dados de identificação digital. Outro grupo frequente de propostas refere-se ao uso do reconhecimento facial na segurança pública. Apenas três proposições se dedicavam ao reconhecimento facial também para fins comerciais: o PL 2392/2022, de autoria do Deputado Guiga Peixoto (PSC/SP), o PL 2537/2019, de autoria do Deputado Juninho do Pneu (DEM/RJ) e o PL 4612/2019, de autoria do Deputado Bibo Nunes (PSL/RS). Em breve análise, no entanto, é possível observar que os projetos não parecem se aprofundar em dinâmicas de regulação centradas no risco, ou mesmo levam em consideração os diferentes objetivos de tecnologias de reconhecimento facial. Nenhum dos projetos, por exemplo, traz definição precisa a respeito da tecnologia.

O projeto apresentado pelo Deputado Juninho do Pneu é o mais curto, com apenas um artigo, e centrado no dever de informação, exi-

10 A pesquisa foi feita em 10/02/2023 utilizando o termo "reconhecimento facial" e abarcando Propostas de Emenda à Constituição (PEC), Projetos de Lei Complementar (PLP), Projetos de Lei (PL), Medidas Provisórias (MPV), Projetos de Lei de Conversão (PLV), e Projetos de Decreto Legislativo (PDL). Foram levadas em consideração apenas propostas ainda em tramitação.

gindo que estabelecimentos comerciais possuam aviso quanto ao uso de reconhecimento facial.

O projeto de autoria do Deputado Bibo Nunes limita-se a definir que "tecnologias de reconhecimento emocional visam a identificar características como personalidade, sentimentos, saúde mental entre outros". No mais, estabelece deveres como a necessidade de supervisão e controle humano, transparência, manutenção de estruturas técnica e administrativa adequadas, uso de tecnologia de acordo com padrões mínimos de precisão, e processo simplificado para questionamentos de decisões tomadas de maneira automatizada. Há poucas ações concretas listadas, entretanto, cabendo à Autoridade Nacional de Proteção de Dados a regulamentação de diversos aspectos da proposição. Ademais, o projeto estabelece que os agentes que utilizam tais tecnologias devem sinalizar o uso de forma clara e visível, permitindo que o indivíduo tenha capacidade de anuência antes do início da captura de sua imagem.

Por outro lado, o projeto também propõe a criação do "Banco Nacional de Reconhecimento Facial e Emocional", no âmbito da Lei de Identificação Criminal (Lei nº 12.037/2009), que teria dados de identificação biométrica facial e emocional de pessoas com mandados de prisão cumpridos ou não. O objetivo seria "subsidiar investigações criminais federais, estaduais ou distritais, auxiliando na captura de foragidos da justiça". A integração ou interoperação dos dados de registros biométricos facial e emocional com outros bancos de dados seria feita por acordo ou convênio com a unidade gestora. A autoridade policial e o Ministério Público poderiam requerer acesso ao juiz competente, no caso de inquérito ou ação penal instauradas. No entanto, não há maiores informações sobre possibilidades e limites ao acesso a dados por parte de autoridades de investigação, ou justificativa apresentada para a coleta de dados referentes ao estado emocional do indivíduo em um banco de dados de identificação criminal de suspeitos, de forma que o projeto se torna ambivalente. Ao mesmo passo em que afirma ter o objetivo de preservar garantias fundamentais e estabelecer compromissos

regulatórios para o desenvolvimento de tecnologias de reconhecimento facial, também segue em direção pantanosa ao propor a criação de um banco de dados que se utiliza dessas tecnologias, inclusive de análise de expressões faciais, sem justificativas a respeito da necessidade ou proporcionalidade da medida.

Já o PL nº 2392/2022 centraliza-se sobre deveres de informação e *accountability* no uso da ferramenta. Primeiro, determina a obrigatoriedade de realização prévia de relatório de impacto à proteção de dados no caso da coleta de dados biométricos que permitam a identificação de um indivíduo. Em segundo lugar, afirma que tais dados não devem ser a única forma de identificação para a utilização de serviços públicos. Por fim, a terceira disposição estabelece que todas as entidades, públicas ou privadas, que fizerem uso dessa tecnologia devem produzir um relatório anual de acesso público que avalie o uso da tecnologia em casos específicos.

TABELA 1. Lista de projetos de lei propostos no Congresso Nacional relativos à regulamentação do reconhecimento facial no setor privado (elaboração própria)

Número	Propositor	Ementa
PL 2537/2019	Juninho do Pneu - DEM/RJ	Obriga o aviso sobre o reconhecimento facial em estabelecimentos comerciais.
PL 4612/2019	Bibo Nunes - PSL/RS	Dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos.
PL 2392/2022	Guiga Peixoto (PSC/SP)	Dispõe sobre o uso de tecnologias de reconhecimento facial nos setores público e privado.

Talvez a última proposta seja a que mais se aproxima de um modelo de regulação baseado em deveres prévios de avaliação do risco, considerando a obrigatoriedade de relatório de impacto e de avaliação periódica da tecnologia. No entanto, o projeto afirma que as regras se aplicam especialmente às tecnologias de reconhecimento facial que permitem identificação biométrica, restando dúvida a respeito de sua aplicação

também para outros propósitos, como a atribuição de características e inferências a respeito de estados emocionais.

O anteprojeto de lei sobre Inteligência Artificial

Em âmbito mais abrangente, a discussão sobre a regulação de inteligência artificial tem tratado o reconhecimento facial com nuances relevantes. Em audiência pública dedicada a discutir a elaboração de projeto de lei de IA, a abordagem regulatória baseada em riscos foi assunto predominante entre os palestrantes.[11] No relatório final da comissão de juristas dedicada a elaborar substitutivo para o projeto,[12] há medidas expressas de avaliação do risco que podem o classificar como alto ou excessivo.

De acordo com o Art. 13 do substitutivo proposto, todo sistema de inteligência artificial deve passar por uma avaliação preliminar realizada pelo fornecedor para classificar seu grau de risco. A finalidade e escopo de utilização é o que definirá se o sistema será considerado de alto risco, assim considerados de antemão aqueles utilizados para (i) aplicação na gestão e funcionamento de infraestruturas críticas, (ii) educação e formação profissional, (iii) avaliação de candidatos em processos seletivos e tomadas de decisão referentes a trabalho, (iv) avaliação quanto a critérios de acesso e concessão de serviços privados ou públicos que sejam

11 Comissão De Juristas Responsável Por Subsidiar Elaboração De Substitutivo Sobre Inteligência Artificial No Brasil. **Relatório Final.** Brasília, DF: Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito, dezembro de 2022. p. 86

12 A comissão foi criada pelo Senado Federal com o objetivo de subsidiar a elaboração de um substitutivo aos Projetos de Lei 5.051/2019, 21/2020 e 872/2021, que regulamentam a inteligência artificial no Brasil. Presidida pelo ministro do superior Tribunal de Justiça, Ricardo Villas Bôas Cueva, a comissão teve como como função debater e propor soluções para orientar a atuação do governo e das empresas na área de inteligência artificial. Mais detalhes podem ser encontrados no site do Senado Federal: https://legis.senado.leg.br/comissoes/comissao?codcol=2504

considerados essenciais, (v) classificação de risco de crédito, (vi) envio ou estabelecimento de prioridades para serviços de resposta a emergências, (vii) administração da justiça, (viii) veículos autônomos, (ix) aplicações na área da saúde, (x) sistemas biométricos de identificação, (xi) investigação criminal e segurança pública, (xii) estudo analítico de crimes, (xiii) gestão da migração e controle de fronteiras. A lista é não exaustiva, considerando que há também previsão de que a autoridade competente a atualize conforme novas hipóteses.

Caso seja classificado de alto risco, torna-se necessária a realização de avaliação de impacto algorítmico e a adoção de medidas específicas de governança, que incluem documentação adequada sobre o funcionamento do sistema, uso de ferramentas de registro automático da operação, realização de testes para avaliar níveis de confiabilidade, gestão de dados para mitigar vieses discriminatórios, adoção de medidas técnicas para viabilizar a explicabilidade dos resultados e supervisão humana dos sistemas. Medidas adicionais são previstas para órgãos do poder público ao contratar, desenvolver ou utilizar sistemas de inteligência artificial considerados de alto risco. Essas medidas incluem a realização de consulta e audiência públicas prévias, definição de protocolos de acesso e utilização do sistema, utilização de dados provenientes de fontes seguras e a criação de mecanismos de supervisão externa e avaliação contínua.

O texto do anteprojeto também traz a vedação a sistemas de inteligência artificial considerados de risco excessivo. Dentre eles, estão considerados: (i) sistemas de inteligência artificial que utilizem técnicas subliminares para induzir comportamentos prejudiciais à saúde ou segurança das pessoas; (ii) sistemas explorem vulnerabilidades de grupos específicos para induzi-los a se comportar de forma prejudicial; (iii) o uso, pelo poder público, de sistemas capazes de avaliar, classificar ou ranquear as pessoas com base em seus atributos de personalidade ou comportamento social para acesso a bens e serviços e políticas públicas. Já o uso de sistemas de identificação biométrica à distância de forma contínua em espaços acessíveis ao público seria permitido apenas em

casos previstos em lei federal específica e com autorização judicial em conexão com a atividade de persecução penal individualizada. Esses casos incluem a persecução de crimes com pena máxima de reclusão superior a dois anos, busca de vítimas de crimes ou pessoas desaparecidas e crime em flagrante.

Percebe-se, a partir da descrição dos artigos na proposta de substitutivo, um caminho definido de atribuição de risco à tecnologia de reconhecimento facial que varia conforme seus propósitos de utilização. Nesse sentido, o risco no uso de um sistema de reconhecimento facial que verifique pessoas no ambiente interno de uma loja não será o mesmo de um sistema que identifique pessoas que andam pelo transporte público diariamente. Na tabela a seguir, é feito um exercício de classificação do risco de determinados sistemas de reconhecimento facial, tomando como base o texto atual do projeto, com base em suas diferentes finalidades.

TABELA 2. Consideração de risco alto ou excessivo de tecnologias de reconhecimento facial, conforme substitutivo apresentado pela Comissão de Juristas.

	Alto risco (condicionamento a medidas mais exigentes de governança)	**Risco excessivo (vedação geral)**
Atribuição de características	Caso seja utilizado para educação, saúde, avaliação de candidatos em processos seletivos, e na avaliação quanto a critérios de acesso e concessão de serviços essenciais.	Quando utilizado pelo setor público para acesso a bens e serviços. Quando utilizado para explorar vulnerabilidades. Quando puder ser utilizado para induzir comportamentos prejudiciais à saúde ou segurança.
Verificação (1:1)	Caso seja utilizado para educação, saúde, avaliação de candidatos em processos seletivos, e na avaliação quanto a critérios de acesso e concessão de serviços essenciais.	Sem previsão específica.
Identificação (larga escala)	Considerado de alto risco sempre que utilizado pelo setor privado ou público.	Considerado de risco excessivo quando utilizado de maneira contínua em espaços acessíveis ao público. Utilização em casos específicos condicionada à existência de lei federal

Fonte: Elaboração própria.

A partir da leitura dos artigos, é possível inferir que grande parte das aplicações de reconhecimento facial hoje existentes seria conside-

rada de alto risco, quando não excessivo. Todavia, o exercício, a essa altura, é apenas hipotético. O substitutivo apresentado pela Comissão de Juristas foi proposto como projeto de lei autônomo pelo presidente do Senado, Rodrigo Pacheco (PSD/MG), no início de maio de 2023.[13] Possivelmente sofrerá ainda mudanças significativas, caso a discussão sobre o projeto tenha sequência nos próximos anos. Até lá, na ausência de lei específica, o reconhecimento facial continuará provavelmente a ser alvo de ações que contestem determinadas aplicações. A litigância no sentido de se consolidar jurisprudência oposta ao reconhecimento facial tem sido usada estrategicamente por organizações, como no caso ViaQuatro. Na arena administrativa, agências reguladoras possuem papel relevante, que tem sido atuado principalmente por autoridades de proteção de dados em casos específicos, como o do Clearview AI.

Considerações finais

Este capítulo se dedicou a analisar as atuais perspectivas de uso do reconhecimento facial pelo setor privado, bem como os debates atuais referentes aos seus riscos e possibilidades de regulação. Nesse sentido, já há casos significativos de questionamento da utilização da tecnologia, especialmente quando empregadas em parcerias público-privadas e no âmbito do espaço público. Aqui, foram destacados dois: o caso ViaQuatro, que questiona o uso de tecnologia capaz de inferir emoções nas plataformas do metrô de São Paulo, e o caso Clearview AI, de aplicativo contestado pelo uso de dados disponíveis publicamente e de compartilhamento com órgãos de investigação criminal.

Em uma segunda parte do capítulo, foi feita uma breve análise sobre o estado atual de propostas regulatórias para o reconhecimento facial, considerando-se as discussões no âmbito da União Europeia, dos EUA, e do Brasil. Há no debate um pêndulo de perspectivas regulatórias que

13 A proposição foi apresentada como Projeto de Lei nº 2338, de 2023.

varia desde a possibilidade de autorregulação do mercado até a possibilidade de medidas mais duras e precaucionárias, como a vedação a determinados usos da tecnologia. De maneira geral, usos públicos têm levantado maior alerta de autoridades regulatórias e de organizações da sociedade civil, especialmente quando utilizada para fins de segurança pública ou persecução penal (ver capítulos 1 e 2). A discussão sobre os usos em âmbito privado da tecnologia aparece de maneira mais residual em projetos de lei específicos sobre o tema. Há, no entanto, intersecção importante da discussão sobre o reconhecimento facial com a regulação de sistemas de inteligência artificial. Nesse sentido, a abordagem regulatória baseada no risco dos sistemas tem ganhado tração, sobretudo na União Europeia (ver capítulo 8).

No Brasil, destaca-se a discussão sobre o projeto de lei destinado à regulação de sistemas de inteligência artificial, em que são colocadas previsões quanto à vedação de tecnologias consideradas de risco excessivo e medidas de governança de maior exigência no caso de alto risco. Em grande parte dos casos, a tecnologia de reconhecimento facial seria considerada, minimamente, de alto risco, quando não de risco excessivo.

Referências

ACLU. In Big Win, Settlement Ensures Clearview **AI** Complies With Groundbreaking Illinois Biometric Privacy Law. **ACLU**, 09 de maio de 2022. Disponível em: <http://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois>. Acesso em: 2 fev. 2023.

BARRETT, Lisa Feldman; **ADOLPHS**, Ralph; **MARSELLA**, Stacy; *et al*. Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements. **Psychological Science in the Public Interest**, v. 20, n. 1, p. 1–68, 2019. Disponível em: <https://doi.org/10.1177/1529100619832930>. Acesso em: 19 mar. 2023.

BIONI, Bruno Ricardo; **LUCIANO**, Maria. O Princípio da Precaução na Regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada? *In*: **Inteligência Artificial e Direito**. São Paulo: Thomson Reuters Brasil, 2019, p. 207–231.

BUOLAMWINI, Joy; **GEBRU**, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: **Proceedings of the 1st Conference on Fairness, Accountability and Transparency**. [s.l.]: PMLR, 2018, p. 77–91.

CJSUBIA. Comissão De Juristas Responsável Por Subsidiar Elaboração De Substitutivo Sobre Inteligência Artificial No Brasil. **Relatório Final.** Brasília, DF: Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito, dezembro de 2022.

CNIL. Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position. 29 octobre 2019. Disponível em: https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position. Acesso em: 25 mar. 2023.

COMISSÃO EUROPEIA. Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain EU legislative acts. Abril de 2021. Disponível em: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. Acesso em: 25 mar. 2023.

DANIEL, Thomas. The cameras that know if you're happy - or a threat. **BBC News,** 16 jul. 2018. Disponível em: <https://www.bbc.com/news/business-44799239>. Acesso em 13. Mar. 2023.

EDPS. European Data Protection Supervisor. *Artificial intelligence act welcomed as an initiative, but the EDPS calls for stronger safeguards.* Disponível em: https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en. Acesso em: 25 mar. 2023.

GUIMARÃES, Leonardo. Hering captura sentimentos dos consumidores em loja conceito. **Consumidor Moderno**. São Paulo, 2 de junho de 2019. Disponível em: https://www.consumidormoderno.com.br/2019/02/06/hering-captura-sentimentos-dos-consumidores-em-loja-conceito/. Acesso em: 20 fev. 2023.

J.E.F. Why San Francisco banned the use of facial recognition technology. **The Economist**, Londres, 16 maio 2019. Disponível em: <https://www.economist.com/democracy-in-america/2019/05/16/why-san-francisco-banned-the-use-of-facial-recognition-technology>. Acesso em: 26 mar. 2023.

LAMBERT, Warren (org.). **Issues with facial recognition technology**. Technology in a globalizing world. New York, NY: Nova Science Publishers, Inc, 2021.

LI, Stan Z.; **JAIN**, Anil K. (Orgs.). **Handbook of Face Recognition**. London: Springer, 2011.

MAHLER, Tobias. Between risk management and proportionality: The risk-based approach in the EU's Artificial Intelligence Act Proposal. **Nordic Yearbook of Law and Informatics**, [S.l.], September 30, 2021. Disponível em: https://ssrn.com/abstract=4001444. Acesso em: 26 mar. 2023.

MEDEIROS, Henrique. Idec entra com ação judicial contra ViaQuatro por coleta indevida de dados - Mobile Time. **Mobile Time**, 2018. Disponível em: <https://www.mobiletime.com.br/noticias/31/08/2018/idec-entra-com-acao-judicial-contra-via-quatro-por-coleta-de-dados-indevidos/>. Acesso em: 3 abr. 2023.

MURGIA, Madhumita. Emotion recognition: can AI detect human feelings from a face? **Financial Times**, Londres, 12 de maio de 2021. Disponível em: <https://www.ft.com/content/cob03d1d-f72f-48a8-b342-b4a926109452>. Acesso em 31 maio de 2023.

PORTMAN Introduces Bill to Guard Against Artificial Intelligence Bias. **United States Senate Homeland Security and Governmental Affairs Committee**, Washington, DC, 21 dez. 2022. Disponível em: https://www.hsgac.senate.gov/media/minority-media/portman-introduces-bill-to-guard-against-artificial-intelligence-bias/. Acesso em: 25 mar. 2023.

RHUE, Lauren. Racial Influence on Automated Perceptions of Emotions. **SSRN Electronic Journal**, 2018. Disponível em: <https://www.ssrn.com/abstract=3281765>. Acesso em: 22 mar. 2023.

SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; **Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas**. InternetLab/IDEC, São Paulo, 2020.

SMITH, Marcus; MILLER, Seumas. The ethical application of biometric facial recognition technology. **AI & SOCIETY**, v. 37, n. 1, p. 167–175, 2022. Disponível em: <https://link.springer.com/10.1007/s00146-021-01199-9>. Acesso em: 3 mar. 2023.

TAVARES, C.; SIMÃO, B., MARTINS, F.; SANTOS, B., ARAÚJO, A. **Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras**. São Paulo: InternetLab, 2023

TEOFILO, D; KURTZ, L; PORTO JR, O; VIEIRA, V. **Parecer do IRIS na Ação civil Pública IDEC vs. Via Quatro.** Belo Horizonte: IRIS, 2019.

YAN, Wudan. Reconhecimento facial com máscara já é uma realidade – gostemos ou não. **National Geographic**, 17 de set. de 2020. Disponível em: <https://www.nationalgeographicbrasil.com/ciencia/2020/09/reconhecimento-facial-com-mascara-ja-e-uma-realidade-gostemos-ou-nao>. Acesso em: 2 abr. 2023.

Tecnologias de reconhecimento facial na administração pública brasileira: Desafios técnicos e sociais para o uso responsável da tecnologia

Rodrigo Brandão

Resumo

Neste capítulo, argumento que os vieses algorítmicos de sistemas de reconhecimento facial podem acentuar chagas sociais, como o racismo e a misoginia, representando, portanto, riscos sociais. Inicialmente, discuto os elementos técnicos e sociais que embasam estes vieses. Na sequência, apresento medidas que podem ser adotadas por gestores públicos para preveni-los ou, ao menos, mitigá-los no ciclo de políticas públicas, e demonstro que, nos casos em que os sistemas de reconhecimento facial já são usados na administração pública brasileira, tais medidas têm sido ignoradas, constituindo, assim, um cenário em que o uso de sistemas de reconhecimento facial tem se dado de modo irresponsável. Por fim, argumento que a alteração desta realidade depende da constituição de alianças entre diferentes atores sociais capazes de demonstrar a agentes públicos que, sem a devida cautela, o uso dos sistemas em questão pode piorar a vida dos cidadãos.

Introdução

A Inteligência Artificial (IA) pode ser definida como "um sistema baseado em máquinas que pode, para um dado conjunto de objetivos

definidos por humanos, realizar predições, recomendações ou tomar decisões, influenciando, assim, ambientes reais ou virtuais. Os sistemas de IA são elaborados para operar com níveis variados de autonomia" (OECD, 2019).[1] Entre as diferentes aplicações possíveis da IA, estão os sistemas de reconhecimento facial (RF) que usam algoritmos de reconhecimento de padrões, frequentemente implementados com técnicas de *machine learning* (ML). Esse subconjunto da IA tem atraído a atenção de diferentes *stakeholders* por conta dos erros que comete ao ser usado em contextos públicos.

Em seu mapeamento de erros do gênero, Silva (2020) nos lembra de uma ocorrência de 2009, quando, "em vídeo publicado no YouTube, um homem negro e uma mulher branca [testaram] um computador da HP em uma loja de eletrônicos. O recurso MediaSmart de rastreamento de movimento de rostos conseguia identificar o rosto da mulher branca, mas não o rosto do homem negro". O autor nos recorda ainda que, seis anos depois, em 2015, a funcionalidade de etiquetação automática do aplicativo Google Photos marcou pessoas negras com a etiqueta "gorilas". Três anos mais tarde, segue Silva (2020), casos como esse foram observados em tecnologias do Face++ e da Microsoft, que associavam emoções negativas a pessoas negras, reforçando, assim, o estigma social de que elas são raivosas; e no Google Vision, que confundia cabelos negros com perucas.

Apesar de antigos e resilientes, erros como os descritos acima não têm sido um empecilho para que os sistemas de RF sejam cada vez mais utilizados pelo setor público brasileiro. Este fenômeno é digno de atenção porque, durante a elaboração e a implementação de políticas públicas, tais erros podem tornar o Estado um reprodutor de chagas sociais, como o racismo e a misoginia. Afinal, "estereótipos desfavoráveis aos negros, por exemplo, são reforçados toda vez que uma estudante negra é indevidamente tomada como possível fraudadora de um passe livre

1 Traduzido pelo autor a partir do original em inglês.

estudantil ao qual tem direito ou quando um jovem negro, de modo igualmente equivocado, é confundido pela tecnologia, levando a polícia a abordá-lo" (BRANDÃO ET AL., no prelo).

Neste capítulo, apresento e discuto medidas que os operadores de políticas públicas podem tomar para minimizar riscos como esses. Com esse objetivo, apresento, na seção 2 deste capítulo, as razões pelas quais os sistemas de RF – assim como outros sistemas baseados em técnicas de ML – geram resultados enviesados. Na seção 3, discuto algumas recomendações para o uso responsável de sistemas de IA/ML por agentes públicos. Por fim, na seção 4, apresento o panorama de utilização dos sistemas de RF pela administração pública brasileira, procurando demonstrar que há uma lacuna entre os modos como os sistemas de IA/ML deveriam ser usados no setor público e como os sistemas de RF, de fato, o são.

Conceitos Gerais: Inteligência Artificial, Machine Learning e Vieses Algorítmicos

Nos Anos 1950, dois eventos marcaram o nascimento da IA. Em 1950, o matemático Alan Turing lançou o artigo *Computing Machinery and Intelligence*, no qual o Teste de Turing foi mencionado pela primeira vez. Já em 1956, durante uma conferência acadêmica em Dartmouth, o termo "inteligência artificial" foi cunhado e a IA foi lançada como área de pesquisa. Nos anos subsequentes, os resultados obtidos nesse campo ficaram aquém do esperado. Essa frustração converteu-se no que ficou conhecido como o "Primeiro Inverno da IA", quando – entre meados dos Anos 1970 e o início dos Anos 1980 – o financiamento e o interesse pela área escassearam de modo expressivo (ANYOHA, 2017).

Ao longo dos primeiros anos da década de 1980, o interesse pela IA recobrou força, pois alguns pesquisadores de ciência da computação conseguiram equipar sistemas computacionais com uma lógica de

raciocínio do tipo *if-then*.[2] A excitação com essa conquista não foi suficiente, contudo, para fazer frente ao interesse por um outro evento que ocorria na mesma época: a massificação do *desktop* (DAUGHERTY & WILSON, 2018). Novamente, o interesse de pesquisa e comercial pela área sofreu forte impacto, e o "Segundo Inverno da IA" teve início. Nesse período, a área não ficou paralisada. Em 1997, por exemplo, o Deep Blue – um computador inteligente da IBM – venceu o campeão mundial de xadrez Garry Kasparov. E, em 2005, um carro autônomo desenvolvido por pesquisadores da Universidade Stanford venceu uma competição científica organizada regularmente pela *Defense Advanced Research Projects Agency* (DARPA), um dos principais órgãos federais da área de Ciência, Tecnologia e Inovação dos Estados Unidos da América (EUA).

Foi a partir de 2010, que a IA recobrou força. A retomada foi puxada pelos "[...] algoritmos de *machine learning* [...] e [...] de *deep learning* (DL, subárea da ML) [que] receberam impulso de novos avanços, em *hardware* e *software*" (ARBIX, 2020, p. 402). Esse impulso, aponta Arbix (2020), foi possível por três fatores: (i) os bancos de dados pessoais já cresciam com velocidade, graças a dinâmicas econômicas e sociais centradas em aplicativos; (ii) a infraestrutura tecnológica estava suficientemente desenvolvida para armazenar essas informações; e (iii) o campo da estatística estava preparado para analisá-las.

Assim como outros campos da IA – como, por exemplo, Representação de Conhecimento e Raciocínio e Sistemas Multi-Agentes –, a área de ML dedica-se a construir algoritmos, isso é, "[…] procedimentos codificados para transformar dados de entrada em uma saída desejada, com base em cálculos especificados" (GILLESPIE, 2014, p. 167).[3] No caso da ML, os pesquisadores desenvolvem procedimentos para a identificação de regulari-

2 No campo da programação, a lógica *if-then* (se-então) consiste em um comando do seguinte tipo: se (*if*) o sistema computacional se deparar com a situação A, deve executar, então (*then*), a ação B.

3 Traduzido pelo autor a partir do original em inglês.

dades em grandes volumes de dados, e trabalham para que os sistemas computacionais que utilizam aprendam esses procedimentos. Em geral, eles utilizam quatro abordagens diferentes: aprendizado supervisionado (*supervised learning*), aprendizado não supervisionado (*unsupervised learning*), aprendizado por reforço (*reinforcement learning*) e aprendizado profundo (*deep learning*) (BERRYHILL ET AL., 2019).

No aprendizado supervisionado, os pesquisadores deixam claro ao sistema computacional qual é o resultado que ele deve alcançar, quais são os padrões de dados associados a este resultado e quais são os procedimentos que ele deve utilizar para buscá-los. No aprendizado não supervisionado, o resultado a ser alcançado pelo sistema computacional não é claro, cabendo a ele identificar, a partir de procedimentos previamente estabelecidos por humanos, se o banco de dados ao qual está exposto possui, ou não, regularidades, e, em caso afirmativo, quais são elas. Os processos de aprendizado por reforço, por sua vez, possuem semelhanças com os processos de aprendizado supervisionado. Em ambos, os pesquisadores deixam claro ao sistema computacional qual é o resultado que ele deve alcançar e quais são os procedimentos que ele deve utilizar para buscá-lo. Todavia, no aprendizado por reforço, o sistema computacional é programado para aprender com os próprios erros como os procedimentos com os quais opera podem ser otimizados na busca pelo resultado que deve atingir.

Por fim, o aprendizado profundo difere das três abordagens anteriores. Nele, o reconhecimento de padrões em grandes volumes de dados é feito por sistemas computacionais que emulam o complexo sistema de camadas do cérebro humano, fazendo com que os pesquisadores não tenham clareza sobre os procedimentos utilizados para a detecção de padrões. Como se vê, os algoritmos de *deep learning* são – como todo e qualquer algoritmo – um conjunto de procedimentos que transformam dados de entrada em uma saída desejada, mas a codificação e os cálculos que embasam essa transformação não são inteiramente conhecidos por agentes humanos.

Os processos de construção de algoritmos variam entre as abordagens acima. Mas, em maior ou menor medida, compreendem cinco etapas. Utilizo informações do trabalho de Ruback et al. (2021) para explicar de maneira simplificada cada uma delas em um processo de aprendizado supervisionado. A primeira etapa é a **coleta de dados** ou a utilização de bancos de dados já disponíveis. Na sequência, ocorre o **pré-processamento,** quando os dados passam por um processo de limpeza – alguns deles são substituídos e algumas de suas características são selecionadas para serem trabalhadas nas etapas futuras do processo.

Limpos, os dados são separados entre dados de treinamento e dados de teste. Inicialmente, os primeiros são utilizados. Os dados de treinamento servem de exemplos para os sistemas que estão sendo treinados e, por isso, eles (os dados de treinamento) precisam estar rotulados. Não raro, essa rotulação é feita por seres humanos, e consiste em uma operação algo simples, como rotular as imagens de um banco de imagens com as etiquetas "gato" e "não-gato", caso a intenção seja ensinar ao sistema qual é o padrão entre diferentes imagens de gatos diferentes.

O resultado dessa etapa é a **produção de vários modelos estatísticos** que, ao serem confrontados com novos rótulos, inferem a probabilidade d'eles serem convergentes ao padrão apreendido pelos sistemas. De acordo com Blackwell (2020), a inferência costuma depender de técnicas estatísticas de regressão linear e de regressão logística, e o padrão apreendido recebe o nome de *ground truth*. Os modelos gerados devem ser capazes de predizer a probabilidade de convergência de um rótulo à *ground truth*. Para isso, eles utilizam funções numéricas que testam um resultado em comparação a todos os resultados possíveis. Em um jogo de tabuleiro, por exemplo, o modelo estatístico irá utilizar funções numéricas para testar todos os cursos possíveis de ação em cada uma das posições em que se encontrar no tabuleiro, e escolher – ou sugerir, a depender do grau de autonomia do modelo – o movimento que tiver maior probabilidade de ser aderente ao que foi definido como "sucesso", como, por exemplo, derrubar o rei, dando, assim, um xeque

-mate. Essa definição de "sucesso", aponta Blackwell (2020), é feita pelos programadores.

Entre os modelos gerados, é escolhido o que apresenta as maiores taxas de sucesso. Caso ele se baseie nos algoritmos criados por desenvolvedores, é possível que estes consigam explicar quais procedimentos foram observados pelos sistemas computacionais. Ou seja, como esses sistemas operaram para testar todas as possibilidades possíveis em um jogo de tabuleiro. Todavia, se o modelo estatístico foi gerado a partir de algoritmos de *deep learning*, os desenvolvedores não podem ter certeza sobre as tecnicalidades do modelo gerado, como, por exemplo, em quais premissas um modelo para concessão de crédito se baseia para classificar, em uma lógica binária, "bons pagadores" e "não-bons pagadores".

Criado o modelo estatístico, ele passa por **rodadas de avaliação**, quando é submetido a *dados de teste*, isso é, dados semelhantes aos que foram utilizados em seu treinamento, mas aos quais ele nunca foi exposto e que não estão rotulados. O resultado desse teste é uma *matriz de confusão*, a qual é formada por quatro elementos: (i) verdadeiros positivos ("câncer predito como câncer"); (ii) falsos positivos ("não-câncer predito como câncer"); (iii) verdadeiros negativos ("não-câncer predito como não-câncer") e; (iv) falsos negativos ("câncer predito como não-câncer"). O modelo pode ser confrontado ainda com *dados de referência*, para que seu desempenho seja comprovado e comparado ao desempenho de outros modelos já existentes. Entre as diversas métricas existentes para avaliar o desempenho dos modelos, a "acurácia" é a mais intuitiva delas. Trata-se da proporção de acertos (a soma de "verdadeiros positivos" e "verdadeiros negativos") no conjunto total de predições realizadas. Todavia, outras métricas podem ser utilizadas, a depender das finalidades da adoção da tecnologia. Pode-se desejar, por exemplo, que a taxa de falsos negativos ("câncer predito como não-câncer") seja tão baixa quanto possível, mesmo que isso eleve a ocorrência de falsos positivos ("não-câncer predito como câncer").

A última etapa é o **pós-processamento**. Nela, são feitas calibrações no modelo de acordo com a utilização que será feita dele. Em um sistema de RF no transporte coletivo, por exemplo, os responsáveis pelo modelo deverão estabelecer parâmetros para a interpretação das probabilidades geradas por ele. A tecnologia capta a foto de um estudante e "diz" qual é a probabilidade de que a foto captada seja semelhante à foto do estudante cadastrada em seu banco de dados. São os responsáveis pelo sistema que devem determinar qual é o limiar que separará "fraudadores" de "não-fraudadores" – por exemplo: "para ser considerado um 'não-fraudador', a probabilidade de correspondência entre as imagens precisa ser de pelo menos 80%". Ruback et al. (2021, p. 8) observam que "[o] processo de desenvolvimento de um modelo de aprendizado de máquina geralmente é incremental, de forma que eles são retroalimentados com *feedbacks* – sobretudo indicando os erros nas predições. Dessa forma, os modelos aprendem com os próprios erros, o que permite a melhora contínua do seu desempenho".

Como se pode perceber, o processo de ML é pervasivo, pois pode ser usado em diversas aplicações de IA – seja para "ensinar" um *software* a reconhecer imagens ou para realizar o processamento de linguagem natural que permite a um *chatbot* "aprender a conversar" com os usuários de um serviço público. Além disso, e mais importante, ele é opaco, já que compreende inúmeros pontos ininteligíveis para atores externos a ele.

Nas primeiras etapas, podem existir dúvidas sobre como os dados foram conseguidos e como foram tratados. Já em relação ao modelo, pode haver incertezas sobre as premissas que ele utiliza para classificar os dados aos quais é exposto, sobretudo se algoritmos de *deep learning* foram utilizados para estruturá-lo. E, por fim, nas etapas finais, os protocolos utilizados para a leitura das informações geradas pelo modelo podem não ser conhecidos. Dúvidas e incertezas como essas são o completo oposto do que Grimmelikhuijsen (2022, p. 4) denomina "transparência algorítmica": "[…] quando atores externos podem acessar os

dados utilizados e o código de um algoritmo, e os resultados produzidos são explicáveis de forma que um ser humano possa entender"[4].

Como veremos na próxima seção, a transparência algorítmica é um dos principais antídotos para um problema recorrente em *outputs* de ML: a geração de resultados tendenciosos ou, no jargão da área, enviesados. Existem diferentes taxonomias de vieses. Suresh & Gutag (2021) abordam vieses históricos, de representação, de mensuração, de agregação, de aprendizado, de avaliação, e no emprego da tecnologia. Adaptando o *framework* desses autores, Ruback et al. (2021), conferem centralidade a quatro deles: (i) viés histórico; (ii) viés de representação (ou de amostra); (ii) viés de avalição; (iii) viés de interpretação humana.

O primeiro deles ocorre "mesmo que os dados sejam medidos e amostrados perfeitamente, se o mundo como *é* ou *foi* leva a um modelo que produz resultados prejudiciais" (SURESH & GUTAG, 2021, p. 4)[5]. Um exemplo desse tipo de viés pode ser encontrado em aplicações de processamento de linguagem natural que, treinadas em bases de textos já antigos, associam as engenharias a homens e a enfermagem a mulheres quando, em mecanismos de buscas textuais, devem completar automaticamente determinadas palavras, como "engenhei-ro" e "enfermei-ra". Por mais que, em alguns países e regiões, homens continuem a ser a maioria entre os profissionais de engenharia e as mulheres, a maioria entre os profissionais de enfermagem, a naturalização dessa realidade já não é livre de contestações.

As ações dos programadores durante o desenvolvimento dos algoritmos também podem contribuir para a reprodução de vieses históricos. Tomemos como exemplo a programação de uma aplicação de RF preocupada em classificar homens e mulheres. Nessa atividade, cabe a eles (os programadores) traduzir o debate contemporâneo sobre identidade de gênero em premissas a serem utilizadas pela tecnologia para

4 Traduzido pelo autor a partir do original em inglês.

5 Traduzido pelo autor a partir do original em inglês.

classificar quem deve ser reconhecido como homem e quem deve ser reconhecido como mulher. A depender das escolhas que forem feitas, as faces de pessoas transgênero podem não ser reconhecidas corretamente pela tecnologia.

Já o viés de representação (ou de amostra) ocorre nas primeiras etapas dos processos de ML, e foi estudado por Buolamwini & Gebru (2018). Ao analisarem alguns dos principais programas de RF do mercado estadunidense, as pesquisadoras descobriram que os algoritmos de análise facial baseados em ML costumam ser treinados em bases de dados desbalanceadas em termos de raça e de gênero. Isso acaba por se traduzir em taxas máximas de erro desproporcionais entre os diferentes grupos sociais: se, entre os homens de pele mais clara, elas giram em torno de 0,8%, elas saltam para até 34,7% entre as mulheres com tonalidades mais escuras de pele. Achados de pesquisa do *National Institute of Standards and Technology* (NIST), dos EUA, vão na mesma direção (HAO, 2019). Pesquisadores ligados à instituição verificaram que, entre pessoas asiáticas e afrodescendentes, as chances de falsos positivos (por exemplo, não-suspeito ser predito como suspeito) são até 100 vezes maiores.

Cabe notar que estudos como esses costumam ser realizados em ambientes controlados, nos quais variáveis como a posição da imagem e a qualidade da luz são conhecidas. Em ambientes reais, os erros dos sistemas de RF tendem a ser maiores. Essa tendência é ainda mais acentuada quando os sistemas devem identificar uma pessoa em meio a multidões, ao invés de autenticar sua identidade em situações específicas. Nas operações de autenticação, o sistema de RF capta a imagem de uma pessoa e a compara a uma fotografia de referência. Nas operações de identificação, por sua vez, a tecnologia deve ser capaz de detectar se as muitas fotografias de seu banco de imagens encontram correspondência entre as inúmeras pessoas que passam em frente a uma câmera.

Ainda sobre o viés de representação (ou de amostra), cumpre observar que

> [...] dados anotados por humanos não são isentos de viés: foi relatado, por exemplo, que diferenças de gênero ou origem étnica e social podem produzir diferentes vieses na avaliação do significado de uma imagem ou de um conceito (Bencke, 2016; Crawford, 2016) (VETRÒ ET AL., 2019, p. 299)[6].

Ou seja, mesmo se um banco de dados for balanceado em termos de raça e de gênero, por exemplo, vieses de representação (ou de amostra) podem acontecer durante a rotulação dos dados de treinamento.

O viés de avaliação, por sua vez, pode ser inserido no modelo de duas maneiras. Primeiramente, os dados de referência podem ser tão desbalanceados quanto os dados de teste. Nesse caso, o desbalanço inicial não ficará evidente. Em segundo lugar, o viés pode ser decorrente da métrica de avaliação escolhida para determinar o que será considerado "sucesso" no funcionamento do modelo.

> Por exemplo, um modelo de reconhecimento facial pode ter uma precisão geral de 80%, mas se formos considerar a precisão dentro do grupo que inclui mulheres negras, a precisão cai para 60%, enquanto que a precisão dentro do grupo que corresponde a homens de pele clara, a precisão sobe para 90% (RUBACK ET AL., 2021, p. 10).

Por fim, o viés de interpretação humana ocorre na fase de pós-processamento, e é mais difícil de ser mensurado. Por essa razão, recorro a um exemplo hipotético para descrevê-lo: ao ser informado sobre possíveis fraudadores no transporte coletivo, o funcionário de um órgão de transporte público municipal responsável por supervisionar o sistema de RF utilizado acata – de modo consciente ou inconsciente – a recomendação do sistema toda vez que o possível fraudador é negro, mas

6 Traduzido pelo autor a partir do original em inglês.

entende, de maneira regular, que o sistema pode ter cometido um erro quando o possível fraudador é branco.

Como se vê, os quatro tipos de viés algorítmico discutidos acima podem funcionar como mecanismos de discriminação social, representando, portanto, um risco social. Essa possibilidade deixa claro que a complexidade no funcionamento das aplicações de IA/ML e as dificuldades para monitorá-la demandam atenção dos gestores públicos, se o objetivo d'eles for utilizá-las para melhorar a vida das pessoas. Na próxima seção, discuto estratégias que eles podem adotar para prevenir ou, pelo menos, mitigar os vieses discutidos.

Uso responsável de sistemas de IA/ML: breves recomendações

Antes de recorrer a uma aplicação de IA/ML – seja contratando-a de terceiros, seja desenvolvendo-a no âmbito de suas repartições –, os agentes públicos devem se perguntar se ela é necessária à operacionalização da política pública em que pretendem empregá-la (GREEN, 2022). Apesar de simples, esse questionamento é essencial para que os gestores públicos coloquem em perspectiva discursos baseados na ideia de *smart city*, sobretudo os de origem empresarial. Sem as devidas ponderações, esses discursos podem levar o poder público a comprar ou a desenvolver produtos tecnológicos apenas para transmitir aos cidadãos uma ideia de modernidade e progresso, sem que tais produtos contribuam de modo efetivo ao aprimoramento das ações do Estado (SADOWSKI & BENDOR, 2019; ENGSTROM & HO, 2020).

A fim de avaliar a pertinência da utilização de aplicações de IA/ML, os agentes públicos podem realizar um procedimento conhecido como avaliação de impacto algorítmico (AIA). As AIAs têm a forma de uma matriz de prejuízos, benefícios e riscos; são feitas antes de os sistemas algorítmicos começarem a ser utilizados; e procuram mitigar eventuais impactos negativos desses sistemas por meio de consultas aos públicos a

serem afetados por eles. Ou seja, diferentemente do que seu nome pode sugerir, as AIAs não são avaliações unicamente técnicas, centradas no código-fonte dos sistemas avaliados. Em diferentes países, agentes públicos utilizam AIAs, por isso há uma miríade de modelos. O mais completo deles é o canadense (GOVERNO DO CANADÁ, sem data).[7]

Diante de sistemas de RF, a realização de AIAs é altamente desejável, uma vez que este subconjunto das aplicações de IA/ML possui um longo histórico de resultados enviesados comprovados (BUOLAMWINI & GEBRU, 2018; NIST *apud* HAO, 2019; SILVA, 2020). Como parte da AIA, os órgãos e entidades do poder público da União, Estados, Distrito Federal e Municípios podem realizar consultas e audiências públicas que congreguem representantes de diferentes segmentos sociais. Por serem amplos, diálogos dessa natureza podem ajudar os gestores públicos a identificar se os usos que pretendem fazer dos sistemas de RF tendem a reproduzir vieses históricos.

Já para evitar vieses de representação (ou de amostra), os agentes públicos devem estar preparados para avaliar a qualidade dos bancos de dados que serão utilizados no funcionamento dos sistemas de RF. Para isso, devem constituir equipes inclusivas e diversas, pois um grupo social – como o dos homens brancos – pode ser, voluntária ou involuntariamente, pouco sensível às consequências do mau funcionamento da tecnologia sobre outro grupo social – como o das mulheres negras. Ou seja, a diversidade é instrumental para a identificação de falta de representatividade nos conjuntos de dados a serem utilizados. A multidisciplinariedade também é chave para a identificação desse problema, já que profissionais de áreas diferentes tendem a atentar para aspectos e resultados distintos do funcionamento da tecnologia. Por essas razões, é recomendável que tanto os times de gestores públicos envolvidos com a contratação ou com o desenvolvimento de sistemas próprios de RF, quanto as equipes que utilizarão essa tecnologia em suas atividades pro-

7 Uma versão traduzida do AIA canadense encontra-se disponível no trabalho de Langevin & Fassio (2022).

fissionais diárias, sejam heterogêneas. A heterogeneidade e a diversidade também são fundamentais para que os vieses de avaliação sejam evitados. Como vimos na seção anterior, esse tipo de viés pode acontecer quando as equipes responsáveis pela avaliação dos modelos estão dispostas a aceitar resultados favoráveis a um determinado grupo social em detrimento de outros, como, por exemplo, um sistema de reconhecimento que apresenta resultados precisos diante de homens brancos, mas fortemente imprecisos frente a mulheres negras. Na fase de avaliação dos modelos, equipes heterogêneas e diversas são mais capazes de identificar e contestar resultados como esse.

Além de heterogêneas, as equipes envolvidas com a aquisição, com o desenvolvimento e com a utilização dos sistemas de RF devem estar aptas a investigar aspectos técnicos complexos, como a qualidade da rotulagem dos dados de treinamento, as premissas escolhidas para estruturar o modelo e a métrica escolhida para determinar o que será considerado "sucesso", a taxa de acurácia da tecnologia em situações de identificação e de autenticação – sobretudo em ambientes não-controlados –, e se algoritmos do tipo *deep learning* foram, ou não, utilizados na construção do modelo. Essas mesmas equipes devem estar preparadas para avaliar ainda se a infraestrutura tecnológica possuída pelo órgão público é adequada à utilização da tecnologia (DESOUZA, 2018; MACIEIRA ET AL., 2020). Avaliações desse último tipo são úteis para que toda e qualquer aplicação de IA tenha seu potencial assegurado, evitando-se, assim, que sua adoção represente desperdício de recursos públicos.

Durante todo o processo de condução da AIA, a estrutura de governança dessa avaliação deve estar clara para todas as partes envolvidas, isso é, todas elas devem saber com clareza quem faz o quê, com que grau de autonomia, e com quais formas de monitoramento e controle. Após concluir a AIA, os gestores públicos podem entender que a utilização de sistemas de RF é salutar às políticas públicas sob sua responsabilidade e, mais importante, que eles estão aptos não só a prevenir os riscos sociais dessa tecnologia, mas também a explicar à população como os *outputs*

dela embasam suas decisões. Nesse caso, eles devem continuar primando pela governança dos sistemas em questão, de modo a assegurar a transparência e a *accountability* algorítmicas.

Para que a transparência algorítmica exista, é preciso que os cidadãos saibam quando estão submetidos a sistemas algorítmicos e como essas tecnologias embasam a tomada de decisões públicas, de modo que eles (os cidadãos) possam demandar respostas e justificativas sobre o uso e o funcionamento desses sistemas sempre que julgarem necessário (ADA LOVELACE INSTITUTE ET AL., 2021). No caso brasileiro, a observância à Lei Geral de Proteção de Dados Pessoais (LGPD) é crítica à promoção desse tipo de transparência. Dois de seus dispositivos são especialmente relevantes: a obtenção de consentimento livre e informado para o tratamento de dados pessoais e a elaboração de relatórios de impacto à proteção de dados pessoais (RIPDPS).

De modo geral, a LGPD estabelece que dados pessoais só podem ser tratados após o titular dos dados pessoais concordar que isso seja feito. Esse consentimento deve se dar por meio de manifestação livre e informada, e deve se referir a uma finalidade específica. Em alguns casos, no entanto, o tratamento de dados pessoais pode ocorrer sem o consentimento prévio e específico dos titulares. Entre essas exceções, está o uso de dados pessoais – inclusive de dados pessoais sensíveis, como os dados biométricos – para a operacionalização de políticas públicas. Ou seja, o mecanismo em questão não é mandatório ao setor público, mas este não está impedido de adotá-lo, sendo desejável que o faça. Ao coletar o consentimento livre e informado dos cidadãos para o tratamento de um de seus dados biométricos (no caso, a imagem de suas faces), o poder público dá ciência a estes de que estão expostos a um sistema algorítmico.

Outro mecanismo da LGPD crítico à promoção da transparência algorítmica é a autorização legal dada à Autoridade Nacional de Proteção de Dados (ANPD) para que solicite aos controladores de dados pessoais (sensíveis) a elaboração de RIPDPS, os quais devem compreender documentos que contenham "a descrição dos processos de tratamento de da-

dos pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (Art. 5º, XVII). A ANPD pode exigir de entes públicos e privados a elaboração desses relatórios a qualquer momento e sempre que os entender pertinentes. Ou seja, ao utilizar tecnologias de IA que dependem de dados pessoais sensíveis, o setor público não é obrigado a produzir RIPDPs, ainda que seja altamente desejável que o faça. Afinal, é por meio deste mecanismo que pode deixar claro, ao contratar, desenvolver e empregar sistemas de RF, como pretende prevenir ou mitigar os riscos sociais decorrentes de vieses algorítmicos produzidos por essa tecnologia.

Por fim, ao recorrer a sistemas de RF, a máquina pública deve estar preparada para adotar também mecanismos que garantam ao cidadão que, se ele sofrer algum dano indevido, ele será reparado e o poder público responderá pelo resultado adverso, por ser responsável pela utilização da tecnologia. Essa estratégia de responsabilização é chamada por Ada Lovelace Institute et al. (2021) de *accountability* algorítmica. Um dos dispositivos do relatório final preparado pela comissão de juristas do Senado Federal encarregada de elaborar um projeto de lei sobre IA revela-se útil à promoção desse tipo de *accountability*, qual seja, "[definir] protocolos de acesso e de utilização do sistema [de IA] que permitam o registro de quem o utilizou, para qual situação concreta, e com qual finalidade" (CJSUBIA, 2022). Protocolos como esse são essenciais para evitar que agentes públicos utilizem os sistemas de RF para vigiar de modo arbitrário e ilegal cidadãos específicos. Todavia, eles não são suficientes para evitar os vieses de interpretação humana.

Estudos diversos identificaram que os operadores de políticas públicas enfrentam dificuldades para contestar os *outputs* de sistemas algorítmicos, fazendo com que estes se comportem como verdadeiros tomadores de decisões públicas, ao invés de apenas subsidiá-las (EUBANKS, 2018; CALO & CITRON, 2020; KUZIEMSKI & MISURACA, 2020; FUSSEY & MURRAY, 2020). Por isso, a utilização de sistemas de RF deve ser acompanhada de instruções claras sobre como os *outputs* da tecnologia (como a identifi-

cação de um possível suspeito na segurança pública ou de um possível fraudador no transporte coletivo) devem ser convertidas em decisões humanas (como perseguir, ou não perseguir, um possível suspeito, ou suspender, ou não suspender, o direito a passagens com desconto de um possível fraudador). Além disso, é necessário que a eficácia desses protocolos seja testada com regularidade, para que se possa averiguar se vieses humanos de raça e de gênero, por exemplo, não estão interferindo de forma negativa no aproveitamento dos resultados da tecnologia.

A operacionalização da transparência e da *accountability* algorítmicas dependem também da existência de canais institucionalmente estabelecidos e notoriamente públicos de diálogo entre o poder público e os diferentes segmentos da sociedade. Para isso, é importante que a figura do encarregado pelo tratamento de dados pessoais – prevista pela LGPD – esteja não só estabelecida, mas também articulada com outras instâncias, como, no caso dos municípios, os conselhos municipais de transparência (quando estes existem).

Como veremos na próxima seção, as recomendações acima encontram pouco eco na realidade brasileira, sinalizando que, no país, o uso dos sistemas de RF na administração pública tem sido pouco responsável.

O Uso de Sistemas de RF na Administração Pública: Panorama e Avaliação

Um número crescente de estudos vem procurando identificar quais aplicações de IA são mais utilizadas pelo setor público brasileiro. Como veremos, ao menos nos planos federal e estadual, os sistemas de RF não estão neste grupo. Esse achado de pesquisa indica haver espaço, portanto, para que a administração pública brasileira utilize tais sistemas com responsabilidade, caso decida recorrer a eles. Um outro conjunto de estudos indica, no entanto, que – nos casos em que as tecnologias de RF já são utilizadas – o uso é pouco ou nada responsável, ignorando quase por completo as recomendações discutidas na seção anterior.

Mapeamento do uso de aplicações de IA

Em estudo promovido pela Transparência Brasil, Coelho & Burg (2020) propõem que os usos de sistemas de IA por órgãos públicos são de quatro tipos diferentes: (i) interno, com tomada de decisão; (ii) externo, com tomada de decisão; (iii) interno, sem tomada de decisão; e (iv) externo, sem tomada de decisão. Ao pesquisar a administração pública federal brasileira, as autoras encontraram exemplos dos três primeiros tipos, em um total de 44 casos de uso. As autoras não especificam qual é, neste universo, a quantidade de ferramentas de RF. Um estudo recente do TCU (2022) e a pesquisa TIC Governo Eletrônico 2021 (NIC.BR, 2022) preenchem parcialmente esta lacuna.

O primeiro desses dois materiais apresenta informações agregadas sobre 263 organizações da administração pública federal. Dessas, 28% utilizam alguma aplicação de IA; 45% não utilizam, mas pretendem utilizar; e, em 27% delas, não há previsão de utilização. Entre os órgãos que utilizam a tecnologia em questão, o principal domínio de aplicação não é a área de reconhecimento de imagens, mas sim a de processamento de linguagem natural – que compreende aplicações como mineração de textos, *chatbots*, análise de sentimentos, processamento de linguagem escrita ou falada – e a construção de modelos preditivos a partir de dados tabulares, como planilhas e bancos de dados.

A pesquisa TIC Governo Eletrônico 2021 (NIC.BR, 2022, p. 79), por sua vez, identificou que aplicações de IA são utilizadas por

> [...] quase metade dos órgãos federais (45%) e por 22% dos estaduais. Isso significa uma estimativa de que cerca de 70 órgãos do nível federal e 304 do estadual já utilizam ferramentas baseadas em IA em suas atividades. A adoção de IA ocorreu em maiores proporções em órgãos do Judiciário (53 órgãos), Legislativo (26 órgãos) e Ministério Público (15 órgãos), em que cerca de metade desses órgãos tinha alguma iniciativa desse tipo.

O estudo detectou também os tipos de IA mais utilizados.

> Tanto no nível federal quanto no estadual, os tipos mais mencionados foram aprendizagem de máquina para predição e análise de dados e automatização de processos de fluxo de trabalho [...]. Destaca-se ainda o uso de IA com tecnologias de mineração e análise de linguagem escrita por aproximadamente um a cada quatro órgãos federais. As demais tecnologias de IA investigadas foram utilizadas por menos de 20% dos órgãos, tanto no nível federal como no estadual, a exemplo do reconhecimento e do processamento de imagens, citados por 13% dos órgãos federais e 6% dos estaduais. (NIC.BR, 2022, p. 82).

Mapeamento e avaliação do uso de sistemas de RF

Reis et al. (2021) analisaram os usos de sistemas de RF nos três níveis federativos, prestando maior atenção, todavia, a estados e municípios. As autoras identificaram 25 casos diferentes de utilização da tecnologia em questão em áreas diversas – como transporte, educação e segurança pública – e distribuídos entre União, Distrito Federal, dez estados e nove municípios. A observação desses casos revelou um elemento comum a todos eles: "a falta de transparência e de mecanismos garantidores de proteção de dados e segurança na implementação das tecnologias de vigilância no Brasil" (REIS ET AL., 2021, p. 40). O estudo das autoras revela ainda que, ao menos em parte, esse déficit de governança se deve à inação dos Poderes Executivo e Legislativo para criar leis estaduais que rejam o uso da tecnologia.

O trabalho de Nunes (2019) apresenta dados iniciais sobre o uso de sistemas de reconhecimento facial pelas polícias de diferentes estados, enquanto Nunes et al. (2022) analisaram, especificamente, o caso fluminense, com foco na cidade do Rio de Janeiro. Ressalto dois fatos mencionados no primeiro desses dois estudos. Primeiramente,

> [o] governo federal tem dado sua contribuição para a expansão desta tecnologia, como, por exemplo, a portaria nº 793 de 24 de outubro de 2019, que regulamenta o uso de dinheiro do Fundo Nacional de Segurança Pública para o "fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por *Optical Character Recognition* – OCR, uso de inteligência artificial ou outros". (NUNES ET AL., 2022, p. 70).

O segundo é que, na avaliação de Nunes (2019), os usos dos sistemas de RF na segurança pública têm acontecido sem quaisquer preocupações ligadas à governança. De acordo com o pesquisador, tais usos não prestam atenção à LGPD, inviabilizando, assim, a *accountability* em relação aos *outputs* do sistema e a ações tomadas a partir deles.

Já Nunes et al. (2022) analisaram o uso de câmeras de RF pela polícia militar na cidade do Rio de Janeiro. O relato dos autores sugere que o governo estadual, sobretudo por meio da Secretaria de Estado de Polícia Militar (SEPM), optou por renunciar a qualquer preocupação com a governança da tecnologia. Ainda na primeira fase da iniciativa, os resultados dos sistemas de RF foram pífios. Relatórios oficiais da Polícia Militar apontam que nenhuma pessoa desaparecida foi encontrada e que

> [...] a correlação entre as faces capturadas e as faces reconhecidas corresponde a uma taxa de 0.082% de *matches* frente à quantidade de informação capturada, ou seja [...] um número baixo frente ao objetivo do projeto (NUNES ET AL., 2022, p. 12).

Além disso, a taxa de falsos positivos foi elevada. Os autores analisaram 11 detenções realizadas no entorno do estádio do Maracanã durante uma partida de futebol. Em apenas quatro casos as pessoas detidas tinham mandados de prisão em seus nomes. Os pesquisadores questionaram a SEPM sobre as outras sete. Inicialmente, obtiveram uma resposta

genérica. Após acionarem a Lei de Acesso à Informação (LAI), descobriram que, "[...] dentre os 11 casos de pessoas detidas com o uso da tecnologia de reconhecimento facial nas partidas do Maracanã, sete foram erros da máquina, ou seja: falsos positivos. Desta forma, o sistema errou em 63% dos casos" (NUNES ET AL., 2022, p. 13). Ainda assim, a iniciativa foi renovada e expandida para outras áreas da cidade.

O *think-and-do tank* Instituto Igarapé (2019), por sua vez, identificou que o número de casos em que tecnologias de RF são utilizadas para operacionalizar políticas públicas saltou de um, em 2011, para 47, em 2019. A instituição também observou que esses usos estavam difundidos por 30 municípios e 16 estados, e concentravam-se em quatro áreas de políticas públicas: transporte, segurança, controle de fronteiras e educação. Nesse universo, a maioria dos casos de uso relacionavam-se ao combate a fraudes em gratuidades de transporte coletivo, especialmente no transporte intermunicipal.

Informações levantadas por Brandão & Oliveira (2021) reforçam essa constatação. Os autores focaram apenas os 17 municípios brasileiros com pelo menos um milhão de habitantes e buscaram ocorrências do termo "reconhecimento facial" em edições de Diários Oficiais eletrônicos publicadas entre janeiro de 2010 e dezembro de 2020. Em dez localidades, identificaram usos de sistemas de RF que haviam sido descontinuados, que estavam em andamento ou em discussão. Em nove deles, o uso dessa tecnologia foi associado ao combate a fraudes em descontos e gratuidades no transporte coletivo; em quatro, a objetivos relacionados à segurança pública; em dois, à operacionalização de políticas de saúde e educação; e em um, a ações na área de assistência social.

Os trabalhos de Brandão & Arbix (2022) e de Brandão et al. (2022) aprofundaram os achados de pesquisa de Brandão & Oliveira (2021). Fazendo-se valer da LAI, os autores realizaram um *survey* junto aos órgãos de transporte coletivo dos 30 municípios brasileiros que atendem a pelo menos um de dois critérios: são capitais estaduais e/ou possuem pelo menos um milhão de habitantes. A investigação apurou qual é o

nível de responsabilidade no uso de sistemas de RF para a prevenção de fraudes em descontos e gratuidades assegurados por lei a públicos específicos, como estudantes e idosos.

Os autores constataram que, no universo pesquisado, 14 municípios utilizam a tecnologia em questão; quatro não a utilizam; e um estava implementando-a no momento da investigação. Demonstrando postura pouca atenta à transparência algorítmica, os outros 11 municípios não participaram da pesquisa. Desses, um ofereceu respostas inconclusivas sobre a utilização de sistemas de RF; quatro ignoraram por completo o pedido de informação; e os outros seis apresentaram problemas na plataforma digital pela qual a LAI é operacionalizada.

Brandão & Arbix (2022) observaram ainda que, entre os 14 municípios que recorrem à tecnologia, apenas cinco deles tomam cuidados consideráveis para que o uso da tecnologia se dê de maneira responsável. Os autores notaram, contudo, que, mesmo nessas localidades, o uso não é tão responsável quanto poderia ser. De modo geral, apontam os autores, os municípios não têm clareza sobre como podem e devem (i) preparar os funcionários públicos envolvidos com a utilização da tecnologia; (ii) utilizar a LGPD a favor da transparência algorítmica; (iii) utilizar a intervenção humana para corrigir resultados enviesados da tecnologia. Os municípios desconhecem ainda qual é o nível de segurança dos sistemas utilizados e se o valor das fraudes evitadas supera o custo dos sistemas empregados.

Em conjunto, os estudos revisados nesta subseção indicam que ainda faltam pesquisas sobre o uso de sistemas de RF em diferentes áreas de políticas públicas, como saúde, educação e assistência social. Eles também apontam que, nos casos em que as aplicações de RF já são empregadas, o uso é pouco ou nada responsável. Essa realidade precisa ser alterada. Para isso, é necessário que diferentes atores, como as organizações do Terceiro Setor e a Academia, se articulem a fim de demonstrar aos agentes públicos quais são os riscos sociais da tecnologia ora em tela e como eles podem ser prevenidos ou, pelo menos, mitigados. Caso con-

trário, os sistemas de RF piorarão a vida cotidiana dos cidadãos, ao invés de melhorá-la.

Referências

ADA Lovelace Institute et al. (2021). "Algorithmic accountability for the public sector – Learning from the first wave of policy implementation". Relatório técnico. Ada Lovelace Institute, AI Now and Open Government Partnership.

ANYOHA, R. (2017). "The History of Artificial Intelligence – Science in the news". Harvard University – The Graduate School of Arts and Science. Available at: https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/

ARBIX, G. (2020). A transparência no centro da construção de uma IA ética. Novos Estudos, CEBRAP, São Paulo, v39, n02, 395-413, MAI.–AGO. 2020.

BERRYHILL, J.; et al. (2019). Hello, World: Artificial intelligence and its use in the public sector. OECD Working Papers on Public Governance, n. 36, 2019.

BLACKWELL, A. (2020). "Objective Functions: (In)humanity and Inequity in Artificial Intelligence". In: Geoffrey E. R. Lloyd and Aparecida Vilaça (Ed.), Science in the Forest, Science in the Past. Hau Books: Chicago.

BRANDÃO, R.; Arbix, G. (2022) Artificial Intelligence, Ethics and Public Policy— The Use of Facial Recognition Systems in Public Transport in the Largest Brazilian Cities. Journal of Service Science and Management, 15, 551-575. doi: https://doi.org/10.4236/jssm.2022.155032

BRANDÃO, R.; et al. (2022). Artificial Intelligence, Algorithmic Transparency and Public Policies: The Case of Facial Recognition Technologies in the Public Transportation System of Large Brazilian Municipalities. In: Xavier-Junior, J.C., Rios, R.A. (eds) Intelligent Systems. BRACIS 2022. Lecture Notes in Computer Science), vol 13653. Springer, Cham. https://doi.org/10.1007/978-3-031-21686-2_39

BRANDÃO, R.; et al. (no prelo). Reconhecimento facial, viés algorítmico e intervenção humana: o caso do transporte público em grandes municípios brasileiros. In: I Seminário Internacional Inteligência Artificial: Democracia e Impactos Sociais, C4AI USP-FAPESP-IBM, dez. 2021. ***Este evento deu origem a um livro, que está em fase de elaboração. Ele será publicado ao longo de 2023. O trabalho em questão será um dos capítulos* **

BRANDÃO, R.; Oliveira, J. L. (2021). Reconhecimento facial e viés algorítmico em grandes municípios brasileiros. In: WORKSHOP SOBRE AS IMPLICAÇÕES DA

COMPUTAÇÃO NA SOCIEDADE (WICS), 2., Porto Alegre. Evento Online. Anais [...]: Sociedade Brasileira de Computação, p. 122-127. ISSN 2763-8707. DOI: https://doi.org/10.5753/wics.2021.15970

BUOLAMWINI, J. & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st conference on fairness, accountability and transparency, PMLR 81*, pp 77-91.

CALO, R.; Citron, D. (2020). The Automated Administrative State: A Crisis of Legitimacy (March 9, 2020). Emory Law Journal, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3553590

CJSUBIA – Comissão de Juristas Responsável por Subsidiar Elaboração de Substitutivo sobre Inteligência Artificial no Brasil. (2022). Relatório Final. Disponível em: https://legis.senado.leg.br/comissoes/mnas?codcol=2504&tp=4

COELHO, J. & Burg, T. (2020). "Uso de inteligência artificial pelo poder público". Relatório técnico. Transparência Brasil.

DAUGHERTY, P. & Wilson, J. (2018), Human + Machine. Reimagining Work in the Age of AI. Harvard Business Review Press, eBook Kindle.

DESOUZA, K. (2018). "Delivering Artificial Intelligence in Government: Challenges and Opportunities". Relatório técnico. IBM Center for The Business of Government.

ENGSTROM, D.; Ho, D. (2020). Algorithmic Accountability in the Administrative State. CSAS Working Paper 19-34; Technology, Innovation, and Regulation, November 15, 2019. Disponível em: https://administrativestate.gmu.edu/wp-content/uploads/2019/11/Engstrom-Ho-Algorithmic-Accountability-in-the-Administrative-State.pdf

EUBANKS, V. (2018). Automating Inequality – How Hig-Tech Tools Profile, Police, And Punish the Poor. New York: St. Martin's Press, 2018.

FUSSEY, P.; Murray, D. (2020). Policing Uses of Live Facial Recognition in the United Kingdom. In: Kak, A. (Org.). Regulating Biometrics – Global Approaches and Urgent Questions. Nova York: AI Now, p.78-85.

GILLESPIE, T. (2014). "The Relevance of Algorithms". In: Tarleton Gillespie, Pablo Boczkowski, Kirsten A. Foot (Ed.), Media Technologies: Essays on Communication, Materiality, and Society. The MIT Press: Cambridge, Massachusetts; London, England.

GOVERNO do Canadá, Página do "Digital Government Innovations". Disponível em: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations.html

GREEN, B. (2022). The Flaws of Policies Requiring Human Oversight of Government Algorithms. *Computer Law & Security Review*, Volume 45: https://ssrn.com/abstract=3921216 or http://dx.doi.org/10.2139/ssrn.3921216

GRIMMELIKHUIJSEN, S. (2022). Explaining Why the Computer Says No: Algorithmic Transparency Affects the Perceived Trustworthiness of Automated Decision-Making. Public Admin Rev. 2022; 1–22. **DOI**: 10.1111/puar.13483

HAO, K. (2019). "A **US** government study confirms most face recognition systems are racist", 20 de dezembro de 2019. Disponível em: https://www.technologyreview.com/2019/12/20/79/ai-face-recognition-racist-us-government-nist-study/ [consultado em 20-02-2021].

INSTITUTO Igarapé. (2019). "Infográfico – Reconhecimento facial no Brasil". Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

KUZIEMSKI, M.; Misuraca, G. (2020). **AI** governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. Telecommunications Policy 44 – 101976. https://doi.org/10.1016/j.telpol.2020.101976

LANGEVIN, C.; Fassio, R. (2022). "Guia de Contratações Públicas de Inteligência Artificial". Relatório técnico. C4**IR** – Centro para a 4ª Revolução Industrial.

MACIEIRA, A.; et al. (2020). "Os três pilares e cinco camadas para transformação digital nas prefeituras". In: Francisco Gaetani e José Henrique Paim (Org.), Os Municípios Vão às Nuvens – A Revolução Digital à Serviço do Desenvolvimento Local. **FGV** Editora: Rio de Janeiro, **RJ**.

NIC.BR. (2022). "Pesquisa sobre o uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro – **TIC** Governo Eletrônico 2021". Relatório técnico.

NUNES, P. (2019). "Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. Retratos da Violência: cinco meses de monitoramento, análises e descobertas – Junho a Outubro 2019". Relatório técnico. Ce**SEC** – Centro de Estudos de Segurança e Cidadania.

NUNES, P.; et. Al. (2022). Um Rio de olhos seletivos – uso de reconhecimento facial pela polícia fluminense. Digital book. Ce**SEC** – Centro de Estudos de Segurança e Cidadania, Rio de Janeiro.

OCDE – Organização para a Cooperação e Desenvolvimento. (2019). Hello, World: Artificial intelligence and its use in the public sector. *OECD Working Papers on Public Governance*, n. 36.

REIS, C.; et al. (2021). "Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil". Relatório técnico. LAPIN – Laboratório de Políticas Públicas e Internet.

RUBACK, L., et al. (2021). Vieses no Aprendizado de Máquina e suas Implicações Sociais: Um Estudo de Caso no Reconhecimento Facial. In: WORKSHOP SOBRE AS IMPLICAÇÕES DA COMPUTAÇÃO NA SOCIEDADE (WICS), 2., 2021, Porto Alegre. Evento Online. Anais [...]: Sociedade Brasileira de Computação. Disponível em: https://sol.sbc.org.br/index.php/wics/issue/view/765

SADOWSKI, J., & Bendor, R. (2019). Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary. Science, Technology, & Human Values, 44(3), 540–563. https://doi.org/10.1177/0162243918806061

SILVA, T. (2020). "Visão computacional e racismo algorítmico: branquitude e opacidade no aprendizado de máquina". Revista da ABPN 12(31), 428-448.

SURESH, H.; Guttag, J. (2021). A Framework for Understanding Sources of Harm throughout the Machine Learning Life Cycle. In Proceedings of EAAMO '21: Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO '21). ACM, New York, NY, USA, 9 pages. https: //doi.org/10.1145/3465416.3483305

TCU – Tribunal de Contas da União. (2022). "Levantamento de tecnologias emergentes – Inteligência Artificial". Relatório técnico. Disponível em: https://pesquisa.apps.tcu.gov.br/#/documento/processo/*/NUMEROSOMENTENUMEROS%253A666220218/DTAUTUACAOORDENACAO%2520desc%252C%2520NUMEROCOMZEROS%2520desc/0/%2520

VETRÒ, A.; et al. (2019). AI: from rational agents to socially responsible agents. DIGITAL POLICY, REGULATION AND GOVERNANCE. VOL. 21 NO. 3, pp. 291-304.

PARTE II

Formas de regulação e resistência às tecnologias de reconhecimento facial

“Tire Meu Rosto da Sua Mira”: Em busca do banimento de tecnologias de reconhecimento facial na segurança pública brasileira

Cynthia Picolo Gonzaga de Azevedo
Horrara Moreira
Rafaela Cavalcanti de Alcântara
Raquel Rachid

Resumo

A partir de articulações realizadas entre organizações sociais, a campanha *Tire Meu Rosto da Sua Mira* tem sua origem em um momento de expansão do uso das tecnologias de reconhecimento facial no Brasil e no mundo. Em razão de uma série de violações que essas tecnologias digitais representam, inclusive potencializando o racismo e a seletividade do sistema penal, a campanha entende que esse uso não pode ser objeto de regulação, contexto no qual almeja por seu respectivo banimento no âmbito da segurança pública brasileira. Assim, este artigo propõe-se a traçar o histórico da iniciativa, que em diálogo com mobilizações internacionais e por meio da capilarização da pauta pelo território nacional, pretende avançar para além da gramática dos direitos digitais. Nesse sentido, a campanha ainda apresenta uma agenda que entende pela insuficiência de mecanismos de diálogo sobre o tema que não se voltem ao efetivo banimento de ferramentas de reconhecimento facial nos moldes propostos.

Introdução

Diante de implementações pouco transparentes e controversas, a Campanha "Tire Meu Rosto da Sua Mira" é uma iniciativa composta por entidades articuladas em prol do banimento total das tecnologias de reconhecimento facial (TRF) na segurança pública brasileira. Lançada durante o Fórum da Internet no Brasil em 2022, a campanha tem suas origens nos debates ocorridos desde o primeiro semestre do ano de 2021, inicialmente, pelo conjunto de organizações que compõem a Coalizão Direitos na Rede (CDR). Esta, por sua vez, é uma rede de entidades que reúne mais de cinquenta organizações acadêmicas e do terceiro setor cujos principais temas de atuação envolvem o acesso à internet, a liberdade de expressão e a proteção dos dados pessoais.

Tendo em vista o contexto temático que guia a atuação das organizações que compõem a CDR, e a partir do consenso pela defesa do banimento total das TRF para fins de segurança pública, compreendeu-se que a rede não deveria capitanear a pauta isoladamente. Assim, a iniciativa, desde o princípio, tem somado esforços com entidades que tradicionalmente debatem temas como a segurança pública, o caráter racista do sistema penal brasileiro e o encarceramento em massa de populações historicamente estigmatizadas.

Nesse sentido, parte-se do entendimento de que o processo de digitalização na segurança pública e na persecução penal se insere em um cenário marcado por uma série de contradições e mazelas no Brasil, sendo necessário refletir a respeito desse panorama antes mesmo de se pensar na eventual incorporação de tecnologias digitais nessas áreas. Esta reflexão, inclusive, desafia a retórica de que essas tecnologias trazem soluções para problemas sociais anteriores e já enraizados.

Enquanto Campanha, ouvimos com frequência que banir é algo muito radical, que deve haver um "outro" jeito de aproveitarmos as

funcionalidades da tecnologia.[1] Mas, que jeito "outro" seria esse? Para nós, o posicionamento é inegociável e, diante das potenciais violações e ameaças a direitos conquistados, é inconcebível que a utilização de sistemas de reconhecimento facial ainda seja defendida como política de segurança pública eficiente. Ainda, apesar da agenda específica da Campanha, estamos cientes dos graves problemas decorrentes de outras formas de tecnovigilância baseadas em dados biométricos (incluindo voz, impressões digitais, contagem de passos, temperatura, batimentos cardíacos, DNA etc.). Essa preocupação de como os nossos dados biométricos estão sendo "sutilmente" coletados e analisados nos faz apoiar outras tantas iniciativas ao redor do mundo.

A Campanha defende, portanto, que as TRFs nunca devem ser usadas em atividades de segurança pública – seja pelo governo ou mesmo pelo setor privado, por meio da delegação da execução de serviços públicos. Isso porque, além de possuírem um alto potencial abusivo e discricionário em seu uso prático, são indiscutíveis e amplamente debatidas as possíveis falhas que essas tecnologias produzem, com consequências muito graves para determinados grupos (BUOLAMWINI & GEBRU, 2018). Essas consequências podem ser visíveis ou latentes, em especial quando se considera a vigilância contínua em tempo-real e a flexibilização da presunção de inocência. Então, as TRFs ou promovem danos graves em razão de erros ou "funcionam bem" e promovem vigilância em massa, além do reforço ao seletivismo penal.

Assim, as autoras abordam neste capítulo um conjunto de experiências advindas das articulações políticas em prol da agenda defendida pela Campanha, apresentando resultados dessas articulações e impactos concretos já observados.[2]

1 As autoras participaram da construção da Campanha em questão, contexto no qual fazem uso da terceira pessoa do plural no presente trabalho ao recorrerem a suas memórias e registros.

2 Como um texto que expressa argumentos propostos coletivamente contra o reconhecimento facial na segurança pública, não serão endereçadas as múltiplas pers-

Breves considerações em prol do banimento das TRFs na segurança pública

Mesmo em um cenário hipotético sem tantas das falhas danosas já observadas em situações concretas, uma suposta identificação por meio das TRFs na segurança pública tornaria o contexto de vigilância que promovem incompatível com o exercício da fruição dos espaços públicos. Seja pelo rastreio constante, que impossibilita o anonimato e inibe o exercício da liberdade de expressão, ou mesmo pela intensificação da perseguição a grupos já estigmatizados (como é o caso de profissionais do sexo, trabalhadores e trabalhadoras ambulantes, grupos considerados "suspeitos" em razão da criminalização da pobreza), não há que se falar em uma solução para seu uso (ver capítulos 1 e 2).

Ainda, como o racismo permeia as relações sociais, não se pode conceber que os bancos de dados do sistema penal estejam ilesos à sua marca. Assim, as TRFs tornam-se verdadeiros aparatos de vigilância à população geral e, especialmente, a grupos historicamente perseguidos. As TRFs e sua aplicação supostamente voltada à maior segurança da população são incompatíveis com garantias fundamentais. Por isso, pedimos pelo banimento do reconhecimento facial no contexto da segurança pública, e não apenas por uma moratória[3] (sendo esta última tão somente uma suspensão do uso até que a atividade seja regulada por atos normativos).

---

pectivas teóricas individuais de suas autoras – as quais agradecem a valiosa contribuição das pesquisadoras Thallita Lima e Karina de Paula, também integrantes da Campanha, quanto às leituras atentas que fizeram a título de revisão e aperfeiçoamento do texto.

3 Diante da pressão popular em face da impossibilidade de se eliminar as ameaças que essas tecnologias representam, até mesmo empresas como Amazon, IBM, Meta e Microsoft estão repensando o uso dessas ferramentas em alguns contextos.

Espaços institucionais de debate não necessariamente chancelam os posicionamentos da Campanha, como é o caso do que foi apresentado por meio do relatório publicizado em dezembro de 2022 pela Comissão de Juristas do Senado (BRASIL, 2022), convertido no Projeto de Lei nº 2338/2023 pelo Senador Rodrigo Pacheco[4]. O PL 2338/2023, que busca estabelecer normas para o desenvolvimento, implementação e uso responsável de sistemas de inteligência artificial (IA) no Brasil, considera em seu artigo 15 o uso de sistemas de IA para identificação biométrica na segurança pública como de risco excessivo, permitindo sua utilização quando da existência de lei federal específica e autorização judicial relativa à atividade de persecução penal em casos específicos (ver capítulo 6).[5]

Ao mesmo tempo em que o referido PL reconheceu os graves riscos das TRFs para fins de segurança pública, permitiu seu uso em determinadas situações – mesmo manifestando-se pela necessidade de regulamentação do uso dessas ferramentas, a o texto foi de encontro à proteção de direitos. Basta refletir em como, na prática, seria impossível o uso de TRFs para mirar apenas indivíduos suspeitos de crimes cuja pena máxima seja de reclusão superior a dois anos, por exemplo (art. 15, I, PL 2338/2023). A realidade é que um número indiscriminado de pessoas continuará, de todo modo, tendo seus dados coletados e sujeitos à vigi-

4 Senado Federal. Projeto de Lei nº 2338/2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233.

5 Art. 15. No âmbito de atividades de segurança pública, somente é permitido o uso de sistemas de identificação biométrica à distância de forma contínua em espaços acessíveis ao público, quando houver previsão em lei federal específica e autorização judicial em conexão com a atividade de persecução penal individualizada, nos seguintes casos: I – persecução de crimes passíveis de pena máxima de reclusão superior a dois anos; II – busca de vítimas de crimes ou pessoas desaparecidas; III – crime em flagrante. Parágrafo único. A lei a que se refere o caput preverá medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal e o controle judicial, bem como os princípios e direitos previstos nesta Lei, especialmente a garantia contra a discriminação e a necessidade de revisão da inferência algorítmica pelo agente público responsável antes da tomada de qualquer ação em face da pessoa identificada.

lância digital. Nesse sentido, a exposição de ideias em fóruns pontuais não tem se mostrado suficiente para o alcance de ações contundentes contra violações notórias.

Postergar a aceitação dessas tecnologias sob a justificativa de que o estabelecimento de regras para o seu uso daria conta de minorar o constrangimento que representam, é empregar uma lente ilusória e distante das tantas mazelas que cercam o sistema penal, que convive com situações absurdas e degradantes (BONFIM, 2022). Nesse sentido, a campanha acredita que são necessárias mudanças estruturais na forma como se conduz a segurança pública, entendendo que a ampliação das estruturas de vigilância com essas tecnologias não apenas deixa de trazer soluções, mas automatiza formas históricas de opressão (BROWNE, 2015).

A complexidade das TRFs apresenta-se tanto pelo modo como são desenvolvidas quanto pelo tipo de análise que fazem para atingir o objetivo esperado. De acordo com Boulamwini *et al* (2020), as tecnologias de reconhecimento facial podem ser definidas como um conjunto de ferramentas digitais utilizadas para realização de tarefas como a avaliação e verificação de rostos humanos, bem como podem ser classificadas a partir do seu tipo de uso. É importante destacar que o reconhecimento facial é uma tecnologia biométrica que utiliza algoritmos para automatizar o reconhecimento de diversos pontos faciais de uma pessoa, como é o caso da distância entre os olhos, por exemplo.

Entre os tipos de uso mais comuns de sistemas de reconhecimento facial temos: (i) a detecção de uma face, diferenciando um rosto de um objeto, por exemplo; (ii) a identificação de atributos da face como gênero, a cor da pele e dos olhos, o tamanho do nariz e da boca – a chamada "biometria facial"; (iii) a identificação de expressões faciais que supostamente levaria ao reconhecimento de emoções, como o sistema proposto pela ViaQuatro no metrô de São Paulo (IDEC, 2021) (ver capítulo 3); e (iv) a verificação de identidade, quando um usuário de um sistema tira uma *selfie* e fornece a foto do seu documento para que o software confirme tratar-se da mesma pessoa, como é o caso do procedimento de

autenticação para acesso à conta pessoal em aplicativos de bancos. Para além desses exemplos, há também a identificação facial que responde à pergunta *"de quem é esse rosto?";* neste caso, o algoritmo procura dentro de seu banco de dados informações sobre qual rosto corresponde à face capturada, aferindo uma pontuação de similaridade ou correspondência (ver introdução).

Foi o que ocorreu com Maria Lêda, em 2019, presa no Rio de Janeiro após o sistema de averiguação facial apontar mais de 70% de chance de ela ser uma pessoa que a Polícia Militar (PM) considerava foragida. Entretanto, a procurada já estava presa: "a verdadeira criminosa foi condenada em maio d[aquele] ano pelo IV Tribunal do Júri a sete anos de reclusão em regime semiaberto por homicídio, sem direito de recorrer em liberdade" (WERNECK, 2019).

Vale ressaltar que em Pequim, na China, tecnologias de reconhecimento facial foram utilizadas para identificar pessoas que foram a manifestações públicas contra as medidas restritivas do Covid Zero. "Embora a construção do sistema de vigilância não fosse segredo, para muita gente na China isso parecia muito remoto. A polícia usa para monitorar dissidentes, minorias étnicas e trabalhadores migrantes" (MOZUR *et al*, 2022). Ainda importa salientar que cidades dos Estados Unidos da América chegaram a utilizar soluções envolvendo tecnologias de reconhecimento facial para identificar pessoas que participaram dos protestos *Black Lives Matter*, após o assassinato de George Floyd (COX, 2020; RIHL, 2021).

No Brasil, país com a terceira maior população encarcerada do mundo (SANTOS, 2021), o uso de tecnologias de reconhecimento facial na segurança pública levaria ao agravamento de práticas racistas que constituem o sistema penal (FLAUZINA, 2006; MELO, 2021). Todavia, apesar da gravidade desses prejuízos, essas tecnologias já estão na grande maioria dos estados brasileiros (VENTURA, 2021). Na Bahia, desde 2018, câmeras de reconhecimento facial foram instaladas com a finalidade oficial de combate à criminalidade (FALCÃO, 2021), mas sem a compro-

vação de se ter efetivamente atingido tal objetivo – apesar das mais de 600 abordagens promovidas pela ferramenta (SSP-BA, 2023) (ver capítulos 1 e 2).

No âmbito da segurança pública, é importante destacar que, embora possa haver a impressão de que a coleta e o tratamento de dados biométricos são realizados somente pelo poder público, muitas dessas conduções são implementadas por meio de contratos com a iniciativa privada. Essas parcerias destinam-se à prestação de serviços que envolvem infraestrutura e ferramentas tecnológicas, podendo incluir o reconhecimento facial.

Com frequência, esses acordos público-privados são pouco transparentes e não fornecem à população detalhes relativos ao tratamento[6] dos dados — cenário que pode ter como consequência, dentre outras, o uso secundário de dados para finalidades de interesse exclusivo das entidades da iniciativa privada, em razão de serem recursos valiosos até mesmo para treinamento de algoritmos voltados à oferta de soluções mercadológicas (JUSTIÇA, 2020). Em outras palavras, não é rara a ocorrência de desvio de finalidade dos dados pessoais utilizados nesse tipo de projeto. As parcerias público-privadas demandam atenção especial, pois o acesso a informações de interesse público sobre esse tipo de arranjo não deveria ser dificultado sob o argumento de que elas estariam protegidas por segredo comercial ou empresarial, por exemplo.

Como já mencionado, mesmo que o Brasil possuísse uma lei em vigor para a regulação do processamento de dados pessoais na segurança pública, ainda assim os perigos que o reconhecimento facial representa não seriam eliminados (ver capítulo 6). Diante de um contexto em que

6 A Lei Geral de Proteção de Dados Pessoais (LGPD), em seu art. 5º, X, define as atividades de tratamento como sendo "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

fatores como racismo, classismo, misoginia e LGBTQIAP+fobia impactam a maneira por meio da qual as pessoas, em sua diversidade, têm seus corpos percebidos, reconhecidos, abordados e até mesmo discriminados e reprimidos, mecanismos cujo funcionamento se baseia na análise de rostos trazem preocupações específicas. Esse quadro é ainda mais preocupante no Brasil, país que mais mata pessoas trans e que é estruturalmente marcado por práticas de policiamento e vigilância racializadas (ONU, 2021a).

Apesar disso, no Brasil já existem câmeras de monitoramento munidas com esse tipo de tecnologia em ruas de diversas cidades, inclusive em relógios públicos e no transporte público (GODOY, 2019; DIAS, 2020; REIS *et al*, 2021). Soma-se a isso o fato de que o uso massivo dessas ferramentas em espaços comuns e frente a um grande número de pessoas, por sua própria natureza, ocorre de forma remota, sem o contato com as pessoas submetidas ao reconhecimento facial. Em geral, não há sequer ciência do uso dos dados biométricos por parte da população diretamente afetada. Assim, seu rosto pode também ter sido submetido ao reconhecimento facial para fins de segurança pública sem que você tenha se dado conta.

Ainda, há registros de que o reconhecimento facial seja também utilizado em aplicativos de celulares de policiais durante abordagens (RODRIGUES, 2019). A possibilidade de circular sem constrangimentos e exercer a fruição dos espaços das cidades, especialmente no caso de determinados grupos, segue ameaçada enquanto esse tipo de projeto existir. Nesse sentido, aqui é interessante também reproduzir trecho da nossa carta política:

> Independentemente das salvaguardas e correções que poderiam ser propostas para a criação de uma tecnologia alegada e supostamente "livre de erros", essa vigilância constante, massiva e indiscriminada é – em si mesma – uma violação dos direitos e das liberdades das pessoas. Por estarmos falando de mecanismos aplicados de forma incompatível com os direi-

> tos humanos, pedimos pelo banimento, e não apenas por uma moratória, do reconhecimento facial no contexto da segurança pública. (TIRE MEU ROSTO DA SUA MIRA, 2022)

Relevante também pontuar que os parâmetros internacionais de direitos humanos (aprofundados adiante) apontam no sentido de que restrições à privacidade e à liberdade de expressão devem obedecer aos princípios da necessidade e proporcionalidade. Como consequência, a vigilância biométrica massiva, aplicada de modo extensivo e indiscriminado torna-se incompatível com os direitos humanos ao, por princípio, estar impossibilitada de alcançar o crivo desses critérios (ARTICLE 19, 2021).

Aspectos internacionais

As TRFs têm ganhado corpo no debate internacional, não apenas pela sua atribuída "eficiência", mas pelas questões problemáticas relacionadas às falhas e à série de graves violações a direitos em diferentes partes do mundo. Um exemplo, retratado no documentário *Coded Bias* (2020), é o uso do reconhecimento facial pela polícia do Reino Unido e a associação incorreta (até o ano de 2018) de 98% dos rostos apontados como correspondentes a pessoas foragidas. Diante dessas preocupações, cidades como São Francisco e Oakland, nos Estados Unidos, baniram o uso de reconhecimento facial em locais públicos (VALENTE, 2019). Já na Itália, em dezembro de 2021, o parlamento introduziu uma moratória sobre sistemas de vigilância que empregam tecnologias de reconhecimento facial a partir das evidências de abusos causados por esses sistemas (PELINO, 2021).[7]

7 A moratória foi estabelecida até 31 de dezembro de 2023. Há que se acompanhar os desdobramentos do tema no país, incluindo eventual elaboração de uma nova lei em matéria de vigilância biométrica.

Em relação ao uso indevido de dados coletados por parte do setor privado, um caso conhecido internacionalmente e que exemplifica o uso de dados coletados pela iniciativa privada para fins de vantagem competitiva sem a ciência da população é o da empresa Axon, atual Taser (CASSANO, 2017). Ela utilizou dados gerados por câmeras corporais que havia doado previamente a departamentos de polícia estadunidenses no desenvolvimento interno de sua inteligência artificial, gozando de benefícios comerciais inestimáveis advindos da extração de dados aos quais dificilmente teria acesso não fosse essa prática unilateral.[8]

Imaginar que essa mesma situação pode ocorrer no Brasil, nos leva a conjecturar um cenário possivelmente desastroso para a nossa coletividade e relações político-sociais mais amplas. Isso porque o episódio representaria a imposição de proveito comercial opaco por meio de uma prática que não poderia ser aceita pela administração pública via instrumento de doação caso a contrapartida estivesse explícita, por exemplo.

É importante lembrar que o Brasil tem sido espaço de "laboratório de testes" para essas tecnologias, como aponta um levantamento da *Al Sur* – que mostra uma parcela significativa das tecnologias utilizadas no Brasil como oriundas de doações de empresas (AL SUR, 2021). Não é raro que, posteriormente ao "experimento", a iniciativa privada ofereça tais tecnologias para a administração pública a título oneroso, após sua incorporação ser tida como necessária – situação em que se observa um mercado proveitoso nesse ciclo de doação como "amostra grátis" (REIS *et al*, 2021).

Além da ausência de quaisquer parâmetros legislativos que busquem resguardar direitos (o que também não atende nossa reivindicação, como já exposto), o uso dessas ferramentas de forma massiva apresenta incoerências em relação a tratados internacionais com os quais o Brasil está comprometido – incluindo a Declaração Universal dos Direitos Humanos

8 Como exemplo de benefícios comerciais de coletas indevidas de dados pessoais, pode-se citar o uso de dados para fornecimento de publicidade direcionada, o mapeamento de perfis para moldar estratégias comerciais, ou até mesmo a revenda de base de dados a outras empresas.

(DUDH) e o Pacto Internacional de Direitos Civis e Políticos (PIDCP). O artigo 17 do PIDCP, por exemplo, protege as pessoas de sofrerem ingerências arbitrárias ou ilegais em suas vidas privadas. O artigo 12 da DUDH apresenta dispositivo com o mesmo conteúdo. Para além do chamado direito à privacidade, o debate internacional também inclui os direitos à liberdade de expressão e de reunião, por exemplo, quando aborda a vigilância massiva sofisticada pelo uso de tecnologias biométricas.

Isso porque são ferramentas "capazes de identificar, seguir, destacar individualmente e rastrear pessoas em todos os lugares aonde elas vão", como aponta a carta política da campanha (TIRE MEU ROSTO DA SUA MIRA, 2022). Uma consequência do impacto do direito à privacidade pelo uso massivo do reconhecimento facial é a restrição à possibilidade de se transitar em espaços públicos de maneira anônima. A limitação da possibilidade de transitar de forma não identificada em espaços públicos e desempenhar as mais diversas atividades – desde o uso de serviços públicos até a participação em um protesto – proporciona o chamado "efeito inibidor" (*chilling effect*), resultando no desencorajamento das pessoas quanto ao desempenho de atos comuns à vida urbana e participação democrática (ARTICLE 19, 2021).

Relevante destacar, por exemplo, que a Relatoria Especial das Nações Unidas sobre os direitos à liberdade de assembleia pacífica e de associação apresentou relatório (ONU, 2019) no qual aborda o uso de ferramentas digitais para vigilância. O documento relembra a aplicação do princípio da proporcionalidade no uso desses mecanismos, de onde deriva a necessidade de que a medida utilizada seja a opção menos invasiva disponível para aquele fim (parágrafo 56). A Relatoria menciona explicitamente preocupações com a proporcionalidade na utilização de tecnologias de reconhecimento facial em locais públicos com um grande número de pessoas, como amplos eventos culturais, esportivos, festivais de música e encontros políticos.

Em 2020, o Alto Comissariado das Nações Unidas para Direitos Humanos lançou relatório sobre o impacto dessas novas tecnologias no

contexto de assembleias, incluindo protestos pacíficos (ONU, 2020). A autoridade recomenda aos Estados que nunca utilizem tecnologias de reconhecimento facial para identificar pessoas que participam pacificamente em uma assembleia, instando moratórias no uso de reconhecimento facial nesses contextos até que as autoridades responsáveis possam demonstrar conformidade com os parâmetros aplicáveis, incluindo privacidade e proteção de dados (parágrafo 53).

Finalmente, é importante destacar o relatório (ONU, 2021b) apresentado posteriormente, em 2021, também pelo Alto Comissariado para Direitos Humanos, com o título "Direito à privacidade na era digital". Ao abordar princípios fundamentais que devem ser observados, o documento aponta que ferramentas de Inteligência Artificial (IA) – como é o caso do reconhecimento facial massivo – devem observar os requisitos de legalidade, legitimidade, necessidade e proporcionalidade, além de igualdade, não discriminação, participação e *accountability* (parágrafo 38). Nesse contexto, recomenda que os Estados reconheçam a necessidade de proteger e reforçar todos os direitos humanos no desenvolvimento, uso e governança da IA como um objetivo central, garantindo também que os requisitos citados anteriormente sejam observados (parágrafo 59). Além disso, também faz um chamado para que os Estados imponham uma "moratória no uso de reconhecimento biométrico remoto em espaços públicos" até que as autoridades responsáveis possam demonstrar observância com uma variedade de requisitos necessários para uma aplicação de IA compatível com os direitos humanos (parágrafo 59).

É inegável uma certa timidez dos organismos internacionais em endereçar o problema por meio de recomendações mais enfáticas, como é o caso do próprio banimento. No entanto, o fato de essas recomendações não serem automaticamente vinculantes confere espaço para avanços pelos Estados, mediados por mobilizações sociais. Somando-se a isso, os relatórios citados por si só demonstram a preocupação com o uso dessas ferramentas no que concerne ao impacto nos direitos hu-

manos, além de indicarem que limitações e freios aos respectivos usos caminham juntos à proteção da população.

Outras campanhas

A Campanha brasileira não está, evidentemente, isolada na reivindicação do banimento do reconhecimento facial. Ainda que outras iniciativas possuam especificidades, chamadas e/ou agendas próprias, as semelhanças permitem acúmulo de aprendizados e diálogos.

Nesse contexto, é interessante destacar a existência da campanha *Ban Biometric Surveillance*,[9] lançada no Brasil em dezembro de 2021.[10] A iniciativa contou com a coordenação e endosso de organizações que constroem a campanha *Tire Meu Rosto da Sua Mira*, apresentando uma carta aberta em que diversas entidades e indivíduos apoiam uma chamada global pelo banimento de tecnologias de reconhecimento facial e biométrico que possibilitem vigilância massiva e discriminatória – o que abrange a implementação em espaços públicos e espaços acessíveis ao público, bem como usos por governos e pelo setor privado.

A campanha destaca a potencial violação de direitos humanos nessas aplicações, pontuando que – por princípio – não podem ser contornados por garantias técnicas ou legais. Assim, a elaboração normativa que para algumas pessoas poderia dar conta da realidade material, converte-se em verniz para impactos sociais decorrentes do fortalecimento do sistema penal por essas tecnologias.

Aproveitando a existência de experiências anteriores, foram realizados encontros *online* entre a campanha *Tire Meu Rosto da Sua Mira* e representantes de outras iniciativas de associações internacionais. Ainda que internamente tenham ocorrido eventuais alinhamentos entre o co-

9 Mais informações em: https://www.accessnow.org/ban-biometric-surveillance/

10 Para acesso ao texto em português: https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Portuguese.pdf

letivo da Campanha brasileira sobre como se dariam esses diálogos, não estiveram vinculados a *scripts* ou a uma lista de perguntas previamente elaboradas, uma vez que se pretendia a construção de espaços de interação irrestrita.

Foram realizadas quatro reuniões entre o final de 2021 e os primeiros meses de 2022. Esses momentos foram sistematizados por uma profissional de facilitação gráfica, cujo conteúdo produzido (exemplos na Imagem 1 e na Imagem 2) seria posteriormente utilizado para divulgação de destaques dos diálogos de forma mais dinâmica do que extensas relatorias, além de representar ferramentas de registro e memória da construção da campanha brasileira possíveis de serem utilizados mais à frente como material de comunicação.

IMAGEM 1. Facilitação gráfica da reunião entre a Campanha Tire Meu Rosto da Sua Mira e a Campanha Argentina #ConMiCaraNo

Fonte: Arquivo da Campanha Tire Meu Rosto da Sua Mira.

IMAGEM 2. Facilitação gráfica da reunião entre a Campanha Tire Meu Rosto da Sua Mira e representante do Conselho Municipal de Oakland

Fonte: Arquivo da Campanha Tire Meu Rosto da Sua Mira.

Em outubro de 2021, ocorreu o primeiro dos encontros, com um representante do Conselho Municipal de Oakland – cidade da Califórnia (Estados Unidos) que proibiu o uso de reconhecimento facial pela administração pública municipal (LECHER, 2019). É possível inferir que as reflexões que essa conversa proporcionou para a Campanha brasileira – lançada no ano subsequente – tenham levado à realização das conversas posteriores com as outras iniciativas.

Na sequência, foram realizados encontros com representantes da *Asociación por los Derechos Civiles* (ADC), organização responsável pela iniciativa *Con Mi Cara No*, que trabalha contra o uso de ferramentas de reconhecimento facial por forças de segurança pública e de inteligência na Argentina; do *European Digital Rights* (EDRi), coalizão de organizações que lidera a campanha *Reclaim Your Face* no continente europeu, com o objetivo de questionar o uso de reconhecimento facial e banir a

vigilância biométrica em massa;[11] e da *Red en Defensa de los Derechos Digitales* (R3D), que organiza a iniciativa *No Nos Vean La Cara* no México e busca chamar atenção para as violações de direitos humanos decorrentes da utilização de ferramentas de reconhecimento facial por parte do governo.[12]

Os encontros, como um todo, possibilitaram o compartilhamento de experiências dos mais diversos tipos com a iniciativa brasileira, incluindo potenciais atividades que poderiam inspirar e/ou servir como referência de "boas-práticas", além de aprendizados que poderiam auxiliar na construção da campanha no Brasil.[13]

Resumidamente, é possível dizer que, a partir do aprendizado decorrido das experiências internacionais, o coletivo brasileiro traçou eixos de atuação, levando em consideração a importância da sensibilização de vários públicos; a necessidade de aproximação de atores-chave em todas as esferas; uma atuação coordenada, que conte inclusive com parcerias; o monitoramento constante da implementação de tecnologias de reconhecimento facial em todo território nacional; o engajamento com veículos midiáticos; e, um dos pontos principais, a amplificação de histórias de abusos reais.

11 No encontro, foi citada ainda a campanha suíça "Stop au contrôle au faciès", originada dos esforços da EDRi, que advoga pelo banimento do reconhecimento facial em espaços públicos. Disponível em: https://www.stop-reconnaissancefaciale.ch/.

12 ConMiCaraNo (http://conmicarano.adc.org.ar/), Reclaim Your Face (https://reclaimyourface.eu/), No Nos Vean La Cara (https://nonosveanlacara.r3d.mx/) e Ban Biometric Surveillance (https://www.accessnow.org/ban-biometric-surveillance/).

13 Referenciando essas iniciativas, cabe registrar nosso agradecimento pelo aprendizado com as experiências internacionais – cuja rede de interações segue sendo muito relevante à campanha brasileira.

Construção e resultados da campanha no Brasil

A articulação de organizações sem fins lucrativos por meio da Coalizão Direitos na Rede tradicionalmente consolida posicionamentos em reuniões periódicas, com abertura para manifestações por parte das entidades. Assim, o debate sobre os perigos do uso de tecnologias de reconhecimento facial levou ao referendo do posicionamento defendido pela Campanha.

Nesse processo de conversas em busca de um posicionamento consensual relativo ao tema, houve muitas manifestações sobre a insuficiência de o escopo da Campanha ser circunscrito à segurança pública, nos marcos do que a Constituição Federal aponta pelo texto de seu art. 144.[14] Isso porque haveria razões para banir outros usos os quais também poderiam levar a potenciais prejuízos à população (como é o caso do uso dessas tecnologias em espaços públicos e em outros setores da administração pública, incluindo escolas públicas).

O posicionamento consolidado pelo conjunto das entidades que integram a CDR foi pela defesa do banimento do reconhecimento facial na segurança pública brasileira[15], havendo ainda a necessidade de amplia-

14 Ainda que haja vastas considerações teóricas críticas ao aparato voltado ao exercício da força pelo Estado, apontando sua existência como ferramenta de gestão da desigualdade e do *status quo* (VITALE, 2021), bem como de realização das relações sociais sob o capitalismo (MCQUADE, 2012), a Constituição Federal da República Federativa do Brasil de 1988 reconhece que "a segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio", por meio da atuação das polícias. Ainda, é importante frisar a dificuldade prática de distanciar a esfera da segurança pública em face da dimensão que costuma ser nomeada de "persecução penal" no contexto do tratamento de dados, o que demanda uma avaliação também crítica ante a propostas de incorporação de TRF neste último âmbito.

15 Considerando que durante o período de consolidação de um posicionamento único pela rede, o banimento do reconhecimento facial na segurança pública foi o aspecto tido como consenso entre as entidades; o alargamento da pauta foi en-

ção daquele debate para entidades que também tivessem preocupações com potenciais abusos, dado o contexto já relatado. Ainda, durante as conversas foi possível tratar de temas conexos – como é o caso do reconhecimento fotográfico.

Assim, iniciou-se um processo de convite a outras entidades para uma reunião que desse início aos movimentos embrionários da campanha, incluindo-se convites a organizações que atuam em pautas atreladas ao fortalecimento da dignidade de populações estigmatizadas (como profissionais do sexo, trabalhadores e trabalhadoras ambulantes, pessoas negras, por exemplo). Durante essa reunião, foi provido um panorama sobre o tema e espaço para diálogo, bem como foi proposta a organização do movimento por meio de grupos de trabalho temporários – os quais dessem conta de estruturar três esferas centrais de atuação, a saber: a) carta-manifesto que representaria o pleito, desdobrando ações futuras; b) levantamento sobre projetos de lei brasileiros que se relacionassem com a temática; e c) oficinas formativas sobre o tema.

Após meses de trabalho e uma série de reuniões para debate e formulação, a carta-manifesto da Campanha e um relatório preliminar sobre os projetos de lei analisados foram validados. Assim, foi possível propor uma oficina durante o mês de dezembro de 2021 para que esses resultados fossem debatidos e confirmados. Nesse sentido, a Campanha pôde dar início a uma nova fase de ampliação de sua bandeira, contando com acúmulos imprescindíveis.

Em maio de 2022, durante o Dia Zero do Fórum da Internet no Brasil (FIB12), na cidade de Natal (RN), foi realizado o lançamento da Campanha. Nessa oportunidade, a iniciativa já contava com uma página na Internet para acesso ao texto da carta-manifesto assinado por instituições e pessoas que o haviam validado previamente. Além disso, novas assinaturas foram coletadas durante o evento.

---

tendido como facultado àquelas que desejassem se juntar a outros movimentos que partem de questionamentos mais abrangentes.

Para além do lançamento da campanha, a iniciativa teve a oportunidade de conduzir um painel a respeito do banimento do reconhecimento facial na segurança pública no último dia do FIB12.[16] Na sequência, foi a vez de aproveitar o espaço da *RightsCon* – conferência internacional anual sobre direitos humanos na era digital – para apresentar a iniciativa e debater possíveis caminhos quanto ao desafio de divulgar e expandir a tese de que o reconhecimento facial na segurança pública não retorna segurança às populações.[17]

No contexto dos debates semanais que a Campanha conduz, reuniões que constituem o fórum deliberativo da iniciativa, foi possível articular projetos em prol da agenda defendida por meio de parcerias com entidades financiadoras, caso dos projetos executados com apoio da Fundação Heinrich Böll e da Access Now.

Ainda, é importante mencionar iniciativas brasileiras correlatas com as quais a Campanha pôde dialogar, destacando-se a "Sai da Minha Cara" (CODING RIGHTS, 2022) e a campanha "Sem Câmera na Minha Cara" (MEU RECIFE, s.d.) – a primeira, mobilizou mais de 50 mandatos parlamentares de todas as regiões do Brasil para a proposição de projetos de lei que impusessem o banimento do uso de tecnologias de reconhecimento facial pela administração pública. A segunda segue mobilizando a agenda pró-banimento na cidade de Recife, após iniciativa da prefeitura para instalação de câmeras de reconhecimento facial pelo município.

No ano de 2022 estivemos presentes em mobilizações pelo Brasil, como o Festival Todo Mundo tem Direitos, promovido pela Assembleia Legislativa do Rio de Janeiro (Alerj); o diálogo promovido em praça pública sobre o que é o reconhecimento facial na segurança pública, tam-

16 A gravação do painel "Reconhecimento Facial: considerações sobre o banimento desta tecnologia digital na segurança pública brasileira" pode ser acessada por meio de: https://www.youtube.com/watch?v=2uJlbZnVqK4&list=PLQq8-9yVHyObTEl6bzX592mUU_zhy6KDt&index=26.

17 Site oficial da conferência: https://www.rightscon.org/.

bém no Rio de Janeiro; ações de incidência política na cidade de Curitiba, considerando um projeto de lei proposto para banimento das TRF; e a articulação política contra a permissão do uso de TRF no Estado do Ceará. Tais mobilizações contribuíram com a ampliação da rede de apoio à campanha, bem como com a percepção dos argumentos que mais mobilizam as pessoas em favor dessa causa – além do entendimento de que há públicos que não se mostram convencidos pelo banimento nos moldes apresentados por razões que vão desde um posicionamento favorável ao vigilantismo a realidades distantes das mazelas do sistema penal.

A partir dessas experiências, é também notória a necessidade de capilarização das articulações atuais, alcançando movimentos sociais diversos e apoio da população contra projetos que prometem segurança e entregam vigilância (seletiva, racializada, cara e falha). Nesse sentido, a Campanha pôde contribuir com as mobilizações de pressão à Prefeitura do Município de São Paulo em prol da suspensão do edital publicado para a execução do "*Smart Sampa*" (MARTINS, 2022), um projeto que propõe a contratação de mais de 20 mil câmeras de videomonitoramento pela Secretaria de Segurança Urbana de São Paulo e que incluía monitoramento de permanência nos espaços da cidade por cor da pele, cruzamento de bases de dados geridas pela secretaria de segurança com outras bases (como da saúde, da educação e do transporte) e implementação das tecnologias de reconhecimento facial, dentre outras problemáticas.

A campanha *Tire Meu Rosto da Sua Mira* reconhece a relevância da suspensão do pregão eletrônico relativo ao programa *Smart Sampa*, celebrando a mobilização de organizações sociais junto de instituições como a Defensoria Pública e a OAB, para além de gabinetes parlamentares envolvidos no diálogo com a população. Ainda, segue entendendo pela necessidade de problematizar o projeto, contestando sua falsa narrativa de entregar melhor segurança à cidade – ao passo que o que propõe, de fato, é a reconfiguração da gestão pública, abrindo brechas para um projeto de "cidade inteligente" ser pautado pela via da seguran-

ça urbana. Assim, seguiremos acompanhando os debates futuros a fim de fortalecer as mobilizações sociais para o enfrentamento a projetos descabidos como esse.

Por fim, para que os materiais até esse momento elaborados pela campanha *Tire Meu Rosto da Sua Mira* fiquem à disposição para ampla utilização, o repositório https://tiremeurostodasuamira.org.br foi confeccionado. Por meio desta página, é possível acessar e assinar a carta -manifesto; ter acesso a notícias sobre as TRF; baixar documentos e pesquisas publicizados; verificar um mapeamento sobre projetos de lei que tratam da matéria no Brasil; e acompanhar as atividades da Campanha. Além disso, é relevante indicar que a iniciativa também está presente em redes sociais tais quais: *Instagram*, *Telegram*, *Twitter*, *Facebook*, *TikTok* e *YouTube*. Ainda, para além de compartilhar conteúdos, a Campanha segue à disposição de novas contribuições que potencializem a pauta do banimento do reconhecimento facial na segurança pública brasileira.

Considerações finais

Como observado, as TRFs – além de serem parciais, falharem e representarem desperdício de dinheiro público – estão ampliando as práticas de vigilância e flexibilizando direitos. Destacando-se a ameaça das tecnologias de reconhecimento facial ao exercício do direito de protesto, por exemplo, reconhecemos que manifestações públicas nas ruas são expressões que devem ser garantidas à população ante ao risco de sua eventual criminalização.

A possibilidade de ser alvo de vigilância permanente pode levar as pessoas a mudarem seus comportamentos, assumindo uma postura de autocensura – assim, mobilizações legítimas podem ser inibidas. A autocensura pode atingir de maneira mais profunda grupos mais vulnerabilizados pela repressão e pela violência estatal. Em casos limites, o uso dessas tecnologias pode ensejar até mesmo a criminalização do direito de protesto.

Em face da intensificação das propostas de implementação de TRF como tendência, dado o acirramento de contradições sociais, entendemos por central o reforço ao movimento proposto pela Campanha quanto à ampliação das representações de grupos ainda não atuantes em seu bojo. A pressão pelo banimento a partir do uso de todos os meios disponíveis para isso (incluídos litígios judiciais) deve ir para além do diálogo com as instituições – que, via de regra, adotam posições conservadoras.

Diante das assimetrias informacionais no Brasil, nosso esforço vem sendo, então, o de mobilizar movimentos políticos que alarguem as discussões a respeito do uso de TRF – em especial, na segurança pública – como forma de alerta ao impacto que essas tecnologias causam à vida de milhares de pessoas, problematizando o sistema penal. Ainda, vale indicar a importância de atuações diretas de pressão institucional para constrangimento de autoridades que validem tais usos, atribuindo a essas decisões os danos que certamente recairão sobre a parte da população que já sofre com as agruras impostas pelo seletivismo do sistema penal.

Apesar de alegações de um pretenso aprimoramento da segurança pública por meio do uso de tecnologias de reconhecimento facial, esse tipo de projeto reproduz a cultura do punitivismo e do encarceramento (ver capítulo 2). Há evidências que mostram como essas tecnologias são usadas de modo abusivo e/ou implementadas com pouca ou nenhuma transparência – quadro que sequer permite que a população questione a maneira como elas funcionam.

Trata-se de um uso de tecnologias de vigilância que, por ser tão perigoso, deve ser rejeitado. Muito longe de um posicionamento utópico, atuamos com base na possibilidade de realização de outros futuros. Acreditamos que podemos construir coletivamente práticas que tornem o debate inclusivo, buscando formas de resistência que gerem atrito, pausem (como aconteceu com a iniciativa "*Smart Sampa*") e possam banir o uso dessas tecnologias na segurança pública no Brasil.

Referências

AL SUR. **Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa.** 2021. Disponível em: https://www.alsur.lat/reporte/reconocimiento-facial-en-america-latina-tendencias-en-implementacion-una-tecnologia. Acesso em: 14 jan. 2023.

ARTICLE 19. 2021. When bodies become data: Biometric technologies and freedom of expression. Disponível em: https://www.article19.org/resources/biometric-technologies-expression-must-be-protected/. Acesso em: 3 abr. 2023.

BONFIM, Denise. Preso diz ter sido obrigado a comer casca de banana com fezes em SP. Ponte Jornalismo, 2022. Disponível em: https://ponte.org/preso-diz-ter-sido-obrigado-a-comer-casca-de-banana-com-fezes-em-sp/. Acesso em 11 mar. 2023.

BRASIL. Relatório Legislativo. Brasília: Senado Federal, 2022. Disponível em: https://legis.senado.leg.br/comissoes/comissao?codcol=2504. Acesso em: 22 fev. 2023.

BROWNE, Simone. Dark matters. Duke University Press, 2015.

BUOLAMWINI, Joy; ORDÓÑEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. Facial recognition technologies: a primer. **The Algorithmic Justice League**, 2020. Disponível em: https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf. Acesso em: 28 dez. 2022.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. Conference on fairness, accountability and transparency. PMLR, 2018.

CASSANO, Jay. Police Body Camera Company, Axon, Is Vacuuming In Data, Stoking Privacy Concerns. **International Business Times**, 2017. Disponível em: https://www.ibtimes.com/political-capital/police-body-camera-company-axon-vacuuming-data-stoking-privacy-concerns-2579107. Acesso em: 14 jan. 2023.

CODED BIAS. Direção: Shalini Kantayya. Produção de Sabine Hoffman e Shalini Kantayya. China, Estados Unidos da América, Reino Unido da Grã-Bretanha e Irlanda do Norte: Netflix, 2020.

CODING RIGHTS. Parlamentares de todas as regiões do Brasil apresentam projetos de lei pelo banimento do reconhecimento facial em espaços públicos, 2022. Disponível em: https://medium.com/codingrights/parlamentares-de-todas-as-regi%C3%B5es-do-brasil-apresentam-projetos-de-lei-pelo-banimento-do-ad33a8e6552e. Acesso em: 14 jan. 2023.

COX, Kate. Cops in Miami, NYC arrest protesters from facial recognition matches. **arsTECHNICA**, 2020. Disponível em: https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches/. Acesso em: 14 jan. 2023.

CRUZ, Bruna Souza. Com didatismo, "Coded Bias" é um "O Dilema das Redes" sobre falhas das IAs. **TILT**, 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/04/10/coded-bias-da-netflix-prova-como-a-tecnologia-e-racista-e-viola-direitos.htm. Acesso em: 14 jan. 2023.

DIAS, Tatiana. As perguntas que o Metrô de São Paulo não respondeu antes de vender seu rosto por R$58 milhões. **The Intercept Brasil**, 2020. Disponível em: https://theintercept.com/2020/02/11/metro-sao-paulo-reconhecimento-facial/. Acesso em: 14 jan. 2023.

FALCÃO, Cintia. Lentes Racistas. Rui Costa está transformando a Bahia em um laboratório de vigilância com reconhecimento facial. **The Intercept Brasil**, 2021. Disponível em: https://theintercept.com/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/. Acesso em: 14 jan. 2023.

FLAUZINA, Ana Luiza Pinheiro. Corpo negro caído no chão: o sistema penal e o projeto genocida do Estado Brasileiro. Dissertação de Mestrado. 2006. Universidade de Brasília. Disponível em: http://www.cddh.org.br/assets/docs/2006_AnaLuizaPinheiroFlauzina.pdf.

GODOY, Ana Luiza. Vereadores conhecem detalhes do cercamento eletrônico. **Câmara POA**, 2019. Disponível em: https://www.camarapoa.rs.gov.br/noticias/vereadores-conhecem-detalhes-do-cercamento-eletronico. Acesso em: 14 jan. 2019.

IDEC. 2021. Idec obtém vitória contra reconhecimento de emoções no Metrô de SP. Disponível em: https://idec.org.br/noticia/idec-obtem-vitoria-contra-reconhecimento-de-emocoes-no-metro-de-sp. Acesso em: 25 fev. 2023.

JUSTIÇA. Justiça dá 30 dias para que Metrô de SP esclareça projeto de câmeras de reconhecimento facial. **G1SP**, 200. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2020/02/12/justica-da-30-dias-para-que-metro-de-sp-esclareca-projeto-de-cameras-de-reconhecimento-facial.ghtml. Acesso em: 14 jan. 2023.

LECHER, Colin. Oakland city council votes to ban government use of facial recognition. **The Verge**, 2019. Disponível em: https://www.theverge.com/2019/7/17/20697821/oakland-facial-recogntiion-ban-vote-governement-california. Acesso em: 22 fev. 2023.

MCQUADE, Brendan. Carceral Forms and Penal Practice from Paulo Condor to the PATRIOT Act: When counterrevolutionary Chickens Come Home to Roost. (In)

SHANTZ, Jeff. Protest and Punishment: the repression of resistance in the era of neoliberal globalization. Carolina do Norte: Carolina Academic Press, 2012.

MARTINS, Lívia. Após questionamentos, Prefeitura de São Paulo suspende pregão eletrônico para contratar sistema de reconhecimento facial. TV Globo, São Paulo, 2 dez. 2022. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2022/12/02/apos-questionamentos-prefeitura-de-sao-paulo-suspende-pregao-eletronico-para-contratar-sistema-de-reconhecimento-facial.ghtml. Acesso em: 25 fev. 2023.

MELO, Paulo Victor. A serviço do punitivismo, do policiamento preditivo e do racismo estrutural. **Le Monde Diplomatique Brasil**, 2021. Disponível em: https://diplomatique.org.br/a-servico-do-punitivismo-do-policiamento-preditivo-e-do-racismo-estrutural/. Acesso em: 14 jan. 2023.

MEU RECIFE. Sem Câmera na Minha Cara, s.d. Disponível em: https://www.semcameranaminhacara.meurecife.org.br/. Acesso em: 15 jan. 2023.

MOZUR, Paul; FU, Claire; CHIEN, Amy Chang. China usa reconhecimento facial para rastrear manifestantes contra Covid zero: 2022. **The New York Times**, republicado por Folha de São Paulo. Disponível em: https://www1.folha.uol.com.br/mundo/2022/12/china-usa-reconhecimento-facial-para-rastrear-manifestantes-contra-covid-zero.shtml. Acesso em 27/12/2022.

ONU. A/HRC/41/41: Rights to freedom of peaceful assembly and of association – Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association. Nações Unidas, 2019. Disponível em: https://www.ohchr.org/en/documents/thematic-reports/ahrc4141-rights-freedom-peaceful-assembly-and-association-report-special. Acesso em: 22 fev. 2023.

ONU. A/HRC/44/24: Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests. Nações Unidas, 2020. Disponível em: https://www.ohchr.org/en/documents/thematic-reports/ahrc4424-impact-new-technologies-promotion-and-protection-human-rights. Acesso em: 22 fev. 2023.

ONU. Brasil é o país que mais mata travestis e pessoas trans no mundo, alerta relatório da sociedade civil entregue ao UNFPA. Nações Unidas Brasil, 2021a. Disponível em: https://brasil.un.org/pt-br/110425-brasil-e-o-pais-que-mais-mata-travestis-e-pessoas-trans-no-mundo-alerta-relatorio-da. Acesso em: 14 jan. 2023.

ONU. Right to privacy in the digital age. Genebra: 2021b. Disponível em: https://digitallibrary.un.org/record/3945627?ln=en. Acesso em: 14 jan. 2023.

PELINO, Enrico. Riconoscimento facciale, perché la moratoria non basta: tutti i nodi della norma italiana. **Network. Digital** 360, 2021. Disponível em: https://www.agen-

dadigitale.eu/sicurezza/privacy/riconoscimento-facciale-perche-la-moratoria-non-basta-tutti-i-nodi-della-norma-italiana/#:~:text=La%20nuova%20previsione%20che%20dispone,sulle%20caratteriste%20biometriche%20dei%20volti. Acesso em: 22 fev. 2023.

REIS, Carolina; ALMEIDA, Eduarda; DA SILVA; Felipe; DOURADO, Fernando. Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil. Brasília: Laboratório de Políticas Públicas e Internet, 2021.

RIHL, Juliette. Emails show Pittsburgh police officers accessed Clearview facial recognition after BLM protests. **PublicSource**, 2021. Disponível em:

HTTPS://WWW.PUBLICSOURCE.ORG/PITTSBURGH-POLICE-FACIAL-RECOGNITION-BLM-PROTESTS-CLEARVIEW/. Acesso em: 14 jan. 2023.

RODRIGUES, Rubens. Policiais poderão fazer reconhecimento facial de suspeitos nas ruas usando câmera do celular. **O Povo**, 2019. Disponível em: https://www.opovo.com.br/noticias/fortaleza/2019/10/10/policiais-poderao-fazer-reconhecimento-facial-de-suspeitos-nas-ruas-usando-camera-do-celular.html. Acesso em: 14 jan. 2023.

SANTOS, Boaventura de Sousa. Contra o racismo carcerário. **Carta Capital**, 2021. Disponível em: https://www.cartacapital.com.br/opiniao/contra-o-racismo-carcerario/. Acesso em: 14 jan. 2023.

TIRE MEU ROSTO DA SUA MIRA. 2022. **Carta Aberta pelo banimento total do uso das tecnologias digitais de Reconhecimento Facial na Segurança Pública.** Disponível em: https://tiremeurostodasuamira.org.br/carta-aberta/. Acesso em: 3 abr. 2023.

SSP-BA. 2023. Chega a 612 o número capturados pelo Reconhecimento Facial. Secretaria de Segurança Pública do Estado da Bahia. Disponível em: https://www.ssp.ba.gov.br/2023/02/13143/Chega-a-612-o-numero-capturados-pelo-Reconhecimento-Facial.html. Acesso em: 25 fev. 2023.

VALENTE, Jonas. Tecnologias de reconhecimento facial são usadas em 37 cidades no país. **Agência Brasil**, 2019. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/tecnologias-de-reconhecimento-facial-sao-usadas-em-37-cidades-no-pais. Acesso em: 14 jan. 2023.

VENTURA, Layse. Tecnologia de reconhecimento facial chega a 20 estados. **Olhar Digital**, 2021. Disponível em: https://olhardigital.com.br/2021/07/10/seguranca/tecnologia-de-reconhecimento-facial-chega-a-20-estados/. Acesso em: 14 jan. 2023.

VITALE, Alex. **Fim do Policiamento**. São Paulo: Autonomia Literária, 2021.

WERNECK, Antônio. Reconhecimento facial falha em segundo dia, e mulher inocente é confundida com criminosa já presa. **O Globo, 11 jul. 2019**. Disponível em: https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913. Acesso em: 27 dez. 2022.

A LGPD Penal e a lacuna regulatória no tratamento de dados pessoais sensíveis por profissionais de segurança

Bianca Kremer
Fernanda dos Santos Rodrigues Silva

Resumo

O capítulo analisa o panorama regulatório atual em matéria de tratamento de dados pessoais no campo da segurança pública e investigações criminais, abordando os processos de discussão em curso por uma LGPD Penal no Brasil. Para tanto, partimos de um questionamento sobre quais são as lacunas regulatórias deixadas pela exceção do Art. 4º, III, da LGPD e seus impactos na segurança jurídica das relações permeadas pelo tratamento de dados pessoais sensíveis para fins de segurança pública. O capítulo utiliza um processo metodológico a partir do uso de técnicas de revisão bibliográfica e análise de legislações, projetos e anteprojetos de Lei. Por fim, o capítulo explora casos concretos e aspectos críticos sobre a interseção entre essa lacuna regulatória e a (des)proteção de dados pessoais sensíveis em contexto de grupos marginalizados, especialmente pessoas negras e pobres no Brasil.

Introdução

Diante das implicações promovidas pelo mundo digital, a modernização dos aparatos de investigação tem gerado desafios às forças de segu-

rança e ao sistema de justiça. De um lado, a necessidade premente de modelos modernos de investigação criminal e novas abordagens para a repressão de condutas impulsionadas pelas novas tecnologias. De outro lado, a ausência de regulamentação jurídica específica sobre o uso de dados pessoais e sistemas automatizados pelos órgãos de segurança pública, e um desconhecimento geral sobre os tipos de tecnologias que têm sido adotados, suas finalidades e extensão de uso.

A proposta de uma LGPD Penal no Brasil possui altíssima relevância dentro de um cenário social cada vez mais hiperconectado e movido a dados. A Lei Geral de Proteção de Dados (LGPD) entrou em vigor em setembro de 2020 com o objetivo de proporcionar ao cidadão brasileiro um controle maior sobre o tratamento de seus dados pessoais, mas excluiu do seu escopo de aplicação o tratamento realizado para fins exclusivos de segurança pública, defesa nacional, segurança de Estado e persecução penal (Art. 4º, III). Desse modo, a LGPD determinou que a matéria seja regulada por legislação específica e estabeleceu diretrizes para sua elaboração.

Com o intuito de suprir essa lacuna legislativa, uma comissão de juristas apresentou à Presidência da Câmara dos Deputados em novembro de 2020 o Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal (APL), também conhecido como LGPD Penal. Trata-se de um texto cujo processo de construção durou cerca de um ano e teve compromisso com o debate público e a participação multissetorial. O APL busca regular as atividades de tratamento de dados em âmbito penal e proporcionar segurança jurídica para que os órgãos de investigação e repressão criminal possam exercer suas atividades com eficiência e sem perder de vista as garantias processuais penais e os direitos fundamentais dos titulares de dados (AZEVEDO et al., 2022).

A despeito dos esforços empreendidos pela Comissão de Juristas, o APL atualmente encontra-se paralisado na Câmara dos Deputados à espera de sua apresentação formal com fins de torná-lo um projeto de lei (PL), e seguir os trâmites comuns do processo legislativo com avaliação

das comissões, votações, envio ao Senado e, por fim, submissão à sanção presidencial (COSTA & REIS, 2021). Vale citar que, em junho de 2022, houve também a propositura de outro Projeto de Lei (PL) pela legislatura do então deputado Coronel Armando (PL), com o objetivo de suprir a mesma lacuna legal, mas trazendo propostas absolutamente distintas.

O objetivo deste capítulo é promover uma reflexão sobre o aparente vazio regulatório no contexto da proteção de dados em âmbito da segurança pública, com especial enfoque em dados pessoais sensíveis e população vulnerável no país. Para tanto, parte das seguintes questões: (1) Quais são as lacunas regulatórias deixadas pelas exceções do Art. 4º da LGPD e de que modo têm impactado o poder punitivo estatal, cada vez mais apoiado no uso de novas tecnologias? (2) Quais são os impactos da ausência de regulação e provisão de segurança jurídica nas relações permeadas pelo tratamento de dados pessoais sensíveis para fins de segurança pública?

O texto tem seu desenvolvimento dividido em duas partes. A primeira aborda o panorama regulatório atual acerca das disputas por uma LGPD Penal no Brasil, trazendo os processos de discussão e elaboração do anteprojeto (APL) da LGPD Penal e do PL 1515/22. Em seguida, o texto articula uma perspectiva crítica sobre essa lacuna regulatória e a sua relação com a (des)proteção de dados pessoais sensíveis, em especial envolvendo grupos marginalizados.

Panorama regulatório em direção a uma LGPD Penal no Brasil

O tema de proteção de dados pessoais no âmbito de investigações criminais vem ganhando fôlego no país, com especial enfoque nos debates sobre vigilância excessiva e uso de tecnologias de reconhecimento facial na segurança pública, cujo uso estreou no Brasil oficialmente no ano de 2018 (ver capítulos 1 e 2). Após um ano de experiências em cinco estados e monitoramento dos casos de prisões e abordagens policiais, a Rede

de Observatórios da Segurança publicou levantamento demonstrando que 90,5% dos presos por monitoramento facial no Brasil eram negros (NUNES, 2019), no contexto de uma sociedade em que 56% da população é autodeclarada negra, categoria composta por pretos e pardos.[1]

Em julho de 2019 foi amplamente noticiado em jornais de grande circulação que o sistema utilizado pela polícia do Rio de Janeiro em caráter experimental abordou equivocadamente uma mulher como procurada pela Justiça na orla da Copacabana (WERNECK, 2019). Dias depois, descobriu-se que a criminosa procurada já estava presa havia quatro anos – um indício de que o banco de dados utilizado detinha graves problemas de atualização, e que a abordagem policial se deu de maneira amplamente enviesada. Este foi apenas um de diversos outros casos em que sistema levou policiais da cidade a prender pessoas por engano com o uso da tecnologia de reconhecimento facial (ALMEIDA, 2019). Levando diversos setores da sociedade civil a mobilizar campanhas pelo banimento do reconhecimento facial na segurança pública e nos espaços públicos (ROSÁRIO, 2022; IDEC, 2022) (ver capítulo 5).

A LGPD é o principal diploma legal em vigor a dispor sobre o tratamento de dados pessoais no Brasil, e o uso de tecnologias de reconhecimento facial no âmbito do setor público encontra-se parcialmente excepcionado do escopo de aplicação da LGPD. Isto porque, conforme a determinação de seu art. 4º, inciso III, a Lei não se aplica ao tratamento de dados pessoais realizados para fins exclusivamente de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Desse modo, apesar de garantir que os princípios gerais de proteção ao titular de dados continuem orientando qualquer esfera de tratamento, até mesmo em contextos de interesse público, o Art. 4º, parágrafo

1 Para mais informações, ver: Desigualdades sociais por cor ou raça no Brasil em 2022. IBGE. Disponível em < https://www.ibge.gov.br/estatisticas/sociais/populacao/25844-desigualdades-sociais-por-cor-ou-raca.html?=&t=resultados>. Acesso em 15 fev. 2023.

primeiro determina a necessidade de legislação específica para regulação das hipóteses do inciso III. O objetivo dessa limitação seria a alegada garantia do interesse público de combater infrações penais, crime organizado, fraudes digitais ou até mesmo terrorismo (OLIVEIRA, 2021).

Atualmente existem algumas propostas de legislação específica em matéria de proteção de dados nas investigações criminais em desenvolvimento no Congresso Nacional. Trazemos destaque especial para duas delas: o Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal (APL), e o Projeto de Lei (PL) nº 1515/2022, proposto pelo então deputado federal Coronel Armando do Partido Liberal de Santa Catarina.

O anteprojeto (APL) foi elaborado por uma Comissão de Juristas composta por 15 especialistas, estabelecida na Câmara dos Deputados em 2020.[2] O grupo organizou "um seminário internacional para discussão das principais questões que circundam as garantias constitucionais e o tratamento de dados na investigação criminal e segurança pública" (COSTA & REIS, 2021). Em novembro de 2020, a Comissão apresentou sua proposta de anteprojeto, com inspiração na própria LGPD e regulações da União Europeia e Estados Unidos da América (COSTA & REIS, 2021).

Ao longo de seu texto, o APL apresenta oito eixos principais: a) âmbito de aplicação da Lei; b) condições de aplicação; c) base principiológica; d) direitos e obrigações; e) segurança da informação; f) tecnologias de monitoramento; g) transferência internacional de dados e; h) a autoridade de supervisão (BRASIL, 2020). Em relação a este último, o anteprojeto sugere que a aplicação, supervisão e monitoramento da LGPD penal esteja a cargo do Conselho Nacional de Justiça (CNJ), em razão da sua autonomia e da pluralidade de sua composição. Dentre seus tópicos,

2 CÂMARA DOS DEPUTADOS. GT - Comissão de Juristas - Segurança pública. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica. Acesso em: 03 mar. 2023.

lançamos especial atenção sobre dois deles: as normas relacionadas ao tratamento de dados sensíveis e às tecnologias de monitoramento.

Em relação ao tratamento de dados sensíveis, o APL possui uma seção específica, de apenas um artigo (art. 13 e parágrafo único), que versa especificamente sobre dados pessoais sensíveis. A redação preconiza que o seu tratamento só poderá ser realizado por autoridades competentes, e se estiver previsto em lei, observadas as suas garantias. Além de estabelecer a necessidade de elaboração de relatório de impacto à proteção de dados pessoais e comunicação ao CNJ. A obrigatoriedade do relatório é reforçada por ocasião do art. 29.

O relatório de impacto aparece também na Lei 13.709/18, a Lei Geral de Proteção de Dados (LGPD, definido como o documento que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. O relatório de impacto é considerado um instrumento de governança de dados e que contribui para que "todos os processos que envolvam tratamento de dados, atuais e novos, possam garantir o atendimento e a preservação dos direitos dos titulares de dados" (GOMES, 2019, p. 12). Trata-se de importante aliado para evitar possíveis abusos por parte do poder público no manejo de informações pessoais.

No que tange a tecnologias de monitoramento, o APL despendeu a seguinte definição: "equipamento, programa de computador ou sistema informático que possa ser usado ou implementado para tratamento de dados pessoais captados ou analisados, entre outros, em vídeo, imagem ou áudio". Nesse sentido, destinou um capítulo para o tema e para o tratamento de dados de elevado risco, em que, dentre outras previsões, restringiu a utilização dessas ferramentas apenas para os casos em que houver previsão legal específica, com o estabelecimento de garantias aos titulares e realização de relatório de impacto de vigilância.

Tanto para a avaliação de risco quanto para análise de impacto regulatório no tema e a criação de política de uso com direitos aos ti-

tulares, são apresentadas diretrizes mínimas de conteúdos obrigatórios (art. 42, §§ 1º, 2º e 3º). Em relação aos dois últimos, os seus requisitos também são considerados aplicáveis para a elaboração de relatório de impacto de proteção de dados pessoais, na hipótese em que autorizada por lei a utilização de tecnologias de monitoramento ou tratamento de dados pessoais de alto risco por autoridade competente.

Para o campo da segurança pública, por sua vez, o Art. 43 do APL traz uma proibição específica de uso: a identificação de pessoas indeterminadas. A ver:

> Art. 43. No âmbito de atividades de segurança pública, é vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial (BRASIL, 2020).

A restrição para uso somente no caso em que houver investigação criminal individualizada e autorizada por lei e decisão judicial auxilia para que um número indefinido de pessoas não seja atingido por um monitoramento ostensivo de suas atividades pelo poder estatal. Ainda que seja importante prezar pela eficiência na segurança pública, tal motivação não pode servir para potenciais violações à privacidade, que podem atingir de maneira ainda mais prejudicial determinados setores da sociedade.[3]

O Conselho Nacional de Justiça é listado como o órgão responsável por emitir opiniões técnicas ou recomendações para utilização dessas ferramentas, devendo publicar relatório anual acerca do seu uso em território nacional, bem como promover auditoria no caso de denúncia

3 Cabe destacar que o texto do APL prevê expressamente que as suas disposições não se aplicam ao tratamento de dados pessoais realizado para fins exclusivos de defesa nacional e segurança do Estado, servindo somente para qualquer tipo de tratamento que seja feito por autoridades em atividades de segurança pública e persecução penal (Arts. 3º e 4º).

por descumprimento das normas previstas no anteprojeto. Dessa forma, é possível constatar que a construção do APL demonstra em mais de uma oportunidade o alinhamento da sua proposta a uma legislação mais protetiva e garantista, preocupada com a segurança das informações dos titulares de dados.

Já o Projeto de Lei 1.515/22 foi proposto pelo então deputado federal Coronel Armando (PL/SC) para disputar a narrativa e o controle sobre o uso e tratamento de dados pessoais para fins de segurança pública, defesa nacional, segurança do Estado e investigação e repressão de infrações penais. Embora não tenha tido movimentações no momento, ainda aguardando a criação de comissão especial na Câmara até o fechamento deste capítulo, o PL 1.515 chamou a atenção de especialistas por apresentar a mesma estrutura do APL, mas fragilizar direitos e garantias fundamentais estabelecidos no anteprojeto.

Organizações da sociedade civil atuantes no campo dos direitos digitais manifestaram-se expressamente contra a tramitação da proposta, em razão de ela: 1) promover o desmonte das garantias democraticamente construídas no âmbito do Anteprojeto de LGPD Penal elaborado por comissão de juristas; 2) ampliar demasiadamente o âmbito de aplicação do texto a matérias que possuem fundamentos e principiologia próprias, como a inclusão de disposições para segurança do Estado e defesa nacional; 3) suprimir conceitos importantes e fragilizar a proteção aos dados cadastrais; e 4) promover o desmonte do arcabouço principiológico de controle sobre as autoridades, como por meio da supressão total dos princípios de proporcionalidade, livre acesso e transparência; 5) enfraquecer o repertório de controle sobre decisões automatizadas; e 6) autorizar de forma demasiadamente genérica o compartilhamento de dados entre entidades da administração pública e o acesso a bancos de dados mantidos por atores privados.[4]

4 O manifesto foi assinado pela Coalizão Direitos na Rede, que reúne mais de 50 organizações acadêmicas e do terceiro setor, voltadas à defesa dos direitos digitais.

Em relação às garantias em torno de tecnologias de monitoramento, por exemplo, o PL 1.515 suprimiu totalmente a seção dedicada a esse tema no anteprojeto, de modo a permitir irrestritamente o tratamento de dados pessoais por essas ferramentas, mesmo sendo uma "prática entendida como de alto risco aos direitos fundamentais e liberdades individuais dos titulares de dados" (AZEVEDO et al., 2022, p. 22). Apenas restou a possibilidade de que a autoridade supervisora, ora atribuída à Autoridade Nacional de Proteção de Dados, e não ao CNJ, possa opinar e solicitar relatório de impacto de proteção de dados às autoridades competentes, conforme arts. 6º, §3º e 44, §1º.

Em relação ao tratamento de dados pessoais sensíveis, cabe destacar algumas alterações importantes em que o PL enfraqueceu direitos e garantias previstos no anteprojeto. Dentre elas, constata-se que a proposta apresentou quatro hipóteses de tratamento para fins de segurança pública, através de seu art. 9º. São elas: para cumprimento de atribuição legal de autoridade competente, na garantia de interesse público; execução de políticas públicas; proteção da vida ou incolumidade física do titular ou terceiro contra perigo concreto e iminente; e para o resguardo de direitos de seus titulares.

Além disso, pesquisadores também identificaram a ausência de condicionantes para o tratamento desses dados, sem o endereçamento do risco envolvido nessa atividade, da mesma forma que para fins de investigações criminais, em que o PL autoriza genericamente o seu uso, limitando apenas à observância de leis processuais penais aplicáveis (AZEVEDO et al., 2022). A fragilização de garantias relacionadas ao compartilhamento de dados pessoais sensíveis também pode ser vista através da mitigação do "princípio constitucional da legalidade

A nota pode ser encontrada em "CDR solicita ao presidente da Câmara dos Deputados a interrupção da tramitação do 'PL da LGPD Penal'". Coalizão Direitos na Rede, 1 de agosto de 2022. Disponível em: https://direitosnarede.org.br/2022/08/01/cdr-solicita-ao-presidente-da-camara-dos-deputados-a-interrupcao-da-tramitacao-do-pl-da-lgpd-penal/. Acesso em: 18 fev. 2023.

e reserva legal [...], privilegiando uma genérica e pretensa eficiência na atuação dos órgãos públicos em detrimento dos direitos fundamentais à privacidade e à proteção de dados dos cidadãos" (AZEVEDO et al., 2022, p. 15).

Esses são apenas alguns exemplos que demonstram o quanto o Anteprojeto de LGPD penal e o Projeto de Lei 1.515/2022, apesar de tratarem do mesmo tema e até possuírem estrutura organizacional similar, possuem divergências importantes quanto à forma de enxergar direitos e garantias aos titulares de dados no âmbito de persecução penal e segurança pública.

De um lado, maiores amarras ao uso de tecnologias de monitoramento e ao tratamento de dados pessoais sensíveis buscam assegurar a proteção da privacidade de indivíduos frente ao poder do aparato persecutório do Estado; de outro, uma maior permissividade no uso dessas informações pelo poder público aparenta buscar priorizar maior peso às investigações na seara criminal. O PL 1515/22 tem sido alvo de críticas por parte da sociedade civil que atua em defesa dos direitos digitais, após análises comparativas e apontamentos críticos sobre seus arranjos normativos. Recomendando o seu arquivamento devido à supressão de diversas garantias dos titulares e ampliação excessiva do poder discricionário do Estado.

De outra sorte, entidades representativas de profissionais da segurança pública manifestarem-se contrariamente ao texto do Anteprojeto elaborado pela Comissão de Juristas, alegando, por exemplo, haver vícios de inconstitucionalidade, possíveis prejuízos à celeridade nas investigações e disposições que inviabilizariam trabalhos de pesquisa e apuração por esses agentes (URUPÁ, 2020). Compreender adequadamente esse cenário nos auxilia a vislumbrar o panorama regulatório de intensas disputas que se apresenta nos (ante)projetos de legislação de proteção de dados em âmbito penal no Brasil, que nunca antes se mostrou tão necessária.

Direito penal e proteção de dados: entre a lacuna regulatória e a desproteção

Os ataques antidemocráticos à sede dos três poderes em Brasília, no dia 8 de janeiro de 2023, chamaram a atenção do país não apenas pela violência empregada por movimentos de extrema direita no episódio, como também pelos desdobramentos das investigações criminais para identificar e responsabilizar seus participantes. No dia 3 de fevereiro, o Ministro do Supremo Tribunal Federal (STF), Alexandre de Moraes, autorizou o Tribunal Superior Eleitoral, a Secretaria Nacional de Trânsito e o Instituto Nacional de Tecnologia da Informação a disponibilizarem dados pessoais de cidadãos e cidadãs para fins de auxiliar na investigação da Polícia Federal (HIRABAHASI, 2023). Em razão disso, o órgão policial pôde ter acesso aos dados biométricos, biográficos e fotografias de todos os indivíduos cadastrados.

Considerando a necessidade de tratamento de dados pessoais, o Ministro fez a ressalva de que fossem observadas as medidas previstas no art. 46 da Lei Geral de Proteção de Dados, que versa sobre a necessidade de adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018).

A previsão do Art. 4º, III, da LGPD denota uma lacuna regulatória, mas jamais um vazio regulatório. Apesar de a Lei não tratar diretamente sobre proteção de dados e segurança pública por vedação expressa no seu Art. 4º, ela apresenta uma série de parâmetros e garantias que devem ser observados. Tais como incidência dos princípios gerais e aspectos de responsabilidade, segurança e boas práticas no tratamento de dados pelo poder público, sem prejuízo de aplicabilidade do ordenamento jurídico pátrio e legislações setoriais concernentes ao tema.

A despeito da não afastabilidade destes elementos por força de lei, pairam muitas dúvidas sobre o modo como, de fato, devam incidir tais deveres sobre os atores do campo da segurança pública e da persecução criminal, de modo a levar a cabo o exercício de algum controle social sobre suas atividades.

Os limites e possibilidades do tratamento de dados pessoais em investigações criminais é um assunto tão relevante no cenário nacional, que também é objeto do Tema 1.148, com repercussão geral reconhecida no STF em julgamento ao Recurso Extraordinário 1.301.250/RJ. Nele se discute um pedido do Ministério Público do Rio de Janeiro (MPRJ) no campo das investigações em torno do assassinato da vereadora Marielle Franco e seu motorista Anderson Gomes, ocorrido em 14 de março de 2018. Envolvendo a constitucionalidade de decreto judicial genérico de quebra de sigilo de dados telemáticos para efeito de divulgação de informações pessoais de usuários indeterminados. A Corte admitiu que:

> Possui índole constitucional e repercussão geral a controvérsia relativa aos limites e ao alcance de decisões judiciais de quebra de sigilo de dados pessoais, nas quais determinado o fornecimento de registros de acesso à internet e de IPs (internet protocol address), circunscritos a um lapso temporal demarcado, sem, contudo, a indicação de qualquer elemento concreto apto a identificar os usuários (BRASIL, 2021).

O MPRJ requereu acesso a dois grupos de dados à empresa Google: (1) a geolocalização de todos os usuários que estavam nos arredores do pedágio da Transolímpica, na zona oeste do Rio; e (2) dados de todos os usuários que fizeram buscas no Google pela agenda da vereadora Marielle Franco na semana anterior ao crime (BARRETO, 2021).

O pedido para quebra de sigilo de dados foi feito em agosto de 2018 pela polícia civil e o MPRJ, e aceito pelo Tribunal de Justiça do Estado do Rio de Janeiro (TJRJ). Determinando a entrega da lista de IPs e *de-*

vice IDs de usuários que pesquisaram entre os dias 7 e 14 de março de 2018 as seguintes combinações de palavras: "Marielle Franco", "vereadora Marielle", "agenda vereadora Marielle", "Casa das Pretas" e "Rua dos Inválidos".

Com o número do IP, a polícia conseguiria chegar ao endereço da conexão de internet de quem fez as pesquisas. Já o *device ID*, é a identificação do computador ou do celular. As investigações desejam o cruzamento das informações do IP com o *device ID* para a formação de uma lista, a partir da qual conseguiriam individualizar quais pessoas figuram como suspeitas, e acessar mais dados e provas sobre as pessoas já identificadas, constatando também outras pessoas que participaram do crime e, sobretudo, o seu mandante. A essa tecnologia dá-se o nome de *Geofencing*: em apertada síntese, ela utiliza recursos para determinar um perímetro geográfico virtual.

A negativa da Google ao pedido do MPRJ se dá sob o argumento de incorrer em grave risco à privacidade de inúmeros brasileiros e brasileiras, uma vez que se trataria de uma ordem de quebra de sigilo demasiado genérica – as palavras-chave são termos comuns, potencialmente pesquisados por milhares de pessoas para os mais diversos fins plenamente lícitos –, capaz de afetar uma grande quantidade de usuários que não estariam sob investigação (CARVALHO, 2021). Desse modo, a ordem buscaria transformar um serviço de pesquisa e acesso a informações na internet em vigilância absoluta e indiscriminada, instaurando um autêntico estado policial. Parecendo perigosa a legitimação de uma ordem judicial genérica que, em última instância, fragiliza toda e qualquer atividade que se desempenha na internet.

O TJRJ e o Superior Tribunal de Justiça (STJ) entenderam pertinentes os pedidos do Ministério Público, e determinaram à Google que fornecesse os dados. Mas o processo segue aguardando desdobramentos no STF, reconhecida a existência de repercussão geral sobre o tema. Para a relatora Ministra Rosa Weber é "inegável a existência de questão constitucional no tema em debate, pois a proteção de dados pessoais, um dos

desafios à privacidade na chamada 'Era da Informação', precisa compatibilizar as quebras de sigilo de dados com os requisitos constitucionais mínimos" (STF, 2021).

Tanto os ataques antidemocráticos de 8 de janeiro, quanto as investigações do caso Marielle denotam, com suas particularidades, a complexidade que circunda as discussões sobre ampliação de tecnologias nas investigações criminais e a ausência de uma LGPD penal brasileira. O interesse público envolvido na persecução penal, principalmente em crimes de grande repercussão nacional, e a necessidade de segurança e garantia de privacidade de dados pessoais dos indivíduos denotam as armadilhas de um cenário de difícil resolução e sem respostas fáceis.

Não obstante, o desafio de encontrar o melhor caminho e construir uma regulação sobre dados na esfera penal esbarra, ainda, na realidade de um Estado reconhecidamente inclinado a uma postura punitivista e vigilantista, que possui uma imagem bem definida de quem é o inimigo penal a ser perseguido pelo aparato estatal: majoritariamente pessoas jovens e pretas.[5] A criação de novas leis penais precisa levar em consideração questões de raça, gênero e classe social, a fim de que não se torne mais um instrumento para a criminalização e encarceramento em massa de pessoas negras periféricas. Os dados de mortes em ações policiais promovido pela Rede de Observatórios de Segurança, por exemplo, revela uma expressiva distribuição racial das ocorrências. Em que negros são 97,9% dos mortos na Bahia, 96,3% em Pernambuco, 92,3% no Ceará, 87,3% no Rio de Janeiro, 75% no Piauí e 68,8% em São Paulo (RAMOS et al., 2022).

Se houvesse um campeonato de encarceramento, o Brasil estaria no pódio, junto aos Estados Unidos (1º) e à China (2º). Segundo dados do CNJ, o Brasil chegou em 2022 à marca de 919.651 pessoas privadas

5 Segundo o Anuário Brasileiro de Segurança Pública de 2022, o perfil da população carcerária demonstra uma intensificação do encarceramento em massa de pessoas negras e jovens, com 46,4% entre 18 e 29 anos e 67,5% de cor/raça negra. Ver em: BUENO & LIMA, 2022.

de liberdade (ABBUD, 2022). Mais da metade tem entre 18 e 29 anos, e a maioria é de pessoas negras. A população negra também é maioria entre os que vivem em favelas e periferias, que têm acesso precário à saúde e educação, os que têm maiores taxas de desemprego, e cuja expectativa de vida é a mais baixa (WERNECK, 2018).

Ao mesmo tempo em que a LGPD penal poderá auxiliar a traçar um caminho para atuações de prevenção e combate ao crime, também deverá se ocupar da limitação do poder punitivo estatal. Evitando, assim, o fomento a um estado autoritário e/ou de vigilância (AZEVEDO et al., 2022). Pois com a utilização de novas tecnologias, o controle por parte do Estado encontra grande potencial de intensificação, de modo a colocar ainda mais em risco direitos e liberdades individuais, em especial de grupos minoritários.

O reconhecimento facial, por exemplo, tem sido uma ferramenta capaz de reproduzir e potencializar opressões já presentes na sociedade, sobretudo quando utilizado pelas forças de segurança e em políticas públicas (ver capítulos 1 e 2). Os vieses de raça, gênero, sexualidade e classe presentes nos algoritmos podem trazer implicações bastante problemáticas e de cunho altamente discriminatório. Elementos técnicos, somados a fatores econômicos, históricos e culturais, afetam sobremaneira minorias étnicas e raciais e pessoas trans (BUOLAMWINI & GEBRU, 2018; SILVA & VARON, 2021). As taxas de acerto na identificação/autenticação por reconhecimento facial estão condicionadas por diferentes fatores, e envolvem iluminação, perspectiva, sombras, expressões faciais, e até mesmo a resolução das imagens e vídeos. Além disso, o treinamento do sistema, aliado à qualidade e ao tamanho dos *Datasets* (conjuntos de dados) utilizados para aferir o padrão facial dos transeuntes também influencia de maneira significativa os resultados aferidos (KREMER, 2022) (Ver Introdução).

Tais tecnologias vêm sendo aplicadas no policiamento de várias cidades ao redor do mundo. A prática foi inaugurada no Brasil em dezembro de 2018 pela secretaria de segurança pública da Bahia, nas ci-

dades de Feira de Santana e Salvador.[6] Desde que implantado, mais de 700 prisões por reconhecimento facial já foram realizadas na região (RECONHECIMENTO..., 2023).[7]

Dentre as mais de 4,3 milhões de imagens registradas, houve também casos de falsos positivos (CELESTINO, 2020). Por exemplo, um adolescente de 17 anos foi abordado dentro de uma estação de metrô para cumprimento de mandado de prisão em aberto por tráfico de drogas. Ao ser conduzido à delegacia, foi constatado que sua apreensão se deu por engano, de modo que a identidade do rapaz não era compatível com a do sujeito apontado pelo sistema de reconhecimento (SILVA, 2019). Em outra situação, um jovem de 25 anos, portador de necessidades especiais e acompanhado de sua mãe, foi abordado dentro de uma padaria quando a caminho de uma consulta médica por ser apontado pelo sistema de reconhecimento facial como alguém com mandado de prisão em aberto (PALMA & PACHECO, 2020).

Em novembro de 2022, a Prefeitura de São Paulo lançou edital de contratação para a iniciativa *Smart Sampa*: uma nova plataforma de videomonitoramento que busca ampliar, modernizar e integrar mais de 20 mil câmeras na capital paulista até 2024 em auxílio a ocorrências da Guarda Civil Metropolitana e demais órgãos de segurança. Com um investimento de R$70 milhões por ano,[8] o novo sistema al-

6 O funcionamento se dá por um sistema de comparação: caso as imagens captadas em tempo real sejam mais de 90% compatíveis com aquelas disponíveis no banco de procurados, são gerados alertas a profissionais que acionam equipes nas ruas para confirmação da identidade dos suspeitos e dão seguimento ao cumprimento do mandado de prisão. Ver: SANTANA, 2019.

7 Homem é preso após reconhecimento facial; Bahia se aproxima de 200 prisões. A Tarde. Salvador. 28 de março de 2020. Disponível em: <https://atarde.uol.com.br/bahia/noticias/2124249-homem-e-preso-apos-reconhecimento-facial-bahia-se-aproxima-de-200-prisoes>. Acesso em 12 de maio de 2020.

8 ARREGUY, Juliana. Prefeitura tentará pela terceira vez comprar câmera de reconhecimento facial. Metrópoles. São Paulo, 13 de junho de 2023. Disponível em: <https://www.metropoles.com/sao-paulo/prefeitura-de-sp-tentara-pela-3-vez-comprar-cameras-de-reconhecimento-facial>. Acesso em: 27 jul. 2023.

meja um monitoramento mais especializado, agregando o conceito de cidades inteligentes, recursos de identificação facial e detecção de movimento que permitem o reconhecimento de placas de veículos, objetos perdidos, pessoas procuradas e, até mesmo, atitudes suspeitas (NOVA..., 2022).

O projeto propõe tecnologia de reconhecimento facial em todas as estações de trem e metrô da capital em tempo real. Em um dos trechos do edital, a tecnologia promete "rastrear uma pessoa suspeita, monitorando todos os seus movimentos e atividades, por características como cor, face, roupas, forma do corpo, aspectos físicos, etc.". Alvo de críticas por setores da sociedade civil e movimentos sociais, o projeto esteve sob a análise no Tribunal de Contas do Município de São Paulo para averiguação de irregularidades, e teve seu edital suspenso por ordem judicial três vezes, tendo sido a última em 26 de julho de 2023, sob o entendimento de ausência de transparência sobre o processamento de dados pessoais dos usuários.

O *Smart Sampa* não é um caso isolado. Como vimos, câmeras de reconhecimento facial têm sido utilizadas no estado da Bahia desde 2018 com a finalidade de combate à criminalidade, sendo considerado por pesquisadores e ativistas um verdadeiro laboratório de vigilância com uso dessa tecnologia (FALCÃO, 2021). No Distrito Federal, por sua vez, o Sistema Córtex do governo federal é apontado como uma das maiores ferramentas de vigilância e controle de que se tem notícia no Brasil. Uma plataforma com tecnologia de inteligência artificial capaz de, em questão de segundos, cruzar informações captadas por câmeras viárias espalhadas por rodovias, pontes, túneis, ruas e avenidas país afora com diversas bases de dados de informações sensíveis, ou até mesmo sigilosas (REBELLO, 2020).

Esses e outros casos refletem uma das principais fragilidades do ordenamento jurídico brasileiro no contexto da proteção de dados pessoais: a adoção progressiva de tecnologias movidas a dados pelos órgãos de segurança pública sem a existência de uma regulação expressa sobre

o tema. Sobretudo envolvendo dados pessoais sensíveis, como as biometrias faciais.

Somado a isso, o período compreendido entre 2020 e 2022 foi marcado por algumas decisões muito relevantes no Supremo Tribunal Federal no que diz respeito ao direito à proteção da privacidade e dos dados pessoais. Influenciando sobremaneira a temática de interseção entre tratamento de dados pessoais sensíveis e segurança pública.

Em 2020 o Supremo Tribunal Federal (STF) deu um importante passo ao reconhecer um direito fundamental autônomo à proteção de dados pessoais, no julgamento das Ações Diretas de Inconstitucionalidade (ADIS) n. 6387, 6388, 6389, 6393 e 6390. Com a promulgação da Emenda Constitucional (EC) 115, em fevereiro de 2022, a proteção de dados pessoais tornou-se expressa na Constituição Federal, e foi elevada à categoria de direito fundamental, acrescendo-se ao Art. 5º o inciso LXXIX. E isso produz efeitos muito relevantes para fins de proteção de direitos no campo da segurança pública, a despeito da existente lacuna legal explícita sobre o tema. Com especial enfoque na hierarquia constitucional do instituto da proteção de dados pessoais, e efeitos de aplicabilidade direta e imediata da norma, nos termos do Art. 5º, §1º da CRFB.

Pouco tempo depois, em setembro de 2022, o STF teve a oportunidade de julgar a ADI 6649, proposta pela OAB Federal, que questionava a constitucionalidade da estrutura de compartilhamento de dados da Administração Pública Federal, amparada pelo Decreto 10.046/19, que cria o Cadastro-Base do Cidadão. Uma base integrada que contém dados gerais sobre todos os brasileiros, acessível a todos os órgãos do Executivo Federal mediante adesão. O decreto estabelece como finalidades do compartilhamento de dados a simplificação de serviços públicos, a redução de custos com o reaproveitamento de sistemas de informática, e também a análise do direito a benefícios sociais. Um importante teste para este novo direito fundamental, e também uma oportunidade para a consolidação das balizas constitucionais do tratamento de dados pessoais no Poder Público (MENDES, 2022).

No julgamento, o STF acabou por não apenas validar a constitucionalidade do Decreto atacado pela OAB, no sentido da possibilidade do compartilhamento de informações, como também condicionou a permissão de acesso aos dados a parâmetros demasiado abertos, tais como: propósitos legítimos, específicos e explícitos, e atendimento do interesse público. Trata-se de um cadastro complexo e demasiado robusto, que comporá seu banco também com dados biométricos (portanto sensíveis) da população brasileira, sem garantias adicionais a esse tratamento e sem a presença de qualquer tipo de instrumento de prestação de contas apto a indicar as finalidades no âmbito da administração pública, entre outros diversos flagrantes vícios de constitucionalidade.

A decisão do STF se mostra conflitante com a construção jurisprudencial que se vinha tecendo, que correlacionava proteção de dados pessoais e exercício pleno da democracia, indo na contramão de alguns dos mais relevantes e emblemáticos posicionamentos jurisprudenciais do cenário internacional em matéria de proteção de dados e exercício da cidadania. A exemplo do julgamento do caso paradigmático sobre o Censo Demográfico na Alemanha em 1983, em que a Corte Constitucional afirmou a importância de cidadãos precisarem ser capazes de saber quem sabe o que sobre eles, quando e em que situação, para que não lhes sobrevenham prejuízos no desenvolvimento de sua personalidade, para sua autodeterminação informativa e para o bem comum de uma sociedade democrática.[9]

Conclusão

O campo jurídico-penal é alvo de disputas constantes, no sentido das reiteradas denúncias de seletividade penal feitas em face dos órgãos do sistema de justiça e do sistema criminal, quanto à construção do *status*

9 BVerfGE [Decisões do Tribunal Constitucional Federal] 65, I – decisão sobre o censo populacional.

de criminoso na sociedade e da funcionalidade do sistema jurídico-penal para a manutenção das desigualdades e reprodução de hierarquias de poder. A proteção de dados, assim como o direito penal, não tem seus debates jurídicos eivados de intencionalidade ou tensionamentos políticos, apesar de a cultura de proteção de dados no Brasil ainda ser jovem e estar em processo de amadurecimento e estruturação.

A incorporação de ferramentas tecnológicas pelas forças de segurança torna esse cenário ainda mais complexo. O objetivo de atribuir maior eficiência à atuação policial traz consigo uma problemática, que reside na adoção às cegas dessas mesmas ferramentas. Têm sido adotadas tecnologias que não são neutras em seus usos e em seu desenvolvimento, razão pela qual é importante uma reflexão sobre a importância da regulação dessas tecnologias, e sobre os riscos de reprodução de padrões historicamente estabelecidos e consolidados no seio social, reforçados pelo uso de novos aparatos tecnológicos (ARRUDA et al., 2022).

Entendemos que as lacunas regulatórias deixadas pela Lei Geral de Proteção de Dados em relação ao tratamento de dados para fins de investigação criminal e persecução penal, a partir das exceções do Art. 4º, inciso III, têm impactado o poder punitivo estatal a partir do apoio cada vez maior no uso de tecnologias movidas a dados. E a compatibilização entre riscos e benefícios do uso de tecnologias tem sido o ponto central dos debates envolvendo *big data* e segurança pública.

A ausência de uma LGPD Penal impacta a provisão de segurança jurídica nas relações permeadas pelo tratamento de dados pessoais sensíveis para fins de segurança pública, mas não afasta em absoluto a incidência dos princípios gerais da lei, nem mesmo os contornos de boas práticas e a arquitetura de responsabilização e o dever de prestação de contas. O Direito é uma importante ferramenta de embate das injustiças, e instrumento de coibição de abusos e riscos que o uso de novas tecnologias pelos órgãos de segurança pública e pelo Estado possam infringir aos indivíduos e à sociedade.

O panorama regulatório que se desenha atualmente no campo político em matéria de LGPD Penal nos mostra que a atual lacuna regulatória possui relação direta com a adoção cada vez mais intensa de aparatos tecnológicos por parte do poder público, das forças de segurança e do sistema de justiça. Em ameaça frontal à garantia de direitos fundamentais para os grupos marginalizados deste país, composto majoritariamente por pessoas negras e pobres.

A proteção de dados pessoais tem se tornado discussão fundamental nos últimos anos na medida que avança a constante coleta de dados pessoais, gerada pelo uso massivo de serviços e bens conectados à internet, associada ao contínuo monitoramento que é feito dos hábitos e comportamentos das pessoas dentro e fora da rede (MULHOLLAND & FRAJHOF, 2020). Diante desses e outros riscos, a estruturação de uma LGPD Penal no Brasil se apresenta como uma importante e necessária iniciativa, capaz de equilibrar a busca pelo interesse público na investigação criminal e o respeito aos direitos fundamentais.

Assim, espera-se de uma LGPD Penal a garantia para ações de prevenção e combate ao crime, porém com o compromisso com a limitação do poder punitivo estatal, de modo a coibir a estruturação um estado autoritário e de vigilância excessiva, cada vez mais conectado e movido a dados. E em consolidação ao devido processo legal, aos princípios de proteção de dados e aos direitos dos titulares.

Referências bibliográficas

ABBUD, Bruno. Pandemia pode ter levado Brasil a ter recorde histórico de 919.651 presos. **O Globo**. Brasilia, 05 jun 2022.Disponível em: https://oglobo.globo.com/brasil/noticia/2022/06/pandemia-pode-ter-levado-brasil-a-ter-recorde-historico-de-919651-presos.ghtml Acesso em: 13 abr 2023.

ALMEIDA, Emily. Homem é preso por engano em Copacabana. Band. 24 jul 2019. Disponível e: https://bandnewsfmrio.com.br/editorias-detalhes/homem-e-preso-por-engano-em-copacabana Acesso em: 15 fev 2023.

ARRUDA, A. J. P.; RESENDE, A. P. B. A.; FERNANDES, F. A. SISTEMAS DE POLICIAMENTO PREDITIVO E AFETAÇÃO DE DIREITOS HUMANOS À LUZ DA CRIMINOLOGIA CRÍTICA. **Direito Público**, *[S. l.]*, v. 18, n. 100, 2022. DOI: 10.11117/rdp.v18i100.5978. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5978. Acesso em: 25 jan. 2023.

AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. Disponível em: bit.ly/3U0OuU0 Acesso em: 01 abr 2023.

BARRETO, Elis. STF decide que recurso do Google no caso Marielle será tema de repercussão geral. **CNN Brasil,** 28 de maio de 2021. Disponível em: https://www.cnnbrasil.com.br/nacional/stf-decide-que-recurso-do-google-no-caso-marielle-sera-tema-de-repercussao-geral/. Acesso em: 17 fev. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 mar. 2023.

BRASIL. Câmara dos Deputados. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal.** Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em: 03 mar. 2023.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário 1301250.** Direito constitucional. Direito processual penal. Quebra de sigilo de dados pessoais. Registros de acesso à internet e fornecimento de ip. Decisão genérica. Não indicação de parâmetros mínimos para identificação dos usuários. Não delimitação, ademais, do espaço territorial em que veiculada a ordem. Proteção à intimidade e ao sigilo de dados (art. 5º, x e xii, cf). Questão constitucional. Potencial multiplicador da controvérsia. Repercussão geral reconhecida. 1. Possui índole constitucional e repercussão geral a controvérsia relativa aos limites e ao alcance de decisões judiciais de quebra de sigilo de dados pessoais, nas quais determinado o fornecimento de registros de acesso à internet e de IPs (internet protocol address), circunscritos a um lapso temporal demarcado, sem, contudo, a indicação de qualquer elemento concreto apto a identificar os usuários. 2. Repercussão geral reconhecida. Recorrente: G. B. I. L.; G. I. Recorrido: Estado do Rio de Janeiro. Relatora: Ministra Rosa Weber, 27 de maio

de 2021. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=-TP&docID=756074304. Acesso em: 26 jul. 2023.

BUENO, Samira; LIMA, Renato Sérgio de (coord). **Anuário Brasileiro de Segurança Pública 2022:** as 820 mil vidas sob a tutela do Estado. Fórum Brasileiro de Segurança Pública, 2022.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: intersectional accuracy disparities in commercial gender classification. **Proceedings of the 1st Conference on Fairness, Accountability and Transparency,** PMLR 81:77-91, 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a.html. Acesso em: 13 abr 2023.

CÂMARA DOS DEPUTADOS. GT - Comissão de Juristas - Segurança pública. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica. Acesso em: 03 mar. 2023.

CARVALHO, Igor. Por que o Google pode ajudar resolver o caso Marielle, mas se recusa. **Brasil de Fato,** Direitos Humanos, 17 de março de 2021. Disponível em: https://www.brasildefato.com.br/2021/03/17/por-que-o-google-pode-ajudar-resolver-o-caso-marielle-mas-se-recusa#:~:text=Desde%200%20dia%2027%20de,de%20seu%20motorista%2C%20Anderson%20Gomes. Acesso em: 18 fev. 2023.

CELESTINO, Samuel. Sistema de reconhecimento facial já registrou mais de 4,3 milhões de imagens. Bahia Notícias. Salvador. 24 de fevereiro de 2020. Disponível em: https://www.bahianoticias.com.br/noticia/244617-sistema-de-reconhecimento-facial-ja-registrou-mais-de-43-milhoes-de-imagens.html Acesso em 14 de maio de 2020.

COSTA, Eduarda; REIS, Carolina. Histórico da LGPD Penal: o que foi feito até aqui e quais são os próximos passos? Privacidade e Proteção de Dados Pessoais. **Blog**. Lapin. 16 abr 2021. Disponível em: https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/. Acesso em: 05 abr. 2023.

DESIGUALDADES sociais por cor ou raça no Brasil em 2022. IBGE. Disponível em https://www.ibge.gov.br/estatisticas/sociais/populacao/25844-desigualdades-sociais-por-cor-ou-raca.html?=&t=resultados. Acesso em 15 fev. 2023.

FALCÃO, Cintia. Lentes racistas: Rui Costa está transformando a Bahia em um laboratório de vigilância com reconhecimento facial. **The Intercept Brasil**. 20 set. 2021. Disponível em: https://www.intercept.com.br/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/. Acesso em: 30 mar 2023.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados: uma breve análise da sua definição e papel na LGPD. **Revista do Advogado,** 2019, p. 12. Disponível

em: https://www.academia.edu/download/61401936/Maria_Cecilia_Oliveira_Gomes_120191202-105461-1advdye.pdf. Acesso em: 03 mar. 2023.

HIRABAHASI, Gabriel. Moraes autoriza que TSE dê acesso da biometria à PF na apuração do 8 de janeiro. **CNN Brasil,** Política, 10 de fevereiro de 2023. Disponível em: https://www.cnnbrasil.com.br/politica/moraes-autoriza-que-tse-de-acesso-da-biometria-a-pf-na-apuracao-do-8-de-janeiro/. Acesso em: 18 fev. 2023.

KREMER, Bianca. Reconhecimento facial no Brasil: uma perspectiva de raça e gênero. **Coding Rights.** Medium. Rio de Janeiro, 7 fev. 2022. Disponível em: https://medium.com/codingrights/reconhecimento-facial-no-brasil-uma-perspectiva-de-ra%C3%A7a-e-g%C3%AAnero-9fe027c3a176. Acesso em: 13 fev 2023.

MENDES, Laura Schertel. Democracia, poder informacional e vigilância. Fumus Boni Iuris. **O Globo.** 13 ago. 2022. Disponível em: https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml Acesso em: 20 out. 2022.

MULHOLLAND, Caitlin; FRAJHOF, Isabela. Prefácio. **A LGPD e o novo marco normativo no Brasil.** Porto Alegre: Arquipélago, 2020.

NOVA Plataforma de videomonitoramento Smart Sampa. **Participe Mais.** Prefeitura de São Paulo, nov. 2022. Disponível em: https://participemais.prefeitura.sp.gov.br/legislation/processes/209 Acesso em: 29 mar 2023.

NUNES, Pablo. Exclusivo: levantamento revela que 90,5% dos presos por reconhecimento facial no Brasil são negros. **The Intercept.** 21 nov 2019. Disponível em: https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/ Acesso em: 27 jan 2021.

OLIVEIRA, Samuel R. **Sorria, você está sendo filmado**. Repensando Direitos na Era do Reconhecimento Facial. São Paulo: Thomson Reuteurs, 2021.

PALMA, Amanda; PACHECO, Larissa. 'O policial já foi com a arma na cabeça dele', diz mãe de rapaz confundido por reconhecimento facial. **Correio 24 horas**. 05 de janeiro de 2020. Salvador. Disponível em: https://www.correio24horas.com.br/noticia/nid/o--policial-ja-foi-com-a-arma-na-cabeca-dele-diz-mae-de-rapaz-confundido-por-reconhecimento-facial/. Acesso em 12 de maio de 2020.

PARLAMENTARES de todas as regiões do Brasil apresentam projetos de lei pelo banimento do reconhecimento facial em espaços públicos. Instituto de Defesa do Consumidor. 20 jun. 2022. Disponível em: https://idec.org.br/release/parlamentares-de-todas-regioes-do-brasil-apresentam-projetos-de-lei-pelo-banimento-do. Acesso em: 03 jul. 2023.

RAMOS, Silvia et al. Pele alvo: a cor que a polícia apaga / Silvia Ramos...[et al.] (Org.). Rio de Janeiro: CESeC, 2022. Disponível em: http://observatorioseguranca.com.br/wordpress/wp-content/uploads/2022/11/EM-EMBARGO-ATE-1711_5-AM-REDE-DE-OBS_PELE-ALVO2_171122.pdf. Acesso em: 13 abr 2023.

REBELLO, Aiuri. Da placa de carro ao CPF: conheça o córtex, sistema de vigilância do governo que integra de placa de carro a dados de emprego. **The Intercept Brasil**. 21 set. 2020. Disponível em: https://www.intercept.com.br/2020/09/21/governo-vigilancia-cortex/. Acesso em: 31 mar 2023.

RECONHECIMENTO facial ultrapassa a marca de 700 presos na Bahia. **Portal Salvador FM,** 24 fev. 2023. Disponível em: https://www.portalsalvadorfm.com.br/noticias/112369,reconhecimento-facial-ultrapassa-a-marca-de-700-presos-na-bahia. Acesso em: 26 jul. 2023.

ROSÁRIO, Fernanda. Tire meu rosto da sua mira: reconhecimento facial pode ser mais uma ferramenta de violação de direitos. **Terra.** 29 nov. 2022. Disponível em: https://www.terra.com.br/nos/tire-meu-rosto-da-sua-mira-reconhecimento-facial-pode-ser-mais-uma-ferramenta-de-violacao-de-direitos,88bce2aef1616bd6affbc7a691de47dap7p8wb66.html. Acesso em 03 jul. 2023.

SANTANA, Marcia. Reconhecimento facial completa um ano e é destaque nacional. **SSP Secretaria de Segurança Pública.** Bahia. 18 de dezembro de 2019. Disponível em: http://www.ssp.ba.gov.br/2019/12/6981/Reconhecimento-Facial- completa-um-ano-e-e-destaque-nacional.html. Acesso em 12 de maio de 2020.

SILVA, Mariah Rafaela; VARON, Joana. **Reconhecimento facial no setor público e identidades trans**. Coding Rights: Rio de Janeiro, 2021. Disponível em: https://codingrights.org/docs/rec-facial-id-trans.pdf. Acesso em: 13 abr 2023.

SILVA, Tarcizio. Reconhecimento facial na Bahia: mais erros policiais contra negros e pobres. **Blog do Tarcizio.** São Paulo. 21 de novembro de 2019. Disponível em: https://tarciziosilva.com.br/blog/reconhecimento-facial-na-bahia-mais-erros-policiais-contra-negros-e-pobres/. Acesso em: 26 jul. 2023.

SUPREMO vai definir limites para a decretação de quebra de sigilo de históricos de busca na internet. **Supremo Tribunal Federal,** 31 de maio de 2021. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=466801&tip=UN. Acesso em: 17 fev. 2023.

URUPÁ, Marcos. Policiais dizem que proposta da LGPD Penal poderia atrapalhar investigações. **Teletime,** 15 dez. 2020. Disponível em: https://teletime.com.br/15/12/2020/policiais-dizem-que-proposta-da-lgpd-penal-poderia-atrapalhar-investigacoes/. Acesso em: 26 jul. 2023.

WERNECK, Antonio. Reconhecimento facial falha em segundo dia, e mulher inocente é confundida com criminosa já presa. **O Globo**. 11 jul 2019. Disponível em: https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913. Acesso em: 28 jan 2021.

WERNECK, Jurema. Cartas pra quem? Prefácio. In: **Vozes do cárcere**: ecos da resistência política. **PIRES**, Thula; **FREITAS**, Felipe (Org.) Rio de Janeiro: Kitabu, 2018.

Reconhecimento facial e segurança pública nas cidades: uma análise crítica na perspectiva das competências federativas e dos direitos fundamentais

Eleonora Mesquita Ceia
Chiara Spadaccini de Teffé

Resumo

O uso de ferramentas de reconhecimento facial para fins de segurança pública é cercado de controvérsias: falhas técnicas e falsos positivos em suas análises mostraram-se capazes de reforçar discriminações em face de pessoas negras e determinados grupos, o que consequentemente pode vir a aumentar abordagens policiais e encarceramentos indevidos. A ampliação de seu uso trouxe também uma série de questionamentos sobre a proteção dos direitos e liberdades fundamentais, diante da possibilidade de tal tecnologia ser utilizada de forma abusiva para fins de vigilância e controles político e social. Além disso, até o momento, as ferramentas de reconhecimento facial não foram reguladas por lei específica e de caráter federal, que aborde tanto a sua aplicação quanto o tratamento de dados pessoais realizado. Regulação essa que se mostra necessária e importante para a proteção de direitos. Na prática, porém, alguns gestores locais não aguardaram a devida regulamentação, havendo certas disposições setoriais sobre tal tecnologia nos âmbitos estadual

e municipal. Diante disso, o artigo tem por objetivo analisar criticamente as principais controvérsias quanto ao reconhecimento facial para fins de segurança pública, a saber, os potenciais conflitos de competência sobre a matéria entre os entes federativos e os riscos de restrição a direitos e liberdades fundamentais.

Tecnologias de reconhecimento facial em cidades inteligentes: contextualização e apresentação dos riscos

A partir da metade do século XX, o Brasil vivenciou um processo de urbanização acelerado e pouco organizado, o qual culminou no surgimento de megacidades, como São Paulo e Rio de Janeiro, as quais concentram cerca de 12 e 7 milhões de habitantes, respectivamente (SEADE, 2022; DATA RIO, 2022). A maioria das cidades enfrenta pressões e demandas relacionadas com moradia, saúde pública, transporte, desemprego, proteção ambiental, alimentação e violência. Buscando soluções, as cidades se engajam em projetos de inovação e cooperação mútua, com base nas noções de "cidades sustentáveis", "cidades solidárias" e "cidades inteligentes" (HIRSCHL, 2020; EDWARDS, 2015).

Nas cidades inteligentes, há sistemas e pessoas interagindo e usando tecnologias, materiais, energias, serviços e financiamentos para catalisar o desenvolvimento econômico e a melhoria da qualidade de vida. Esses fluxos de interação são considerados inteligentes por fazerem uso estratégico de infraestrutura, serviços e informação, com planejamento e gestão urbana, para dar respostas às necessidades sociais e econômicas da sociedade. Busca-se, hoje, cidades criativas e sustentáveis, que façam uso da tecnologia em seu processo de planejamento e gestão, com a participação dos cidadãos. Nelas ocorre a implementação de tecnologias para conduzir e monitorar a vida urbana, com o objetivo de solucionar seus maiores desafios, como a violência urbana, apontada como um dos principais problemas das cidades brasileiras, depois da saúde e da educação (G1, 2020; PÚBLICA, 2020).

Portanto, novas tecnologias estão sendo cada vez mais utilizadas em atividades voltadas à investigação, repressão de infrações penais e segurança pelas autoridades locais. Uma dessas tecnologias é o reconhecimento facial, cujo uso para fins de segurança pública apresenta complexidades e polêmicas: falhas técnicas e falsos positivos em suas análises mostraram-se capazes de reforçar discriminações em face de pessoas negras e determinados grupos, o que consequentemente pode vir a aumentar abordagens policiais e encarceramentos indevidos. A ampliação de seu uso trouxe também uma série de questionamentos sobre a proteção dos direitos fundamentais, diante da possibilidade de tal ferramenta ser utilizada de forma abusiva para fins de vigilância e controles político e social (EDPB, 2022).

Nesse contexto, diferentes instituições ao redor do mundo, incluindo algumas organizações brasileiras, apresentaram em junho de 2021 uma "Carta aberta para banimento global de usos de reconhecimento facial e outros reconhecimentos biométricos remotos que permitam vigilância em massa, discriminatória e enviesada" (ACCESSNOW, 2021). Em junho de 2022, foi lançada a campanha *#SaiDaMinhaCara*, em que 50 parlamentares de diferentes partidos apresentaram projetos de lei visando a banir o uso do reconhecimento facial em espaços públicos. A ação envolveu deputados estaduais e vereadores, além de organizações (MEDIUM, 2022).

Até o momento, no Brasil, o uso dessas tecnologias para fins de segurança pública ainda não foi regulamentado por lei federal específica, a qual deverá tratar acerca de sua aplicação, dos protocolos operacionais, do respectivo tratamento de dados pessoais e de medidas protetivas aos direitos fundamentais relacionados, como responsabilizações específicas em casos de erros ocorridos durante essa implementação. Entende-se que a temática do racismo estrutural se encontra conectada com essa questão em vários eixos, seja pelo desenho e treinamento dos algoritmos, seja na própria escolha dos locais para operações e a instalação de câmeras.

De acordo com a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), o tratamento de dados pessoais feito exclusivamente para segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais deverá ser regulado por legislação específica. Na prática, porém, as autoridades locais não esperaram pela devida regulamentação. Diversas cidades brasileiras já vêm fazendo uso de tecnologias de reconhecimento facial, inclusive para o combate à violência urbana (INSTITUTO IGARAPÉ, 2020). Iniciativas de leis estaduais e municipais, assim como projetos de lei sobre o mesmo assunto, vêm surgindo.

Nesta lógica, este capítulo tem como objetivo analisar as principais controvérsias sobre tecnologias de reconhecimento facial para fins de segurança pública, a saber, os riscos de violação a direitos fundamentais e os potenciais conflitos de competência entre entes federativos na sua regulação. Com ênfase na autonomia das cidades, prevista na Constituição de 1988, haverá reflexão acerca da competência dos municípios para legislarem sobre a aplicação de reconhecimento facial na seara da segurança pública.

Proteção de dados pessoais, reconhecimento facial e segurança pública: como garantir direitos e assegurar deveres?

A tecnologia expande o alcance das capacidades humanas, registrando com precisão localizações geográficas, dados sensíveis e pessoas com quem interagimos. Dessa forma, mostra-se necessário definir quando, onde, como e para que finalidades poderão ser tratados dados pessoais. Igualmente, estabelecer boas práticas e garantias para a pessoa em todas as atividades relacionadas com dados, tendo em vista os valores estratégico, financeiro e comercial que detêm. Os cruzamentos e inferências obtidos a partir do tratamento de informações pessoais têm impulsionado significativamente setores ligados à economia, ao merca-

do e à segurança, havendo, por consequência, o aumento de estruturas de vigilância e extração de dados.

A utilização de *big data* e inteligência artificial nas atividades do Estado vai ao encontro de um discurso de ampliação da eficiência e digitalização da Administração Pública. Entende-se que grandes bases de dados acessíveis a um maior número de instituições permitem o aumento da precisão dos diagnósticos, do planejamento e da sinergia das atividades. Contudo, a ampliação da capacidade do Estado de lidar com as informações aumenta também seu poder perante os cidadãos e afirma as assimetrias entre as partes.

No campo da segurança pública, as ferramentas de reconhecimento facial tornam mais invasivos os mecanismos de identificação, rastreamento e vigilância utilizados tanto preventivamente quanto para a persecução penal. Algumas soluções permitem a identificação de objetos e de pessoas em imagens, assim como aplicativos de análise de áudio demonstram a capacidade de detectar, por exemplo, sons de tiros, batidas de carros ou aglomerações, com envio de alertas automáticos às autoridades responsáveis. A rastreabilidade das pessoas tem se tornado cada vez mais sofisticada, incluindo o compartilhamento de dados entre agentes para fins de controle e segurança, como em aeroportos, locais de grandes eventos e áreas identificadas como de maior atenção.

Essa dinâmica é analisada por Shoshana Zuboff (2015; 2019), que desenvolveu o conceito de *capitalismo de vigilância*: uma estrutura que considera a experiência humana como matéria-prima, gratuita e disponível para práticas comerciais ocultas de extração, previsão e venda de dados. Ao oferecer serviços aparentemente gratuitos para bilhões de pessoas, os provedores responsáveis por tais serviços monitoram o comportamento dos usuários, obtendo detalhes surpreendentes, inferindo informações e, até mesmo, moldando comportamentos e desejos, dentro de lógicas comerciais e econômicas. Já não basta automatizar o fluxo de informações sobre nós; o objetivo passou a ser nos automatizar. Esta seria outra fase na evolução do capitalismo: visaria a

explorar as previsões comportamentais derivadas da vigilância imposta aos usuários.

Dessa forma, produtos ou serviços "inteligentes", personalizados ou conectados representariam parte da cadeia de fornecimento de dados comportamentais que seriam usados para prever nosso futuro em uma economia de vigilância. Embora alguns desses dados sejam aplicados à melhoria de serviços, muitos deles alimentam processos preditivos que antecipam o que você fará agora, em breve e depois. Esses produtos de previsão estariam sendo negociados em um novo tipo de mercado que Zuboff chamou de *mercados futuros comportamentais*.

Criou-se, então, o que foi chamado por Frank Pasquale (2015) de espelho unidirecional (*one way mirror)*, em que os dados pessoais dos cidadãos têm sido utilizados por governos e agentes econômicos para que eles saibam tudo sobre as pessoas, enquanto elas nada ou pouco sabem sobre os dois primeiros. Suas previsões são *sobre* nós, mas não *para* nós. Tudo isso aconteceria por meio de monitoramento e de vigília constantes acerca de cada passo da vida dos indivíduos, o que levaria a um verdadeiro *capitalismo de vigilância*, cuja principal consequência seria a consolidação de uma sociedade também de vigilância.

Nesse contexto, trazendo princípios essenciais para a proteção de dados pessoais e direitos aos titulares, a LGPD entrou em vigor em setembro de 2020 no Brasil. Ato contínuo, em fevereiro de 2022, foi promulgada a Emenda Constitucional nº 115, que alterou a Constituição Federal de 1988 para incluir a proteção de dados pessoais entre os direitos fundamentais. Portanto, essa proteção tornou-se explicitamente cláusula pétrea, sendo garantida a indivíduos e grupos.

A proteção da privacidade e dos dados pessoais representa uma significativa forma de conter os efeitos nocivos do capitalismo de vigilância e das manipulações oriundas das grandes plataformas e estruturas políticas. Considerando a importância da informação para as relações de poder e as assimetrias muitas vezes existentes entre controladores e titulares de dados, a LGPD e as demais normas voltadas à proteção e ao

tratamento de dados buscam garantir instrumentos jurídicos e técnicos que aumentem o poder e o controle da pessoa física sobre seus dados.

A LGPD oferece proteção e garantias ampliadas aos dados pessoais sensíveis[1], reconhecendo que se trata de categoria especial de informações, fundamentada nos princípios do livre desenvolvimento da personalidade e da não discriminação. Diante do conteúdo e da natureza da informação que os dados sensíveis trazem, eles apresentam dados cujo tratamento pode ensejar discriminações ilícitas ou abusivas de seu titular, devendo, portanto, ser protegidos de forma ampliada (TEFFÉ, 2022).

O tratamento de dados sensíveis para fins legítimos e específicos deverá ser acompanhado por salvaguardas adequadas, como bases legais específicas e mais restritas para o seu tratamento, conforme o artigo 11 da LGPD (VIOLA; TEFFÉ, 2023);[2] análises de risco; relatórios de impacto à proteção de dados pessoais;[3] e medidas de segurança organizacional e técnica. Ações alinhadas à lógica do *privacy by design* (CAVOUKIAN, 2010; EDPB, 2020) deverão ser tomadas no desenvolvimento de tecnologias de vigilância e controle, sendo incluídas avaliações prévias de impacto e medidas técnicas e organizacionais de prestação de contas (TEFFÉ, 2021).

1 Em seu Art. 5º, inciso II, a LGPD detalha dados que considerou sensíveis: aqueles que versam sobre origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político. São também sensíveis os dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos.

2 Ressalta-se o enunciado n. 690, aprovado na IX Jornada de Direito Civil do CJF, em maio de 2022: "A proteção ampliada conferida pela LGPD aos dados sensíveis deverá ser também aplicada aos casos em que houver tratamento sensível de dados pessoais, tal como observado no §1º do art. 11 da LGPD." De acordo com a LGPD (Art. 11, § 1º), a proteção disposta em seu artigo 11 será aplicada, também, a qualquer tratamento de dados pessoais que *revele* dados sensíveis e que possa causar danos ao titular, ressalvado o disposto em legislação.

3 Dispõe o enunciado n. 679, aprovado na IX Jornada de Direito Civil do CJF, em maio de 2022: "O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deve ser entendido como uma medida de prevenção e de accountability para qualquer operação de tratamento de dados considerada de "alto risco", tendo sempre como parâmetro o risco aos direitos dos titulares".

Em tecnologias de vigilância costuma ocorrer expressivo tratamento de imagens e de dados biométricos, em virtude de eles oferecerem meios de identificar e autenticar indivíduos, com base em um conjunto de dados verificáveis, únicos e específicos sobre seus titulares. Com a biometria, mostra-se possível estabelecer a identidade de alguém medindo e analisando seus atributos fisiológicos (morfológicos ou biológicos) ou comportamentais. À medida que a tecnologia avança, o uso de características humanas como informação continuará a apresentar desafios às noções de privacidade e proteção de dados. A biometria é geralmente considerada forte e valiosa para sistemas de autenticação. No entanto, é necessário entender maneiras de proteger melhor esses dados e evitar tratamentos desproporcionais e não estritamente necessários. Além de questões relacionadas à segurança pública, persecução criminal e prevenção do terrorismo, nos últimos tempos, tem havido um crescente debate sobre o estabelecimento de bases de dados biométricos para identificação de cidadãos em processos de validação de identidade e para concessão de benefícios financeiros do governo.

O artigo 4º da LGPD apresenta hipóteses em que esta lei não se aplicará ao tratamento de dados pessoais realizado por agentes públicos e/ou privados. A disposição mostra-se particularmente relevante para o presente estudo, uma vez que ela excepciona, em seu inciso III, da aplicação direta da LGPD o tratamento de dados realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais. Dispõe o §1º, do art.4º, da LGPD, que o tratamento de dados pessoais previsto no inciso III será regido por *legislação específica*, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. Adicionalmente, a Autoridade Nacional de Proteção de Dados emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de

impacto à proteção de dados pessoais (§3º), sendo este um caso de obrigatoriedade de elaboração do relatório (TEFFÉ; FERNANDES, 2020).

Diante da previsão legal, uma comissão de juristas foi criada pelo presidente da Câmara na época para elaborar anteprojeto de legislação específica, que foi divulgado em novembro de 2020 e ficou conhecido como a "LGPD Penal". Este projeto busca oferecer parâmetros específicos para operações de tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal, visando a equilibrar tanto a proteção do titular contra abusos quanto o acesso de autoridades a ferramentas e plataformas para segurança pública e investigações (CÂMARA DOS DEPUTADOS, 2019). Quando publicada, esta legislação específica impactará profundamente as estruturas públicas que fazem uso de reconhecimento facial e será relevante para promover um tratamento adequado e em âmbito federal à temática.

No Brasil, até o momento, o uso de tecnologias de reconhecimento facial vem ocorrendo em certos casos, tanto pelo setor público quanto pelo privado, havendo, porém, pouquíssima regulação a respeito do tema. Há algumas escassas normas estaduais[4] e muni-

4 No âmbito do Distrito Federal, a Lei nº 6.712/20 dispõe sobre o uso de tecnologia de reconhecimento facial na segurança pública. Há, ainda, leis estaduais sobre a aplicação de reconhecimento facial em estádios de futebol, como a Lei nº 21.737/15 do Estado de Minas Gerais e a Lei nº 8.113/19 do Estado de Alagoas. Nas duas, não há qualquer indicação acerca da finalidade e da necessidade do uso dessa tecnologia no referido ambiente. Acerca do tratamento de dados biométricos e da identificação de pessoas naturais em transportes para controle das gratuidades e dos benefícios tarifários, no estado do Rio de Janeiro, vale mencionar a Lei nº 4.291/04. No estado do Rio de Janeiro, a Lei nº 9.167/21 dispõe que o Poder Executivo poderá instituir o Banco de Dados de Reconhecimento Facial e Digital de Crianças e Adolescentes Desaparecidos, vinculado ao Detran/RJ. Ainda no RJ, o Decreto nº 48.230/22 institui o comitê gestor de tecnologia da informação dos órgãos e secretarias com atribuições de segurança pública e dá outras providências. No Ceará, o Decreto nº 34.135/21 dispõe sobre o recadastramento e a prova de vida dos beneficiários do sistema único de previdência social do estado do Ceará e do sistema de proteção social dos militares do estado do Ceará e institui a plataforma digital "cearáprev on line". Nele, há referência a reconhecimento facial como possibilida-

cipais[5] abordando superficialmente áreas de sua aplicação, como para a segurança pública e identificação de pessoas. Paralelamente, encon-

de de reconhecimento de pessoa e prova de vida. Na Paraíba, a Lei nº 11.858/21 obriga o aviso sobre o reconhecimento facial em estabelecimentos comerciais. Em Rondônia, o Decreto nº 27.481/22 regulamenta a Carteira de Identidade Funcional do Estado de Rondônia. Em formato digital, ela disporá – entre outros requisitos – "de recurso de comparação facial para ativação no dispositivo, com utilização de biometria facial, com tecnologia de detecção de vida por meio da ferramenta Liveness Check, a qual possibilita verificar se a pessoa do outro lado da tela está ao vivo, evitando, assim, que o sistema de reconhecimento facial possa ser ludibriado".

5 A Lei nº 1.556/2019 autoriza o Poder Executivo a promover a instalação de câmeras de vídeo, com dispositivo para gravação de imagens, bem como equipamentos de reconhecimento facial nos estabelecimentos pertencentes à rede pública municipal de ensino do Município de Terra Boa – Paraná. No Município de Paranaguá (PR), o Decreto nº 3763/2016 dispõe sobre o sistema de bilhetagem eletrônica no serviço público de transporte coletivo urbano de passageiros do município de Paranaguá, havendo possibilidade de controle do sistema de bilhetagem eletrônica por meio de reconhecimento facial. No município de Cascavel, o Decreto nº 12.333/15 dispõe sobre o sistema de bilhetagem eletrônica no serviço público de transporte coletivo urbano de passageiros do município de Cascavel, havendo possibilidade de controle do sistema de bilhetagem eletrônica por meio de reconhecimento facial. No Município de Jaraguá do Sul (SC), o Decreto nº 16.376/2022 regulamenta os procedimentos administrativos para implantação do sistema de reconhecimento biométrico facial no transporte coletivo de passageiros do município de Jaraguá do Sul. No mesmo local, o Decreto nº12.295/2018 regulamenta o Sistema de Bilhetagem Eletrônica (SBE) no Sistema de Transporte Coletivo de Passageiros do Município de Jaraguá do Sul. No município de Ibicaré, a Lei nº 2.015/22 autoriza o poder executivo a firmar termo de cooperação com o estado de Santa Catarina, por intermédio da secretaria de estado da segurança pública. Em São Paulo, seus municípios apresentam leis que versam sobre reconhecimento facial especialmente aplicado para identificação de pessoas em contextos de segurança. A Lei nº 4.161/2022 torna obrigatória a instalação de câmeras de monitoramento no interior dos veículos de transporte escolar municipal de José Bonifácio. A Lei nº 1.187/22 autoriza o poder executivo a firmar convênio com o estado de São Paulo, por intermédio da secretaria da segurança pública. A Lei nº 4.157/21 regulamenta o serviço de transporte remunerado privado individual de passageiros mediante compartilhamento de veículos a partir de plataforma tecnológica, no âmbito do município de Itararé/SP. A Lei Complementar nº 2.983/19 autoriza o poder executivo a conceder isenção de tarifa do transporte público urbano coletivo de passageiros, no âmbito do município, sob a gestão da Transerp

tram-se em discussão projetos de lei em diferentes âmbitos acerca do tema.[6]

Acertadamente, em maio de 2023, iniciou a tramitação do PL 2338, que dispõe sobre o uso da Inteligência Artificial. Em seu texto, há tratamento normativo a sistemas biométricos de identificação utilizados no âmbito de atividades de segurança pública (art. 15) e referências específicas quanto ao seu risco.[7] Não há dúvida de que o desenvolvimento de leis federais voltadas ao tema dentro dos recortes de IA e de proteção de dados são fundamentais para a adequada regulação da matéria.

Não obstante a falta de legislação específica em vigor, algumas cidades vêm fazendo o uso de tal tecnologia buscando, como afirmam, promover a segurança pública; identificar suspeitos e procurados pela Justiça; controlar entradas no território e o acesso a locais restritos; coibir o uso indevido de gratuidades; e evitar crimes em transportes públicos, estádios de futebol, pedágios e espaços públicos.

Neste debate, algumas questões nos preocupam: como é feito o monitoramento? Qual a localização das câmeras? Elas trabalham 24 horas por dia? Os dados são analisados em tempo real? Para onde vão os da-

– empresa de trânsito e transporte urbano de Ribeirão Preto s/a, às pessoas com deficiência.

6 Recorda-se, aqui, o projeto de lei federal nº 2.392/2022, apresentado em agosto de 2022, que dispõe sobre o uso de tecnologias de reconhecimento facial nos setores público e privado. Em São Paulo, o projeto de lei nº 385/22 dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo Poder Público no Estado de São Paulo.

7 A proposta brasileira para a IA dialoga com a proposta europeia, apresentada em abril de 2021 e que caminha rapidamente para ser aprovada na região. O chamado *AI Act* introduz regras para tecnologias que fazem uso de biometria e as diferencia de acordo com seus níveis de risco e características. No cenário europeu, verifica-se especial preocupação a respeito da utilização de sistemas de reconhecimento facial aplicados em tempo real em espaços públicos. Informações disponíveis em: https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence Acesso em: 16 maio 2023.

dos processados pelos dispositivos? Qual é o tempo de retenção? Quem pode acessar as informações? Como as pessoas são identificadas? Qual banco de dados é utilizado para identificar as pessoas?

Criar bancos de dados mais diversificados para treinar máquinas e IAs, buscar equipes mais diversas, trabalhar códigos inclusivos, auditar tecnologias e evitar práticas discriminatórias são questões essenciais para o desenvolvimento de tecnologias mais inclusivas, justas e éticas (SELINGER; LEONG, 2021).

A utilização de tecnologias de reconhecimento facial traz diversas controvérsias. Em todo o mundo, cidades e empresas privadas vêm debatendo amplamente sua aplicação, limites e, até mesmo, eventual banimento. Busca-se também maior aprimoramento tecnológico e desenvolvimento de legislação específica. Além das questões relacionadas à proteção das liberdades fundamentais, existe uma grande preocupação de que os sistemas de reconhecimento facial sejam imprecisos e perpetuem cenários de preconceito, estigmatização e discriminação racial. A relação desenvolvida entre reconhecimento facial, segurança pública e policiamento gera profundas preocupações quanto aos riscos de uma aplicação ampla e generalizada de tal ferramenta.

Diferenças na taxa de acerto no reconhecimento de pessoas de diferentes raças (sendo os falsos positivos mais comuns em rostos de negros), gêneros e idades já foram demonstradas. O viés é especialmente agravado no campo da segurança pública, devido às relações históricas de desigualdade e discriminação contra populações socialmente vulneráveis. Sem os devidos cuidados, os algoritmos podem aprofundar as desigualdades e fazer com que medidas coercitivas sejam tomadas de forma equivocada. Dada a expansão dessa tecnologia e os riscos que ela pode gerar, mostra-se necessário promover um debate público, multissetorial e informado sobre onde, como e quando aplicá-la.

Indubitavelmente, a utilização de ferramentas de reconhecimento facial com análise em tempo real em espaços públicos, no estado da arte em que se encontram, é cercada de polêmicas por afetar diversas ques-

tões relacionadas às liberdades fundamentais e igualdade. Os recursos de identificação pessoal por meio da tecnologia de reconhecimento facial possuem atributos únicos que requerem atenção e regulação destacada. Eles permitem capturar imagens faciais remotamente, sem conhecimento ou consentimento de seus titulares, na busca por identificá-los. No entanto, alega-se que a proibição total de seu uso, em qualquer circunstância, poderia prejudicar questões de interesse coletivo e público, como ações estatais e policiais voltadas principalmente ao combate ao tráfico de pessoas, armas e drogas; à prevenção do terrorismo; a programas sociais para localização de desaparecidos; e à contenção da violência urbana.

Assim, são sugeridas, além de uma legislação geral, forte e de âmbito federal sobre a matéria, que aborde aspectos tanto de IA quanto de proteção de dados, medidas como: relatórios de análise de impacto regulatório; avaliação de impacto na proteção de dados; análises de riscos e de assimetrias; supervisão humana na aplicação e uso das tecnologias;[8] treinamento de pessoal e restrição de acesso às tecnologias e bancos de dados; autorização judicial prévia; restrições à imposição de vigilância em tempo real; desenvolvimento de protocolos específicos envolvendo as forças de segurança; responsabilização efetiva por erros e excessos; e investimento constante no aprimoramento da tecnologia.

Políticos e legisladores de todo o mundo têm a oportunidade de discutir – em contextos multissetoriais – como implementar controles mais rígidos sobre o uso desses sistemas. Considerando as experiências estrangeiras e os debates atuais, o Brasil deve seguir as mais avançadas estratégias de IA para desenvolver leis que efetivamente protejam os

8 Conforme o artigo 14 – *Human oversight* – da Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas sobre a inteligência artificial (*Artificial Intelligence Act*) e que altera certos atos legislativos da união. Disponível em: eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (acesso em 21 de novembro de 2022)

direitos humanos. Sabe-se que, com uma eventual expansão do reconhecimento facial para fins de segurança pública, o Estado terá ampla capacidade de rastrear seus cidadãos, verificar os locais que frequentam e manter bancos de dados com informações bastante precisas sobre eles. Fato, sem dúvida, extremamente preocupante em termos de proteção aos direitos fundamentais. A coleta de imagens de rostos pode acabar ocorrendo sem o conhecimento efetivo dos indivíduos, abrindo as portas para uma vigilância biométrica coletiva, opaca e não transparente. Isso impõe a observância de normas legais e códigos de ética, sendo relevante também a contínua fiscalização e responsabilização dos agentes.

A autonomia e a relevância das cidades na federação brasileira: um estudo das competências legislativas para a regulação de tecnologias de reconhecimento facial voltadas à segurança pública

Conforme discutido, existem várias preocupações sobre o uso de sistemas de reconhecimento facial nas cidades. Assim, mostra-se essencial uma regulamentação bastante restrita e específica sobre a sua eventual utilização para fins de segurança pública. No contexto do federalismo brasileiro surge o seguinte questionamento: qual é o ente federativo responsável por legislar sobre o uso de sistemas de reconhecimento facial para fins de segurança pública? A questão ainda não foi discutida pelo STF, nem recebeu atenção especial dos constitucionalistas. Apesar de a União não ter editado normas gerais sobre o tema, alguns estados e municípios têm se adiantado em aprovar legislação específica para atender às suas demandas.

A Federação é um espaço de convivência entre esferas de poder autônomas. É a Constituição Federal a garantidora da unidade harmônica entre os entes da Federação, ao prever mecanismos efetivos de resolução de conflitos e um sólido sistema de repartição de competências, o

qual parte do pressuposto de que não existiria hierarquia entre eles. A Constituição apresenta um complexo sistema de distribuição de competências, que conjuga a enumeração explícita de competências administrativas, legislativas e tributárias para os entes federativos com áreas de competência compartilhada entre eles. A alocação das competências entre os entes da Federação é realizada com base no princípio da predominância do interesse, segundo o qual o ente federativo que tiver em determinada matéria interesse preponderante será competente para tratar dela.

As matérias que recaem sobre as competências legislativas privativas da União são extremamente amplas, abarcando grande parte dos temas relacionados ao Direito, com a possibilidade de a União, por meio de lei complementar, delegar aos Estados o poder de legislar sobre questões específicas das matérias elencadas no artigo 22 da Constituição. Neste sentido, a Federação brasileira é centralizada, pois, de fato, há um maior número de competências atribuídas ao ente central do que aos entes subnacionais, "o que em grande medida corrói o caráter cooperativo do federalismo brasileiro" (SILVA, 2021, p. 354).

Aos estados, a Constituição aloca a competência legislativa privativa do artigo 25, §2º, as competências concorrente e suplementar do artigo 24 e as competências residuais do artigo 25, §1º. Aos municípios são atribuídas competências legislativas privativas e suplementares sobre assuntos de interesse local previstas no artigo 30 da Constituição e, por sua vez, ao Distrito Federal são reservadas competências de natureza estadual e municipal, em razão de sua natureza de ente híbrido (DOLINGER; BARROSO, 2014).

A Constituição, em seu artigo 24, confere também à União competências legislativas ao lado dos estados e Distrito Federal. Neste domínio, os entes possuem competência para legislar, mas sob condições distintas. No âmbito da competência concorrente, os estados e o Distrito Federal, na ausência de lei federal, podem legislar plenamente, com o objetivo de atender suas peculiaridades (artigo 24 §3º). Sobrevindo nor-

ma geral da União, a lei estadual ou distrital terá sua eficácia suspensa, no que lhe for contrário (artigo 24 §4º).

No âmbito da competência suplementar, a União estabelece bases, diretrizes e princípios gerais que servem de norte para o sistema jurídico, enquanto estados, Distrito Federal e municípios editam normas específicas de forma a complementar a legislação federal. Vale sublinhar que os municípios possuem tão somente a competência suplementar, no que couber, sobre as matérias dispostas no artigo 24 da Constituição, observada a cláusula do interesse local, de acordo com os incisos I e II do artigo 30.

Logo, estados e municípios devem ter prioridade na atuação específica, para atender às demandas de sua população, que variam segundo fatores socioeconômicos do ente, contanto que em respeito à legislação federal. Conforme o fenômeno do bloqueio de competências, normas estaduais, distritais e municipais contrárias à legislação federal serão consideradas inconstitucionais e, por consequência, terão seus efeitos suspensos. Do mesmo modo, o artigo 24 da Constituição impõe limites à atuação da União:

> Se a autoridade central ultrapassar os limites de sua competência legislativa, a lei resultante será inconstitucional e, consequentemente, nula. (...) nas áreas de competência concorrente, a União apenas editará normas gerais. A edição de normas específicas – invadindo a jurisdição dos estados – viola a atribuição de competência legislativa prevista na Constituição (DOLINGER; BARROSO, 2014, p. 157-158).

Dadas as considerações anteriores, cabe analisar a relevância que as cidades vêm tomando nas últimas décadas, emergindo como atores significativos em processos de tomada de decisão em temas diversos. O processo de urbanização acarretou o deslocamento de poder político e econômico aos governos locais responsáveis pela gestão dessas áreas urbanas. Algumas cidades tornaram-se verdadeiras metrópoles, onde sur-

gem novas identidades e centros de poder (DILL, 2001). O poder central, cada vez mais visto como burocrático e distante do cidadão, vem perdendo terreno para o poder local. As cidades passam a conduzir experimentos bem-sucedidos voltados ao bem-estar social, meio ambiente e proteção de minorias, assumindo um papel ativo na governança global (BLANK, 2010).

Nessa perspectiva, o federalismo brasileiro (SILVA, 2021) é caracterizado como um "federalismo profundo", que leva a sério o papel dos municípios (KING, 2014). A Constituição brasileira atribui às cidades uma posição de destaque em comparação com outras constituições federativas. Em seu artigo 182, prevê a implementação de uma política de desenvolvimento urbano que priorize a função social das cidades e o bem-estar público. Em adição, em julho de 2001, foi publicado o Estatuto da Cidade, Lei nº 10.257, que regulamenta o capítulo "política urbana" da CF/88.

No entanto, de acordo com as normas constitucionais que regem a Federação brasileira, a autonomia municipal é mais limitada que a estadual. Ao contrário dos estados, os municípios brasileiros não possuem constituição, mas são organizados por leis orgânicas ordinárias. Eles não têm uma representação política forte no nível federal como os estados. Assim, os municípios não participam do processo de reforma constitucional nem do sistema de controle abstrato de constitucionalidade perante o Supremo Tribunal Federal (STF). Além disso, o exercício das competências municipais está sujeito à Constituição Federal e à constituição estadual. Os municípios brasileiros dependem financeiramente dos recursos distribuídos pela União e pelos estados (DOLINGER; BARROSO, 2014). Na prática, o financiamento de projetos de desenvolvimento urbano depende, em grande parte, do alinhamento político entre os governos federal, estaduais e municipais (HIRSCHL, 2020).

O artigo 29 da Constituição Brasileira estabelece a autonomia municipal e as suas prerrogativas legislativas e administrativas, inclusive a

gestão financeira. Os municípios têm competência legislativa complementar, nas matérias enumeradas no art. 24, para atender às demandas e necessidades locais por meio da edição de normas específicas em consonância com as legislações federal e estadual vigentes. Além disso, as cidades legislam sobre assuntos de interesse local, como, por exemplo, coleta de lixo e horário de funcionamento de comércios e estabelecimentos (DOLINGER; BARROSO, 2014).

Parte da doutrina defende uma interpretação ampla do termo "interesse local" para garantir a efetividade das atribuições constitucionais aos municípios e o valor constitucional da descentralização. Caso contrário, restariam poucas competências aos municípios, dadas as amplas competências da União e os poderes residuais reservados aos estados. Assim, entende-se que o termo "interesse local" não se restringiria a assuntos de interesse exclusivo de determinado município, mas abrangeria qualquer assunto que se mostrasse necessário para o estabelecimento de políticas locais, ainda que afetasse indiretamente outras unidades da Federação (HERMANY, 2012).

Dentro dessa perspectiva, o princípio da subsidiariedade é de fundamental importância. A subsidiariedade é uma noção presente nas estruturas federativas que reconhecem aos municípios um *status* especial (BLANK, 2010), como o federalismo brasileiro. O princípio declara que o governo central exercerá suas atribuições apenas para apoiar os entes subnacionais, ou seja, só atuará se os governos subnacionais estiverem impossibilitados de realizar sozinhos a tarefa a ser realizada (HALBERSTAM, 2009). Quando aplicado no contexto da repartição de competências entre os entes federativos, o princípio da subsidiariedade serve para conciliar uniformidade e flexibilidade face às realidades regionais e locais, "enfatizando uma visão mais pluralista e espacialmente consciente do direito público" (HIRSCHL, 2020, p. 15). No que diz respeito à competência legislativa municipal, a noção de subsidiariedade privilegia a realização do interesse local, de acordo com as legislações federal e estadual vigentes (LIMA, 2013).

Por vezes, surgem dificuldades de interpretação na definição das competências de cada ente. Uma matéria de direito civil – que se enquadra no poder legislativo privativo da União – pode ser, ao mesmo tempo, matéria de interesse local de determinado município. A definição do conteúdo preponderante de determinada lei é definida pelo STF quando exerce seu papel na solução de conflitos entre as competências dos entes federativos. A partir da identificação do tema preponderante, o STF atribui ao ente federativo responsável por regular sobre ele (conforme a CF/88) a respectiva competência legislativa. Na jurisprudência do STF, não há fatores ou critérios fixos para a definição do tema preponderante e, por consequência, a competência federativa. Sobre o uso de TRFs o STF ainda não se pronunciou a respeito.

De todo modo, ao se analisar sua jurisprudência, percebe-se que o STF costuma decidir em favor da União em controvérsias relativas a matérias de competência privativa federal (DOLINGER; BARROSO, 2014, p. 159). No que diz respeito às competências concorrentes e suplementares, o STF "raramente declara uma lei federal inconstitucional com base na alegação de que suas normas não são gerais" (SILVA, 2021, p. 371). No entanto, em determinados casos, o Tribunal aplica os princípios da subsidiariedade e da cooperação, garantindo, assim, o exercício das competências pelos municípios, tendo em conta as respectivas realidades.

A Constituição brasileira de 1988 é um marco histórico no que diz respeito à descentralização política em favor das cidades. Os municípios passaram a ser responsáveis pela implementação da maior parte das políticas e serviços sociais, além de exercer novas competências legislativas relacionadas a assuntos de interesse local. Não obstante, a Federação brasileira continua caracterizada como centralizada, não apenas pela dependência financeira da maioria dos municípios das transferências federais de receitas – para atender às necessidades da população –, mas também pela ampla competência legislativa da União na definição de regras e diretrizes gerais a serem observadas pelos municípios na execução das políticas e serviços sociais (PIANCASTELLI, 2006).

Em todo o caso, a resposta à questão deve ser fundamentada por normas constitucionais relativas à repartição das competências federativas e princípios fundamentais que orientam a sua aplicação, nomeadamente os princípios do interesse predominante e da subsidiariedade. O primeiro passo é identificar o assunto dominante na questão específica do uso de tecnologias de reconhecimento facial para fins de segurança pública. Isso é importante, na próxima etapa, para apontar qual unidade da federação terá interesse predominante no assunto, com base nas normas e princípios constitucionais federativos.

A dificuldade reside na identificação do assunto dominante relacionado ao uso de tecnologias de reconhecimento facial para fins de segurança pública. É possível identificar dois grandes temas nessa matéria: a) "direito civil" e "proteção e tratamento de dados pessoais"[9] (Art. 22, incisos I e XXX, respectivamente, da CF), por se tratar de tecnologia cujo funcionamento depende do tratamento de dados pessoais, mas que afeta também diretamente os direitos da personalidade, previstos no Código Civil Brasileiro; e b) segurança pública, porque a prevenção e o combate a crimes são as finalidades específicas pretendidas pelos sistemas de reconhecimento facial neste caso.

Se o direito civil ou o tratamento de dados pessoais for matéria dominante, a União terá competência para legislar sobre o uso de tecnologias de reconhecimento facial para fins de segurança pública, nos termos do artigo 22 da Constituição. Nesse cenário, os estados e o Distrito Federal somente poderiam legislar sobre questões específicas quanto ao

9 Em fevereiro de 2022, entrou em vigor a Emenda Constitucional nº 115, que acrescentou o inciso XXX ao artigo 22 para estabelecer a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. O objetivo é uniformizar a legislação devido à existência de vários projetos de lei estaduais e municipais sobre o tema e, consequentemente, evitar a fragmentação normativa e a multiplicidade de critérios definidos por cada região e município. A Emenda Constitucional nº 115/22 também incluiu o inciso XXVI ao artigo 21, para determinar a competência exclusiva da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei.

uso de tecnologias de reconhecimento facial, para fins de segurança pública, quando autorizados pela União por meio de lei complementar (artigo 22, par. único). Atualmente, não existe nenhuma lei complementar vigente desse tipo. Por sua vez, aos municípios não seria atribuída qualquer competência nas matérias enumeradas no artigo 22, pelo que não lhes seriam reconhecidas competências legislativas sobre a utilização de tecnologias de reconhecimento facial para efeitos de segurança pública.

Quando trata de temas ligados à vigilância e segurança pública, no julgamento de conflitos de competências entre os entes federativos, o STF prioriza o interesse dos entes subnacionais. Em 2020, o STF, por maioria de votos, declarou constitucional a Lei nº 10.501/1997, do estado de Santa Catarina, com efeitos gerais. A lei obriga bancos e instituições financeiras localizadas neste estado a instalar sistemas de segurança, como guardas, portas de segurança e alarmes. O relator, Ministro Edson Fachin, em seu voto, seguido pela maioria, julgou improcedente a ação e declarou constitucional a lei estadual baseada no poder legislativo dos estados, Distrito Federal e municípios em matéria de segurança pública. A Constituição utiliza a expressão "é dever do Estado" para tratar de temas específicos, nomeadamente segurança pública (artigo 144), saúde (artigo 196), educação (artigos 205 e 208) e desporto (artigo 217). Saúde, educação e esporte são elencados como matérias de competência legislativa concorrente e complementar dos estados, Distrito Federal e municípios (artigo 24 IX e XII). Em consonância com essa consideração, o Tribunal entende que a Constituição também confere ao tema da segurança pública a qualificação de matéria de competência legislativa dos estados, do Distrito Federal e dos municípios (SUPREMO TRIBUNAL FEDERAL, 2020).

O Ministro Fachin esclarece que a lei estadual de Santa Catarina abrange dois temas principais, especificamente instituições financeiras e segurança pública. De um lado, a União tem competência privativa para legislar sobre as instituições financeiras (artigo 22 VI e VII); de outro, os estados têm competência concorrente e suplementar para legislar sobre

segurança pública (art. 24, IX e XII). Nesses casos, o Ministro adverte que dúvidas sobre o exercício da competência legislativa pelos entes federativos poderão surgir e o princípio do interesse predominante nem sempre oferecerá uma solução satisfatória. Com isso, o intérprete deverá invocar outros princípios do federalismo brasileiro, como a subsidiariedade e a cooperação, para dirimir o conflito de competência.

O presente trabalho segue o entendimento do STF expresso no caso descrito acima: "Nos casos em que houver dúvida quanto à identificação da competência legislativa, por haver mais de uma matéria abrangida pela disposição legal em causa, o tribunal deve escolher a interpretação que não prejudique a competência que as entidades de menor dimensão têm para legislar sobre determinada matéria" (SUPREMO TRIBUNAL FEDERAL, 2020, p. 3). Para as iniciativas de regulação de TRFs em nível estadual e municipal, a referida decisão do STF é um precedente importante em favor do reconhecimento da prevalência das competências dos entes subnacionais em matérias de interesse regional e local.

É possível entender que o assunto dominante relacionado ao uso de tecnologias de reconhecimento facial para fins de segurança pública seria a segurança pública. Nesta matéria, os estados, o Distrito Federal e os municípios têm poderes concorrentes e complementares para legislar junto à União, conforme decisão do STF. Em seu voto, o Ministro Alexandre de Moraes destacou que:

> Quando aplicado no âmbito da Federação brasileira, o princípio da subsidiariedade (...) deve potencializar a atuação preponderante do ente federado dentro de sua esfera de competência na medida em que sua maior capacidade de resolução de assuntos de interesse público, observadas as peculiaridades regionais. A maior autonomia do Estado para legislar sobre assuntos relacionados à segurança pública e penitenciária possibilitará melhor observância das peculiaridades regionais e eficiência no combate ao crime organizado, inclusive no interior das unidades penitenciárias (SUPREMO TRIBUNAL FEDERAL, 2020, p. 11).

Tramita no Congresso Nacional a Proposta de Emenda Constitucional (PEC) nº 33/2014, que pretende alterar os artigos 23 e 24 para inserir textualmente o tema da segurança pública no âmbito das competências comuns, concorrentes e suplementares dos entes federativos. Na justificativa da proposta, os autores explicam que a alteração serve apenas para sanar a omissão do constituinte originário (SENADO FEDERAL, 2014). Da mesma forma, o Ministro Fachin destaca em seu voto que a PEC nº 33/2014 "procura, assim, explicitar o que já decorre de uma interpretação sistemática da Constituição" (SUPREMO TRIBUNAL FEDERAL, 2020, p. 6), qual seja, o poder legislativo dos entes subnacionais além da União sobre a matéria de segurança pública.

Em conclusão, defendemos que todos os entes da Federação brasileira têm competência para legislar sobre a matéria específica do uso de tecnologias de reconhecimento facial para fins de segurança pública, quando este tema for reconhecido como o preponderante pelo STF no julgamento de conflitos de competência federativa. Entretanto, necessário ressaltar que nesta hipótese caberá à União estabelecer em lei os princípios, limites e regras gerais sobre o assunto, podendo, os estados, o Distrito Federal e os municípios complementarem a legislação federal por meio da edição de normas específicas para atender às necessidades regionais e locais na área de segurança pública.

Considerações finais

O processo de urbanização tem levado as cidades a ocuparem posição de destaque no cenário mundial. Por meio de lideranças responsivas e boas práticas, muitas cidades começam a experimentar com sucesso programas econômicos, sociais e ambientais, revelando-se como espaços de eficiência e inovação. Nessa perspectiva, mostra-se de grande importância o conceito de cidades inteligentes, que utilizam novas tecnologias para implementar políticas públicas e impulsionar processos que garantam qualidade de vida aos cidadãos.

A violência urbana é um problema comum nas chamadas megacidades. Dessa forma, é cada vez mais frequente a utilização de novas tecnologias no combate à criminalidade. Conforme destacado, existem várias preocupações associadas ao uso de sistemas de reconhecimento facial para fins de segurança pública, como vigilância em massa, tratamento abusivo ou indevido de dados pessoais sensíveis, violações a direitos e liberdades fundamentais, alta taxas de erro (especialmente em face de certos grupos e minorias) e falta de transparência. Esses riscos são exacerbados em sociedades caracterizadas pela desigualdade social e pela discriminação racial. Justamente por isso, tais tecnologias precisam, além de discussões multissetoriais aprofundadas e um desenvolvimento mais refinado, de uma regulamentação base que observe cuidadosamente a proteção dos direitos fundamentais, normas internacionais de direitos humanos e considerações éticas.

Com base nas normas constitucionais vigentes e na jurisprudência do STF, é possível concluir que todos os entes da federação brasileira têm competência para legislar sobre a matéria específica do uso de tecnologias de reconhecimento facial para segurança pública. Caberá à União, porém, estabelecer inicialmente em lei os princípios e normas gerais sobre a matéria, e aos estados, Distrito Federal e municípios complementarem a legislação federal, por meio da edição de normas específicas para atender às suas demandas particulares no campo da segurança pública, mas sem desrespeitar os parâmetros gerais estabelecidos pela União.

Conforme explicado, ainda não existe uma lei federal sobre o uso de sistemas de reconhecimento facial no Brasil nem uma legislação específica para a proteção de dados pessoais dentro das atividades de segurança pública, defesa nacional ou investigação e repressão de infrações penais. Para a coexistência harmônica entre as diversas legislações, será fundamental que, por um lado, a União edite normas gerais sobre o tema – estabelecendo princípios e diretrizes gerais de ação para os demais entes federativos – e, por outro, os estados, Distrito Federal e municípios desenvolvam leis específicas respeitando as normas gerais

federais. Os municípios também devem observar a legislação estadual vigente. A posição favorável à competência legislativa de todos os entes federativos brasileiros sobre o uso de tecnologias de reconhecimento facial para fins de segurança pública reflete a vontade da Constituição de 1988 de concretizar a descentralização política e, consequentemente, o exercício democrático do poder político.

Um marco legal sobre o uso de tecnologias de reconhecimento facial, especialmente para fins de segurança pública, mostra-se urgente no Brasil, diante das diversas aplicações já presentes dessa tecnologia e de seus possíveis riscos para os direitos e garantias fundamentais. A coleta de imagens pessoais vem ocorrendo, por vezes, sem um efetivo conhecimento dos indivíduos, abrindo as portas para uma vigilância biométrica coletiva, opaca e não transparente. Isso impõe a observância de normas legais e códigos de ética, sendo relevante também a contínua fiscalização e responsabilização dos agentes.

De acordo com o modelo cooperativo do federalismo brasileiro, é possível conciliar a autonomia local – com atenção especial às peculiaridades das cidades – com a necessidade de articulação de ações entre todas as unidades federativas, com base em diretrizes gerais definidas pela União. Assim, é imprescindível a edição de legislação federal que estabeleça um modelo normativo geral baseado nos princípios constitucionais, em estudos recentes a respeito da temática, boas práticas internacionais e na LGPD brasileira, de forma a se garantir ampla proteção aos direitos e responsabilidades específicas a todo agente que utilizar ferramentas de reconhecimento facial.

Referências

ACCESSNOW. **Ban Biometric Surveillance**. 2021. Disponível em: https://www.accessnow.org/campaign/ban-biometric-surveillance/ (acesso em 16 de novembro de 2022)

BLANK, Yishai. Federalism, Subsidiarity, and the Role of Local Governments in an Age of Global Multilevel Governance. **Fordham Urban Law Journal**, v. 37, n. 2, 2010, pp. 509-558.

CÂMARA DOS DEPUTADOS. Exposição de motivos: Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. O Anteprojeto de Lei, na versão apresentada pela Comissão de Juristas. 2019. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf (acesso em 18 de novembro de 2022)

CÂMARA RIO. "Identificação facial é tema de audiência de Comissão Especial". 30 de junho de 2021. Disponível em: http://www.camara.rio/comunicacao/noticias/394-identificacao-facial-e-tema-de-audiencia-de-comissao-especial (acesso em 28 de novembro de 2022)

CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Disponível em: https://iapp.org/resources/article/oipc-privacy-by-design-resources/ (acesso em 9 de abril de 2021)

DATA RIO. **População residente estimada do Município do Rio de Janeiro – 1970 a 2021**. 21 de setembro de 2022. Disponível em: https://www.data.rio/documents/90106eb8874f4e8fbbc27678bbb1e772/about (acesso em 16 de novembro de 2022)

DILL, Guenter. O município em tempos de globalização. In: HOFMEISTER, Wilhelm; CARNEIRO, José Mário Brasiliense. **Federalismo na Alemanha e no Brasil**. Série Debates, n. 22. São Paulo: Fundação Konrad Adenauer, 2001.

DOLINGER, Jacob; BARROSO, Luís Roberto. Federalism and Legal Unification in Brazil. In: HALBERSTAM, Daniel; REIMANN, Mathias (eds.). **Federalism and Legal Unification: a Comparative Empirical Investigation of Twenty Systems**. Dordrecht: Springer, 2014, pp. 153-167.

EDPB. **Guidelines 4/2019 on Article 25 Data Protection by Design and by Default**. 20 de outubro de 2020.

EDPB. **Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement.** Versão 2.0. Adotada em 26 de abril de 2023.

EDWARDS, Lilian. Privacy, security, and data protection in smart cities: a critical EU law perspective. **CREATe Working Paper** 2015/11. Disponível em: https://www.create.ac.uk/publications/privacy-security-and-data-protection-in-smart-cities-a-critical-eu-law-perspective/ (acesso em 28 de novembro de 2022)

EUR-LEX. **Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial** (Artificial Intelligence Act) e altera determinados atos legislativos da União. Disponível em: ht-

tps://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206&qid=1669129300818 (acesso em 22 de novembro de 2022)

G1. "Em ano de pandemia, saúde bate recorde como principal problema apontado pelos eleitores nas capitais, segundo Ibope". **g1.globo.com**, 9 de outubro de 2020. Disponível em: https://g1.globo.com/politica/eleicoes/2020/eleicao-em-numeros/noticia/2020/10/09/em-ano-de-pandemia-saude-bate-recorde-como-principal-problema-apontado-pelos-eleitores-nas-capitais-segundo-o-ibope.ghtml (acesso em 16 de novembro de 2022)

HALBERSTAM, Daniel. Federal Powers and the Principle of Subsidiarity. In: AMAR, Vikram David; TUSHNET, Mark V. (eds.). **Global Perspectives on Constitutional Law**. New York/Oxford: Oxford University Press, 2009, pp. 34-47.

HERMANY, Ricardo. (Re)Discutindo as políticas públicas no espaço local: interconexões entre federalismo, subsidiariedade e direito social no Brasil. In: MAUÉS, Antonio Moreira (org.). **Federalismo e Constituição: estudos comparados**. Porto Alegre: Lumen Juris, 2012, pp. 83-109.

HIRSCHL, Ran. **City, State**: Constitutionalism and the Megacity. New York: Oxford University Press, 2020.

INSTITUTO IGARAPÉ. **Tecnologias policiais no contexto brasileiro**. 25 de junho de 2020. Disponível em: https://igarape.org.br/tecnologias-policiais-no-contexto-brasileiro/ (acesso em 16 de novembro de 2022)

KING, Loren. Cities, Subsidiarity and Federalism. In: FLEMING, James E.; LEVY, Jacob T. (eds.). **Federalism and Subsidiarity**. New York/London: New York University Press, 2014, pp. 291-331.

LIMA, Martonio Mont'Alverne Barreto. Art. 29. In: CANOTILHO, J. J. Gomes et al. (coords.). **Comentários à Constituição do Brasil**. São Paulo: Saraiva, 2013, pp. 782-785.

MEDIUM. "Parlamentares de todas as regiões do Brasil apresentam projetos de lei pelo banimento do reconhecimento facial em espaços públicos". *medium.com*, 21 de junho de 2022. Disponível em: https://medium.com/codingrights/parlamentares-de-todas-as-regi%C3%B5es-do-brasil-apresentam-projetos-de-lei-pelo-banimento-do-ad33a8e6552e (acesso em 16 de novembro de 2022)

PARLAMENTO EUROPEU. Resolução relativa à inteligência artificial no direito penal e seu uso pela polícia e pelas autoridades judiciais. 6 de outubro de 2021. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html (acesso em 28 de novembro de 2022)

PARLAMENTO EUROPEU. Resolução de 6 de outubro de 2021 relativa à inteligência artificial no direito penal e seu uso pela polícia e pelas autoridades judiciais em matéria penal. Disponível em: (acesso em 28 de novembro de 2022)

PASQUALE, Frank. **The black box society**. Cambridge: Harvard University Press, 2015.

PIANCASTELLI, Marcelo. The Federal Republic of Brazil. In: MAJEED, Akhtar et al (eds.). **Distribution of Powers and Responsibilities in Federal Countries**. Montreal: McGill-Queen's University Press, 2006, pp. 67-90.

PÚBLICA. "Os maiores desafios na gestão de cidades em 2021". *publica.inf.br*, 15 de dezembro de 2020. Disponível em: http://www.publica.inf.br/blog/os-maiores-desafios-na-gestao-de-cidades-em-2021 (acesso em 16 de novembro de 2022)

SEADE. "SP tem 9 municípios que concentram 42% da população paulista; São José está na lista". 20 de abril de 2022. Disponível em: https://www.seade.gov.br/sp-tem-9-municipios-que-concentram-42-da-populacao-paulista-sao-jose-esta-na-lista/ (acesso em 16 de novembro de 2022)

SELINGER, Evan; LEONG, Brenda. The Ethics of Facial Recognition Technology. In: VÉLIZ, Carissa (ed.), **The Oxford Handbook of Digital Ethics**. online edn, Oxford Academic, 2021. Disponível em: https://academic.oup.com/edited-volume/37078/chapter-abstract/337809992?redirectedFrom=fulltext (acesso em 20 de fevereiro de 2023)

SENADO FEDERAL. **Proposta de Emenda Constitucional nº 33**. 2014. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/118712 (acesso em 21 de fevereiro de 2023)

SILVA, Virgílio Afonso da. **Direito Constitucional Brasileiro**. São Paulo: Edusp, 2021.

SUPREMO TRIBUNAL FEDERAL. Pleno. **Ação Direta de Inconstitucionalidade nº 3.921/Santa Catarina**. Voto do Ministro Relator Edson Fachin. Julgamento em 28 de setembro de 2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2539577 (acesso em 21 de fevereiro de 2023)

TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Orgs.). **O Direito Civil na Era da Inteligência Artificial**. v. 1. São Paulo: Editora do Tribunais, 2020, pp. 283-310.

TEFFÉ, Chiara Spadaccini de. Compliance de dados em tecnologias de segurança e vigilância. In: FRAZÃO, Ana; CUEVA, Ricardo (Orgs.). **Compliance e políticas de proteção de dados**. v. 1. São Paulo: Thomson Reuters, 2021, pp. 1193-1230.

TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis**: qualificação, tratamento e boas práticas. São Paulo: Foco, 2022.

VETTORAZZO, Lucas; PITOMBO, João Pedro. "Rio e Salvador terão sistema de reconhecimento facial no Carnaval". *Folha de São Paulo*. 27 de fevereiro de 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/02/rio-e-salvador-terao-sistema-de-reconhecimento-facial-no-carnaval.shtml (acesso em 14 de maio de 2023).

VIOLA, Mário; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). **Tratado de Proteção de dados pessoais**. 2.ed. Rio de Janeiro: Forense, 2023, pp. 115-146.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, 30, 2015, pp. 75–89.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

Inovações europeias para a regulação de IA e tecnologias de reconhecimento facial: lições para o Brasil?

Sérgio Branco[1]

Resumo

O reconhecimento facial é uma tecnologia de inteligência artificial que vem sendo adotada em diversas localidades do mundo com a promessa de redução de índices de criminalidade. Contudo, o reconhecimento facial é também instrumento para violação de diversos direitos pessoais e coletivos e não pode ser implementado sem um debate público adequado e informado. Embora a inteligência artificial abranja uma série de ferramentas, com utilidades, propósitos e consequências variadas, é chegada a hora de ser regulada de modo abrangente, incluindo a tecnologia de reconhecimento facial. A União Europeia apresentou, em 2021, uma proposta inicial para tratar de inteligência artificial, em cujo texto se propõe o banimento do reconhecimento facial, exceto em casos bastante específicos. O Brasil, no momento, começa a debater publicamente que regras deverá adotar na regulação do tema, e nesse sentido cabe a reflexão sobre o quanto a proposta da União Europeia pode servir de

1 Gostaria de agradecer à professora e pesquisadora Chiara de Teffé pela sua contribuição valiosa e construtiva durante o processo de elaboração do artigo.

inspiração para o legislador brasileiro. É o que pretendemos identificar neste artigo.

Introdução

Em junho de 2001, o diretor de cinema estadunidense Steven Spielberg lançou o filme "Inteligência Artificial" (*A.I.: Artificial Intelligence*).[2] Ambientado no século XXII, o filme narra a história de um menino-robô chamado David que deseja se tornar uma pessoa de verdade para recuperar o amor de sua "mãe", que é humana.

No segundo ato do filme, quando David tenta descobrir como encontrar a Fada Azul, que ele imagina ser capaz de transformá-lo em um ser humano e promover um reencontro com a mãe dele, somos espectadores de uma cena fascinante por duas razões: uma prospectiva e outra retrospectiva.[3] Vejamos a razão prospectiva.

David entra em um tipo de cyber café acompanhado de outro robô, de aparência adulta, chamado Gigolo Joe. No cyber café, mediante o acionamento de um botão, um personagem holográfico chamado Dr. Know surge atrás de uma cortina para espanto de David e afirma: "perguntem ao Dr. Know, não há nada que eu não saiba".

Animado com a proposta, David indaga onde ele poderia encontrar a Fada Azul, ao que o Dr. Know responde que é necessário pagar para se obter a resposta. Aqui, temos uma intervenção profética de Gigolo Joe: "nos tempos em que vivemos, David, nada custa mais do que a informação".[4]

É interessante que, antes da disseminação das redes sociais, do chamado capitalismo de vigilância e da preocupação com a proteção de

2 Disponível em: https://www.imdb.com/title/tt0212720/releaseinfo/?ref_=tt_dt_rdat. Acesso em: 02 mar. 23.

3 A cena pode ser vista em: https://www.youtube.com/watch?v=xoQkgAuE-Pbk&ab_channel=DanJeremyBrooks Acesso em: 02 mar.23.

4 Tradução do original realizada pelos autores.

dados pessoais, o roteiro de Inteligência Artificial tenha apontado para a direção certa de algo que seria um consenso incontestável menos de duas décadas depois: nada custa (no sentido de atribuição de valor) mais do que a informação. Faltou apenas dizer que esse pagamento seria cobrado em dados pessoais coletados, não em moeda corrente.

A segunda razão, retrospectiva, é de ordem pessoal. Eu vi o filme "Inteligência Artificial" em um cinema do Rio de Janeiro, no final de 2001, quando estava com 27 anos. Diante da promessa do Dr. Know ("perguntem ao Dr. Know, não há nada que eu não saiba"), lembro de pensar enquanto assistia ao filme: "seria tão bom se houvesse de fato algo assim no mundo – alguém, algo, a quem pudéssemos recorrer para perguntar o que quiséssemos". Isso, claro, sem poder prever que um dia estaria escrevendo sobre isso.

Olhando para trás, pode parecer estranho ter vivido em um mundo sem o Google, mas a verdade é que o Google começou a operar em 1998 e, em 2001, ainda estava longe de ser o motor de busca dominante para os usuários da internet, por conta da precisão de seus resultados.[5] Naquele momento, não era óbvio que em tão pouco tempo teríamos à nossa disposição um verdadeiro Dr. Know (exceto pelo holograma, felizmente), que poderíamos consultar para fazer todo tipo de pergunta. Na verdade, o conceito em si de inteligência artificial parecia um tanto difuso e futurístico – o que incluía ferramentas de busca e hologramas como prognósticos para o século XXII.

Desde o lançamento do filme, as aplicações de inteligência artificial se multiplicaram para muito além de uma simulação de diálogo (pergunta/resposta), embora seja um tópico particularmente atraente nos dias de hoje.

5 Há quem avalie que em março de 2002, o Google respondia por 16% do tráfego de buscas, atrás do Yahoo, com 36% à época. Disponível em https://www.manningmarketing.com/articles/top-search-engines-2002-2005/ . Acesso em: 02 mar. 23.

O uso da internet, difundido, democratizado e aperfeiçoado tecnicamente nas duas últimas décadas, é o exemplo mais eloquente de uso da inteligência artificial em nosso quotidiano. Podemos citar, dentre muitas outras funcionalidades, algoritmos de recomendação de conteúdo, tradutores de texto, aplicativos de rota de trânsito, análise de comportamento de consumidor, segurança digital, ferramentas de criação de conteúdo artístico e, naturalmente, aplicativos de reconhecimento facial.

A inteligência artificial não é mais um exercício de futurologia – embora também seja, pois está em franca construção. Ela se encontra presente no nosso dia a dia e, fruto de escolhas humanas, é uma promessa e uma ameaça. Tanto é capaz de prever doenças (BBC, 2021; HARVARD MEDICAL SCHOOL, 2022) como aprofundar desigualdades em grupos já marginalizados (ACLU, 2021). O conhecido experimento com a Tay, inteligência artificial da Microsoft, em 2016, teve consequências bastante desanimadoras. Em apenas 24 horas de interação com o Twitter, "os usuários da rede social a corromperam. Em um dia, ela passou de uma inocente robozinha para uma racista, transfóbica e desagradável vomitadora de caracteres" (TECMUNDO, 2016).

Segundo Byung-Chul Han (2022, p. 71-77), "[o] afetivo é essencial para o pensamento humano. A primeira imagem mental é o arrepio da pele. A inteligência artificial não pode pensar porque não se arrepia". E acrescenta: "[e]m sua comoção inicial, o pensamento está, por assim dizer, fora de si. A tonalidade afetiva fundamental o desloca em um fora. A inteligência artificial não pensa porque ela nunca está fora de si. Espírito significa originalmente ser-fora-de-si ou comoção. A inteligência artificial pode até calcular muito rapidamente, mas a ela falta o espírito. Para ela, calcular a comoção seria apenas um incômodo" (HAN, 2022, p. 74). Enfim, "[a] inteligência artificial é apática, quer dizer, sem páthos, sem paixão. Ela calcula" (HAN, 2022, p. 74).

Desse cálculo, contudo, advêm consequências reais. O uso de inteligência artificial em nosso cotidiano é irreversível e certamente crescente. Contudo, falta à inteligência artificial "a negatividade da ruptura, que

deixa surgir o novo no sentido enfático" (HAN, 2022, p. 81). Sendo assim, "[n]o fim das contas, tudo continua no mesmo".

Esse é o problema. Se as aplicações de inteligência artificial reproduzirem tal qual o mundo físico onde vivemos, vamos também reproduzir toda a forma de machismo, racismo, homofobia, transfobia, xenofobia, desigualdade e discriminação, dos mais variados tipos, contra os quais ainda temos que lutar. Por isso, o debate sobre o desenvolvimento e a regulação de novas tecnologias é indispensável no presente, quando ainda há tempo de moldar um mundo melhor, o mundo onde pretendemos viver nas próximas décadas.

Por conta da evolução da inteligência artificial, a União Europeia decidiu legislar sobre o tema. No momento, o que se tem é uma proposta abrangente, que propõe uma disciplina a partir da segmentação de riscos que determinada tecnologia pode representar. Trata-se claramente de uma estratégia europeia de liderar o debate público global. Neste breve estudo, vamos nos ater ao tema do reconhecimento facial e como a União Europeia pode contribuir para o debate do assunto no Brasil.

A Proposta de Regulação de Inteligência Artificial na Europa

Em abril de 2021, a União Europeia publicou sua proposta de regulamento para estabelecer normas de regulação para a inteligência artificial (COMISSÃO EUROPEIA, 2021a; COMISSÃO EUROPEIA, 2021b; COMISSÃO EUROPEIA, 2021c; COMISSÃO EUROPEIA, 2022) ("Proposta Europeia"). O documento é bastante extenso, de modo que vamos abordar aqui apenas os pontos diretamente relacionados ao tema em análise.

A exposição de motivos da Proposta Europeia apresenta os eixos estruturantes do documento:

> A proposta estabelece regras harmonizadas para o desenvolvimento, a colocação no mercado e a utilização de sistemas de IA na União na sequên-

> cia de uma abordagem proporcionada baseada no risco. **Propõe-se uma definição inequívoca e preparada para o futuro de "inteligência artificial"**. **Algumas práticas de IA particularmente prejudiciais são proibidas**, uma vez que violam os valores da União, e são propostas restrições e salvaguardas específicas relativamente a determinadas utilizações de sistemas de identificação biométrica à distância para efeitos de manutenção da ordem pública. A proposta estabelece uma metodologia de análise de riscos sólida para definir sistemas de IA de **"risco elevado"** que criam riscos significativos para a saúde e a segurança ou para os direitos fundamentais das pessoas. Esses sistemas de IA terão de cumprir um conjunto de requisitos obrigatórios horizontais para uma IA de confiança e seguir procedimentos de avaliação da conformidade antes de poderem ser colocados no mercado da União. Os fornecedores e os utilizadores desses sistemas também estão sujeitos a obrigações previsíveis, proporcionadas e claras para garantir a segurança e o respeito da legislação em vigor que protege os direitos fundamentais ao longo de todo o ciclo de vida dos sistemas de IA. **No caso de alguns sistemas de IA específicos, apenas são propostas obrigações de transparência mínimas**, em particular quando são utilizados sistemas de conversação automática ou "falsificações profundas" (Grifos nossos).

Ou seja, conforme se depreende da leitura do texto acima, a Proposta Europeia foi elaborada levando-se em consideração o grau de risco de determinada tecnologia de inteligência artificial, conforme definição constante do próprio texto.

Nesse sentido, a definição de sistema de inteligência artificial proposta é a de "programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage", nos termos do art. 3º, (1).

O reconhecimento facial é "um método de identificação ou verificação da identidade de uma pessoa a partir da imagem do seu rosto. No contexto atual, as tecnologias de reconhecimento facial (TRF) correspondem a softwares, programas de computador, que empregam diferentes técnicas de inteligência artificial para reconhecer ou identificar rostos humanos a partir de uma imagem, geralmente obtida a partir de fotos ou vídeos" (OLIVEIRA, 2021, p. 43).

Como é fácil imaginar, as tecnologias de reconhecimento facial parecem promissoras como meio de garantir a segurança pública. Afinal, a disseminação de câmeras em ambientes urbanos, conectadas a centros de inteligência que funcionam a partir de coleta incessante de dados, faz crer que teremos como resultado a diminuição de crimes (ver capítulos 1 e 2). Se todos são vigiados, então todos se comportam melhor. O problema é que não apenas essa correlação mostra-se falaciosa como também os efeitos colaterais do reconhecimento facial podem ser bastante graves, acirrando preconceitos, assimetrias e discriminações ilícitas ou abusivas.[6] Dentre eles, podemos citar a falta de precisão tecnológica, enviesamento (machismo algorítmico e racismo algorítmico) e ameaça à privacidade e demais direitos fundamentais, sendo uma ferramenta eficiente para opressão (OLIVEIRA, 2021, pp. 130-131).

Tais motivos levaram ao banimento do uso da tecnologia de reconhecimento facial em algumas cidades estadunidenses (BAN FACIAL RECOGNITION, 2023) e em alguns países.[7]

Nos termos da Proposta Europeia, em sua versão original, as tecnologias de reconhecimento facial se encontravam fortemente reguladas. Inseridas na categoria de "práticas proibidas", seriam toleradas apenas

6 Remetemos o/a leitor/a aos Capítulos 1, 2 e 5, além da obra de OLIVEIRA, 2021.

7 Na Bélgica, há quem defenda que mesmo um teste com a tecnologia pode ser considerado ilegal. Disponível em https://www.rtl.be/actu/belgique/societe/histoire-belge-les-cameras-intelligentes-qui-vont-sanctionner-le-gsm-au-volant/2022-11-05/article/499617#:~:text=%22La%20biom%C3%A9trie%20et%20la%20reconnaissance,%2C%20insiste%2Dt%2Dil. Acesso em: 02 mar. 23.

em situações muito excepcionais, conforme art. 5º, (1) (d), da Proposta Europeia:

> Art. 5
> 1) Estão proibidas as seguintes práticas de inteligência artificial: (...) **d) A utilização de sistemas de identificação biométrica à distância em «tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, salvo se essa utilização for estritamente necessária para alcançar um dos seguintes objetivos: i) a investigação seletiva de potenciais vítimas específicas de crimes, nomeadamente crianças desaparecidas; ii) a prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de um ataque terrorista; iii) a deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal referida no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho 62 e punível no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro.** (Grifo nosso).

Os limites do uso de tecnologia de reconhecimento facial seriam, então, detalhados nos itens seguintes (2), (3) e (4):

> 2) A utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d), deve ter em conta os seguintes elementos: a) A natureza da situação que origina a possível utilização, em especial a gravidade, a probabilidade e a magnitude dos prejuízos causados na ausência da utilização do sistema; b) As consequências da utilização do sistema para os direitos e as liberdades de todas as pessoas afetadas, em especial a gravidade, a probabilidade e a magnitude dessas consequências. Além disso, a utilização

de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d), deve observar salvaguardas e condições necessárias e proporcionadas em relação a tal utilização, nomeadamente no respeitante a limitações temporais, geográficas e das pessoas visadas. **3)** No tocante ao n.º 1, alínea d), e ao n.º 2, cada utilização específica de um sistema de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública está sujeita a autorização prévia concedida por uma autoridade judiciária ou por uma autoridade administrativa independente do Estado-Membro no qual a utilização terá lugar após apresentação de um pedido fundamentado em conformidade com as regras de execução previstas no direito nacional a que se refere o n.º 4. Contudo, numa situação de urgência devidamente justificada, a utilização do sistema pode ser iniciada sem uma autorização e esta pode ser solicitada apenas durante ou após a utilização. A autoridade judiciária ou administrativa competente apenas deve conceder a autorização se considerar, com base em dados objetivos ou indícios claros que lhe tenham sido apresentados, que a utilização do sistema de identificação biométrica à distância «em tempo real» em apreço é necessária e proporcionada para alcançar um dos objetivos especificados no n.º 1, alínea d), conforme identificado no pedido. Ao decidir sobre o pedido, a autoridade judiciária ou administrativa competente tem em conta os elementos referidos no n.º 2. **4)** Um Estado-Membro pode decidir prever a possibilidade de autorizar total ou parcialmente a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública dentro dos limites e sob as condições enumeradas no n.º 1, alínea d), e nos n‍ºs 2 e 3. Esse Estado-Membro estabelece na sua legislação nacional as regras pormenorizadas aplicáveis ao pedido, à emissão e ao exercício das autorizações a que se refere o n.º 3, bem como à supervisão das mesmas. Essas regras especificam igualmente em relação a que objetivos enumerados no n.º 1, alínea d), incluindo quais

> das infrações penais referidas na subalínea iii) da mesma, as autoridades competentes podem ser autorizadas a usar esses sistemas para efeitos de manutenção da ordem pública.

De acordo com o texto acima exposto, a tendência parecia ser o uso excepcional da tecnologia de reconhecimento facial na União Europeia (CARTA CAPITAL, 2021; TECHCRUNCH, 2021), como, por exemplo, para a investigação seletiva de potenciais vítimas específicas de crimes, nomeadamente crianças desaparecidas, ou a prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de um ataque terrorista (Artigo 5º, 1, d), desde que observadas as condições presentes nos itens 2, 3 e 4 do mesmo artigo.

Contudo, em 14 de junho de 2023, o Parlamento Europeu aprovou mudanças no texto da Proposta Europeia, tornando mais severas as regras relativas à adoção do reconhecimento facial. O banimento da tecnologia se tornou mais explícito e foram excluídas as hipóteses de exceção, como se pode ver abaixo (COMISSÃO EUROPEIA, 2023):

> Art. 5
> Estão proibidas as seguintes práticas de inteligência artificial: (...) **d) A utilização de sistemas de identificação biométrica à distância em «tempo real» em espaços acessíveis ao público** (grifo nosso).

Como se percebe, neste caso a proibição parece ser incondicional. Além disso, foram incluídas outras hipóteses de proibição expressa (COMISSÃO EUROPEIA, 2023), identificadas nos itens (da) (db) (dc) e (dd) relacionadas, respectivamente, (i) à análise preditiva de risco de uma pessoa cometer um crime; (ii) à criação ou expansão de bases de dados de reconhecimento facial a partir da coleta de imagens da internet ou de circuitos fechados; (iii) a sistemas de IA para inferir emoções de pessoa física para efeitos de manutenção de ordem pública, para controle de

fronteiras, em local de trabalho e instituições de ensino e, finalmente, (v) a sistemas de IA para a análise de registros de filmagem de espaços acessíveis ao público exceto em determinados casos em que haja autorização judicial e desde que estritamente necessário para a pesquisa direcionada ligado a um crime grave específico definido no TFUE (Tratado de Funcionamento da União Europeia).[8]

Consequentemente, foram excluídas as seções (2), (3) e (4), onde se detalhavam os limites aceitáveis para a utilização de tecnologias de reconhecimento facial.

O texto final ainda não foi aprovado, mas com as decisões tomadas em junho de 2023, o reconhecimento facial na Europa como medida de segurança pública tende a se tornar uma atividade extremamente limitada.

8 Versão original das alterações prevê que: *(d a) the placing on the market, putting into service or use of an AI system for making risk assessments of natural persons or groups thereof in order to assess the risk of a natural person for offending or reoffending or for predicting the occurrence or reoccurrence of an actual or potential criminal or administrative offence based on profiling of a natural person or on assessing personality traits and characteristics,including the person's location, or past criminal behaviour of natural persons or groups of natural persons; (d b) The placing on the market, putting into service or use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage; dc) the placing on the market, putting into service or use of AI systems to infer emotions of a natural person in the areas of law enforcement, border management, in workplace and education institutions. (d d) the putting into service or use of AI systems for the analysis of recorded footage of publicly accessible spaces through 'post' remote biometric identification systems, unless they are subject to a pre-judicial authorisation in accordance with Union law and strictly necessary for the targeted search connected to a specific serious criminal offense as defined in Article 83(1) of TFEU that already took place for the purpose of law enforcement.* (COMISSÃO EUROPEIA, 2023)

O Enquadramento Regulatório Brasileiro – Em Construção[9]

Em 2021, foi publicada no Brasil a Estratégia Brasileira de Inteligência Artificial (Ebia). Entretanto, ao contrário do que ocorreu em países como Canadá, Estados Unidos, Portugal, Espanha, França, Alemanha, Austrália e Japão, bem como em alguns países em desenvolvimento, como México e Índia, por exemplo, a estratégia mostrou-se pouco robusta e não avançou em questões relevantes como riscos atrelados ao desenvolvimento de IAs, ética, transparência, possibilidades de aplicação industrial, pesquisa e futuro do trabalho.[10]

Segundo seus autores, o Ebia "assume o papel de nortear as ações do Estado brasileiro em prol do desenvolvimento das ações, em suas várias vertentes, que estimulem a pesquisa, inovação e desenvolvimento de soluções em Inteligência Artificial, bem como, seu uso consciente, ético e em prol de um futuro melhor" (MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, 2021).

O documento está dividido em 9 eixos temáticos: (i) legislação, regulação e uso ético; (ii) governança de inteligência artificial; (iii) aspectos internacionais; (iv) qualificações para um futuro digital; (v) força de trabalho e capacitação; (vi) pesquisa, desenvolvimento, inovação e empreendedorismo; (vii) aplicação nos setores produtivos; (viii) aplicação no poder público e (ix) segurança pública (MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, 2021).

9 Esta seção contém trechos traduzidos do original "*AI Regulation in Brazil: Detailing the current legislative proposal*" (BRANCO; SOUZA, 2023).

10 Estudo que compara a estratégia de inteligência artificial de Argentina, Brasil, Chile, Colômbia e Coreia do Sul: https://www.ipea.gov.br/portal/categorias/45-todas-as-noticias/noticias/13389-estudo-compara-estrategias-de-inteligencia-artificial-em-cinco-paises. Acesso em: 02 mar. 23.

O Ebia apresenta recomendações que se encontram alinhadas com a experiência internacional e com o PL 21/20,[11] que estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil, tais como:

> A IA deve beneficiar as pessoas e o planeta, impulsionando o crescimento inclusivo, o desenvolvimento sustentável e o bem-estar. Os sistemas de IA devem ser projetados de maneira a respeitar o Estado de Direito, os direitos humanos, os valores democráticos e a diversidade, e devem incluir salvaguardas apropriadas – possibilitando a intervenção humana sempre que necessário – para garantir uma sociedade justa. Organizações e indivíduos que desempenham um papel ativo no ciclo de vida de IA devem se comprometer com a transparência e com a divulgação responsável em relação a sistemas de IA, fornecendo informações relevantes e condizentes com o estado da arte que permitam: (i) promover a compreensão geral sobre sistemas de IA; (ii) tornar as pessoas cientes quanto às suas interações com sistemas de IA; (ii) permitir que aqueles afetados por um sistema de IA compreendam os resultados produzidos; e (iv) permitir que aqueles adversamente afetados por um sistema de IA possam contestar seu resultado. Os sistemas de IA devem funcionar de maneira robusta, segura e protegida ao longo de seus ciclos de vida. Os riscos em potencial devem ser avaliados e gerenciados continuamente (MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, 2021, p. 7).

11 Após sua aprovação pela Câmara dos Deputados em 29 de setembro de 2021, o texto foi encaminhado ao Senado para posterior discussão e votação. Até o momento, não há prazo definido para que o Senado vote o projeto de lei. Ainda que o referido PL 21/2020 ofereça uma abordagem mais baseada em princípios para o desenvolvimento e operação de sistemas de inteligência artificial, alguns elementos já fornecem um vislumbre de como a legislação futura pode abordar temas delicados, como soberania nacional de dados, requisitos de transparência e a responsabilidade pelo uso das tecnologias. Sob o guarda-chuva de itens muito genéricos já existe um conjunto relevante de dispositivos que poderiam ser aplicados imediatamente pelos Tribunais – se o PL 21/20 for aprovado.

Embora o documento traga, ao final de cada um de seus eixos temáticos, ações estratégicas a serem adotadas, seu grau de concretude é baixo. É mais um rol de intenções, sem prazo, delegação de tarefas ou identificação dos responsáveis que podem efetivamente conduzir à sua concretização. O documento é importante do ponto de vista ideológico, mas traz poucos elementos concretos para a regulamentação da inteligência artificial no Brasil.

No entanto, o uso da IA não é novidade para o governo brasileiro, principalmente quando levamos em consideração o Poder Judiciário. Desde 2017, o Supremo Tribunal Federal (STF) vem usando uma ferramenta de inteligência artificial chamada Victor. Fruto de parceria entre o STF e a Universidade de Brasília (UnB), "o Victor foi idealizado para auxiliar o STF na análise dos recursos extraordinários recebidos de todo o país, especialmente quanto a sua classificação em temas de repercussão geral de maior incidência" (SUPREMO TRIBUNAL FEDERAL, 2021). A experiência estimulou outros tribunais a desenvolverem seus próprios recursos de inteligência artificial, como o Sócrates no Superior Tribunal de Justiça (STJ) e o Hércules no Tribunal de Justiça de Alagoas, entre muitos outros. No âmbito do executivo e da administração pública, o uso e o investimento em sistemas dotados de IA vêm se mostrando crescentes mais recentemente (TRIBUNAL DE CONTAS DA UNIÃO, 2022; ENAP, 2022).

Apesar desses exemplos isolados, a falta de uma política pública unificada para a regulamentação da inteligência artificial gera incertezas e impede a obtenção de melhores resultados tanto na esfera pública quanto na privada. Por exemplo, uma pesquisa promovida pelo Conselho Nacional de Justiça (CNJ), em parceria com o Instituto de Tecnologia e Sociedade (ITS), apontou, entre outras coisas, que:

> (i) Inexiste uma política diretiva clara para o uso de IA no sistema judiciário, nem, tampouco, uma política com um conjunto de princípios e comandos claros a assegurar o uso seguro e ético da IA. (ii) Os tribunais

> não estão se comunicando com o CNJ ou outros tribunais a respeito do desenvolvimento de suas próprias ferramentas. Existem evidências de colaboração entre alguns tribunais, porém esse processo ainda é incipiente. (...) (v) Ainda há de ser implementado um mecanismo de monitoramento e avaliação que assegure que a IA seja utilizada eticamente dentro do Poder Judiciário (ITS, 2020, p. 8).

Após diversas críticas relacionadas à superficialidade tanto do Ebia quanto do PL 21/20 (CONJUR, 2021), o Senado Federal apresentou, em dezembro de 2022, relatório de comissão de juristas para subsidiar elaboração de substitutivo sobre inteligência artificial no Brasil (SENADO FEDERAL, 2022). Com mais de 900 páginas, o documento foi elaborado a partir de contribuições em audiências públicas, seminários internacionais, contribuições escritas, análise de autoridades regulatórias em países da OCDE.

Com texto mais robusto do que o PL (45 artigos, diante dos escassos 10 artigos do PL atual) e semelhantemente à Proposta Europeia, a minuta de substitutivo qualifica os riscos decorrentes de uso de ferramentas de inteligência artificial em (i) risco excessivo e (ii) alto risco.

Dentro da seção relativa ao risco excessivo, foram vedadas a implementação e o uso dos seguintes sistemas de inteligência artificial:

> I – que empreguem técnicas subliminares que tenham por objetivo ou por efeito induzir a pessoa natural a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança ou contra os fundamentos deste lei;
> II – que explorem quaisquer vulnerabilidades de grupos específicos de pessoas naturais, tais como associadas à sua idade ou deficiência física ou mental, de modo a induzi-las a se comportar de forma prejudicial à sua saúde ou segurança ou contra os fundamentos desta lei;
> III – pelo poder público, para avaliar, classificar ou ranquear as pessoas naturais, com base no seu comportamento social ou em atributos da sua

> personalidade, por meio de pontuação universal, para o acesso a bens e serviços e políticas públicas, de forma ilegítima ou desproporcional.

Contudo, a tecnologia de reconhecimento facial contaria com regulação própria. O tema é inserido na seção do risco excessivo, porém com nuances de exceção. O texto abaixo, constante originalmente do relatório de comissão de juristas acima referido, passou a integrar, com a mesma redação, o PL2.338/2023, recentemente apresentado pelo Senador Rodrigo Pacheco, para regular o uso de inteligência artificial no Brasil:

> Art. 15. No âmbito de atividades de segurança pública, somente é permitido o uso de sistemas de identificação biométrica à distância de forma contínua em espaços acessíveis ao público, quando houver previsão em lei federal específica e autorização judicial em conexão com a atividade de persecução penal individualizada, nos seguintes casos: I – persecução de crimes passíveis de pena máxima de reclusão superior a dois anos; II – busca de vítimas de crimes ou pessoas desaparecidas; III – crime em flagrante. Parágrafo único. A lei a que se refere o caput preverá medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal e o controle judicial, bem como os princípios e direitos previstos nesta Lei, especialmente a garantia contra a discriminação e a necessidade de revisão da inferência algorítmica pelo agente público responsável antes da tomada de qualquer ação em face da pessoa identificada.

É importante observarmos que no âmbito da segurança pública e, consequentemente, no uso de reconhecimento facial por agentes de segurança, há que se levar em conta a discriminação algorítmica e seus resultados, como o reforço a atos de todo tipo de perseguição e prejuízo a extratos sociais historicamente marginalizados e silenciados.

Como alerta Samuel Oliveira (OLIVEIRA, 2021, p. 131), o "uso da câmera de segurança e, recentemente, da tecnologia de reconhecimento facial, não impede a ocorrência de crimes. O que frequentemente acontece é que a presença de aparatos de vigilância faz com que os crimes simplesmente ocorram em outros lugares, menos vigiados". Além disso, "o videomonitoramento não impede a ocorrência de crimes violentos, provavelmente porque esses crimes geralmente são espontâneos, não premeditados. Além de sistema de vigilância não necessariamente aumentarem a segurança, eles podem tornar as pessoas menos seguras se virem câmeras e erroneamente presumirem que alguém está assistindo e que prontamente irá socorrê-las se necessário, uma vez que a maioria das câmeras não é monitorada em tempo real. Assim, apesar de câmeras de segurança possivelmente reduzirem a ocorrência de crimes de menor potencial lesivo, como furtos e roubos, não são efetivas na maioria das situações".

Sendo assim, não podemos correr o risco de instituir políticas públicas que, a pretexto de aumentar a segurança dos indivíduos, tenha como resultado, na verdade, práticas discriminatórias e ineficientes (conforme já tratado nos Capítulos 1 e 2).

O PL 2.338/2023 repete, com ajustes de redação, o texto sugerido no relatório apresentado pelo Senado Federal após contribuição da comissão de juristas. O resultado é uma aproximação maior à Proposta Europeia, com a classificação dos sistemas de inteligência artificial em graus de risco, o que facilitaria a tomada de decisão na forma de regular cada um deles. Ainda assim, conforme visto acima, a União Europeia tornou, em junho de 2023, ainda mais restritiva a aplicação de reconhecimento facial em razão dos graves riscos que pode apresentar à tutela de interesses individuais e coletivos. No mesmo sentido, seria recomendável o Brasil adotar um debate profundo e crítico para seguir o caminho mais favorável à tutela de tais direitos.

Lei Geral de Proteção de Dados

Em 2018, foi aprovada a Lei Federal 13.709, conhecida como "Lei Geral de Proteção de Dados" (doravante, "LGPD"). O tema da proteção de dados adquiriu, nas duas últimas décadas, cada vez maior relevância no ambiente digital. Embora a matéria já fosse tratada na Lei 12.965/14 ("Marco Civil da Internet", ou "MCI"), somente com a edição da LGPD o assunto recebeu a profundidade necessária para sua disciplina.

Fortemente inspirada pelo regulamento europeu de proteção de dados (*General Data Protection Regulation* – GDPR),[12] a LGPD abrange, por exemplo, os requisitos para a proteção de dados pessoais; como o tratamento de dados pessoais pode se dar; regras para o tratamento de dados de crianças e de adolescentes; direitos dos titulares de dados; tratamento de dados pelo poder público; transferência internacional de dados; agentes de tratamentos; segurança de dados e boas práticas; fiscalização e criação da Autoridade Nacional de Proteção de Dados (ANPD).

Dentre os temas acima elencados, o que mais nos interessa no âmbito deste estudo são os dados pessoais sensíveis. Mas comecemos pela ideia, central para a LGPD, de conceito de dado pessoal.

Em seu art. 5º, I, a LGPD determina que dado pessoal é "informação relacionada a pessoa natural identificada ou identificável". Afinal, a lei se aplica apenas a dados de pessoas físicas, excluídas, portanto, as pessoas jurídicas.

A seguir, no inciso II, apresenta espécies de dados pessoais sensíveis como sendo "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

12 Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 02 mar. 23.

O tratamento de dados pessoais sensíveis apresenta hipóteses legais específicas dentro da lei, conforme previsto em seu artigo 11.

Os dados pessoais sensíveis têm tratamento diferenciado em nossa legislação em razão do potencial lesivo em seu tratamento inadequado. Assim, dados pessoais sensíveis podem ser entendidos como aqueles que "compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação" (BIONI, 2019, p. 85).

Por isso, "mais importante do que identificar a natureza própria ou conteúdo do dado – conforme o rol do artigo 5º, II, da LGPD – é constatar a potencialidade discriminatória no tratamento de dados pessoais. Isto é, a limitação para o tratamento de dados se concretizaria na proibição de seu uso de maneira a gerar uma discriminação, um uso abusivo e não igualitário de dados" (MULHOLLAND, 2020, p. 122).

Embora a LGPD não defina o que são dados biométricos, o Decreto n. 10.046/19[13] qualifica "atributos biométricos" como sendo "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar" (TEFFÉ, 2022, pp. 108-109).[14]

13 "Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados", Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 02 mar. 23.

14 Sabe-se que a "biometria é a ciência de se estabelecer a identidade de alguém, a partir da medição e análise de seus atributos fisiológicos ou comportamentais mensuráveis. No primeiro caso, são exemplos a impressão digital, o reconhecimento da íris, a identificação por retina, a definição dos traços do rosto, a arcada dentária, a geometria da mão e a altura da pessoa. As medidas fisiológicas geralmente oferecem o benefício de permanecer mais estáveis ao longo da vida de um indivíduo. No segundo caso, é possível mencionar: a forma como a pessoa digita, como anda, gestos característicos, dinâmica da assinatura (velocidade do movimento da caneta, acelerações, pressão exercida e inclinação), a altura que o indivíduo costuma segurar o celular, a forma com que ele movimenta o mouse do

Quanto ao uso de dados biométricos, Chiara de Teffé (2022, pp. 110-111) esclarece:

> Vistas comumente como um meio de identificação e autenticação, as informações biométricas vêm sendo tratadas para variados fins e contextos: de sistemas de reconhecimento facial e de voz, para permitir que funcionários acessem ambientes específicos ou encontrar pessoas procuradas pela polícia, a impressões digitais para liberar o acesso ao almoço de uma escola primária. À medida que a tecnologia avança, o uso de características humanas como informação continuará a representar desafios para as noções de privacidade e de proteção de dados pessoais. A confiabilidade das informações e sistemas biométricos vem sendo incrementada, sendo a biometria geralmente considerada forte e valiosa para fins de autenticação. Inclusive, sistemas de identificação multibiométrica vêm sendo amplamente adotados. Contudo, entender formas de melhor proteger tais dados e evitar tratamentos desproporcionais ou ilícitos ainda são desafios que precisam ser mais bem trabalhados.

De fato, no estágio atual das tecnologias de reconhecimento facial, quando em confronto com o quadro legislativo brasileiro sobre o assunto, é bastante temerária a adoção indiscriminada de tecnologia de reconhecimento facial com o argumento, por exemplo, de incrementar a segurança pública – ainda que a LGPD expressamente informe que ela não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública (art. 4º, III, a).

O que ocorre é que não apenas os erros no processo de reconhecimento se sucedem (reforçando preconceitos históricos), como a LGPD, ao considerar dados biométricos como dados sensíveis, de fato cria

computador, a pressão que ele exerce no teclado ou na tela e, até mesmo, como corrige as palavras (TEFFÉ, 2022, p. 108)".

uma camada de proteção à adoção da tecnologia sem maiores cuidados (VICENTE, 2019; BOMFIM & RIOS, 2022; SCHENDES, 2023; GUIMARÃES, 2021).

Prova disso foi a polêmica envolvendo o metrô da cidade de São Paulo, cujo projeto de implementação de câmeras para reconhecimento facial foi interrompido em março de 2022 por decisão do Tribunal de Justiça do Estado, retomado alguns meses depois (G1, 2022) e mais uma vez suspenso (LACERDA, 2023).

Conclusões

A inteligência artificial é uma realidade múltipla. Ela se insere em nosso quotidiano em atividades aparentemente inofensivas (como algoritmos de recomendação de livros com base em seu histórico de compra ou tradução automática de texto) e em outras cujo risco elevado de uso de inteligência artificial se evidencia (como é o caso do uso de ferramentas de reconhecimento facial). A variedade de usos e de riscos a ela associados torna a regulação de algo tão fluido e sujeito ao célere avanço tecnológico algo particularmente complexo.

A União Europeia saiu na frente com uma proposta de regulação que promete influenciar a tomada de decisões em outros territórios – como ocorreu com o GDPR na construção da lei brasileira de proteção de dados.

Assim como tem sido tendência nas últimas décadas, a regulação proposta pela União Europeia parte de princípios e de classificações que, assim se espera, possam permitir que a lei se adapte às necessidades da passagem dos anos.

Dessa forma, os sistemas de inteligência artificial seriam qualificados em razão do risco decorrente de sua adoção: se excessivo, se alto ou se aceitável. O reconhecimento facial, por exemplo, se enquadraria na categoria de risco excessivo, e, portanto, proibida.

Assim como a União Europeia, o Brasil ainda está na fase de construir propostas de regulação de ferramentas de inteligência artificial. Como

seus principais instrumentos (o Ebia e o PL 21/20) carecem de maior concretude, a comissão constituída pelo Senado Federal apresentou, no final de 2022, proposta de substitutivo do PL. Mais recentemente, foi apresentado o PL 2.338/2023, com origem no Senado Federal, tendo por objetivo tratar da inteligência artificial de modo mais amplo e concreto.

Em conexão com o texto que vem sendo debatido na União Europeia, também no Brasil as ferramentas de inteligência artificial seriam classificadas a partir do risco de sua adoção, situando-se o reconhecimento facial no risco mais elevado.

De fato, são muitos os direitos que se encontram potencialmente ameaçados pelo uso público e indiscriminado da tecnologia de reconhecimento facial. Isso sem contar com a alta taxa de falsos positivos que têm levado à prisão de inocentes e a perpetuação de discriminações sociais e raciais sistêmicas.

Ainda que o desafio de regular o desenvolvimento e a implementação de ferramentas de inteligência artificial esteja muito longe de ser simples, ele se tornou inadiável. Quer na Europa, quer no Brasil, precisamos definir com muita clareza quais limites pretendemos impor a tecnologias de reconhecimento facial, de modo a impedir que direitos individuais e coletivos sigam sendo violados.

Referências

ACLU. "How Artificial Intelligence Can Deepen Racial and Economic Inequities". *Aclu.org*, 13 de julho de 2021. Disponível em: https://www.aclu.org/news/privacy-technology/how-artificial-intelligence-can-deepen-racial-and-economic-inequities (acesso em 02 de março de 2023)

BAN FACIAL RECOGNITION. **Ban Facial Recognition. The Interactive Map**. 2023. Disponível em: https://www.banfacialrecognition.com/map/ (acesso em 02 de março de 2023)

BBC. "Artificial Intelligence may diagnose dementia in a day". *BBC.com*, 10 de agosto de 2021. Disponível em: https://www.bbc.com/news/health-57934589 (acesso em 02 de março de 2023)

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2019.

BRANCO, Sérgio; CANO, Flávia Parra e SOUZA, Carlos Affonso. *La Réglementation de l'Intelligence Artificielle au Brésil: la Décortication des Proposition Législatives Actuelles*. *In*: CASTETS-RENARD, Céline e EYNARD, Jessica (orgs.). **Un Droit de l'Intelligence Artificielle – Entre Règles Sectorielles et Régime Général – Perpesctives Comparées**. Bruxelas: Bruylant, 2023.

CARTA CAPITAL. "Europa avança para o banimento do reconhecimento facial". *cartacapital.com.br*, 29 de junho de 2021. Disponível em: https://www.cartacapital.com.br/blogs/intervozes/europa-avanca-para-o-banimento-do-reconhecimento-facial/ (acesso em 02 de março de 2023)

COMISSÃO EUROPEIA. **Regulamento do Parlamento Europeu e do Conselho que Estabelece Regras Harmonizadas em Matéria de Inteligência Artificial**. 2021a. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN (acesso em 02 de março de 2023)

COMISSÃO EUROPEIA. **Coordinated Plan on Artificial Intelligence**. 2021b. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/plan=-ai#:~:text=The%20key%20aims%20of%20the,AI%20policy%20to%20avoid%20fragmentation.&text=The%20Coordinated%20Plan%20on%20Artificial%20Intelligence%202021%20Review%20is%20the,global%20leadership%20in%20trustworthy%20AI (acesso em 06 de março de 2023)

COMISSÃO EUROPEIA. **A European Approach to artificial intelligence**. 2021c. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (acesso em 06 de março de 2023)

COMISSÃO EUROPEIA. **Liability Rules for Artificial Intelligence**. 2022. Disponível em: https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en (acesso em 06 de março de 2023)

COMISSÃO EUROPEIA. **Artificial Intelligence Act**. **Amendments adopted by the European Parliament on 14 June 2023. 2023. Disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf** (acesso em 19 de junho de 2023)

CONJUR. "Projeto de Marco Legal da IA ainda é superficial, apontam especialistas". 11 de outubro de 2021. Disponível em: https://www.conjur.com.br/2021-out-11/projeto-marco-legal-ia-ainda-superficial-apontam-especialistas (acesso em 02 de março de 2023)

ENAP. "Governo Federal investirá R$ 36 milhões em inteligência artificial aplicada a serviços públicos. 02 de agosto de 2022. Disponível em: https://www.enap.gov.br/pt/acontece/noticias/governo-federal-investira-r-36-milhoes-em-inteligencia-artificial-aplicada-a-servicos-publicos-2 (acesso em 06 de março de 2023)

LACERDA, Lucas. "Smart Sampa pode violar direitos de negros e LGBT+, aponta Tribunal de Contas". *folha.uol.com.br*, 13 de fevereiro de 2023. Disponível em: https://www1.folha.uol.com.br/cotidiano/2023/02/smart-sampa-pode-violar-direitos-de-negros-e-lgbt-aponta-tribunal-de-contas.shtml (acesso em 05 de março de 2023)

G1. "Metrô de SP inicia operação de sistema de reconhecimento facial; TJ chegou a impedir instalação". *g1.globo.com*, 21 de novembro de 2021. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2022/11/21/metro-de-sp-inicia-operacao-de-novo-sistema-de-monitoramento-eletronico-por-meio-de-reconhecimento-facial-tj-chegou-a-impedir-instalacao.ghtml (acesso em 02 de março de 2023)

HAN, Byung-Chul. **Não-Coisas – Reviravoltas do Mundo da Vida**. Petrópolis: Vozes, 2022.

HARVARD MEDICAL SCHOOL. "How AI Can Help Diagnose Rare Diseases". *Harvard.edu*, 18 de outubro de 2022. Disponível em: https://hms.harvard.edu/news/how-ai-can-help-diagnose-rare-diseases#:~:text=Known%20as%20SISH%20(self%2Dsupervised,to%20respond%20to%20similar%20therapies (acesso em 02 de março de 2023)

ITS. **O Futuro da IA no sistema judiciário brasileiro**. 2020. Disponível em: https://itsrio.org/wp-content/uploads/2020/07/TRADUC%CC%A7A%CC%83O-The-Future-of-AI-in-the-Brazilian-Judicial-System.pdf (acesso em 06 de março de 2023)

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO. **Estratégia Brasileira de Inteligência Artificial**. 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-diagramacao_4-979_2021.pdf (acesso em 02 de março de 2023)

MULHOLLAND, Caitlin. *O Tratamento de Dados Pessoais Sensíveis*. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o Novo Marco Normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

SCHENDES, William. "Erro de reconhecimento facial leva a prisão de homem negro". **Olhar Digital**, 10 de janeiro de 2023. Disponível em: https://olhardigital.com.br/2023/01/10/seguranca/erro-de-correspondencia-de-reconhecimento-facial-leva-a-prisao-de-homem-negro/ (acesso em 02 de março de 2023)

OLIVEIRA, Samuel R. de. **Sorria, Você está Sendo Filmado – Repensando Direitos na Era do Reconhecimento Facial**. São Paulo: Thomson Reuters Brasil, 2021.

GUIMARÃES, Hellen. "Nos erros de reconhecimento facial, um "caso isolado" atrás do outro". *piaui.folha.uol.com.br*, 24 de setembro de 2021. Disponível em: https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/ (acesso em 02 de março de 2023)

BOMFIM, Fabiano; **RIOS**, Alan. "Reconhecimento facial erra de novo e acusa inocente". *noticias.r7.com*, 14 de janeiro de 2022. Disponível em: https://noticias.r7.com/brasilia/reconhecimento-facial-erra-de-novo-e-acusa-inocente-21012022 (acesso em 02 de março de 2023)

SENADO FEDERAL. "Inteligência Artificial: comissão de juristas entrega relatório nesta terça". 05 de dezembro de 2022. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/12/05/inteligencia-artificial-comissao-de-juristas-entrega-relatorio-nesta-terca (acesso em 02 de março de 2023)

SUPREMO TRIBUNAL FEDERAL. "Projeto Victor avança em pesquisa e desenvolvimento para identificação dos temas de repercussão geral". 19 de agosto de 2021. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=471331&ori=1 (acesso em 02 de março de 2023)

TECHCRUNCH. "European Parliament backs ban on remote biometric surveillance". *techcrunch.com*, 06 de outubro de 2021. Disponível em: https://techcrunch.com/2021/10/06/european-parliament-backs-ban-on-remote-biometric-surveillance/ (acesso em 02 de março de 2023)

TECMUNDO. "Tay: Twitter conseguiu corromper a AI da Microsoft em menos de 24 horas". *Tecmundo.com.br*, 24 de março de 2016. Disponível em: https://www.tecmundo.com.br/inteligencia-artificial/102782-tay-twitter-conseguiu-corromper-ia-microsoft-24-horas.htm (acesso em 02 de março de 2023)

TEFFÉ, Chiara Spadaccini de. **Dados Pessoais Sensíveis – Qualificação, Tratamento e Boas Práticas**. Indaiatuba: ed. Foco, 2022.

TRIBUNAL DE CONTAS DA UNIÃO. "TCU avalia uso de inteligência artificial pelo governo federal". 1º de junho de 2022. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-avalia-uso-de-inteligencia-artificial-pelo-governo-federal.htm (acesso em 06 de março de 2023)

VICENTE, João. "Reconhecimento facial erra muito, e você deveria se preocupar com isso". *uol.com.br*, 27 de maio de 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/05/27/tecnicas-de-vigilancia-como-identificacao-facial-ainda-sao-falhas.htm (acesso em 02 de março de 2023).

Este livro tem como objetivo apresentar o panorama atual dos debates em torno do desenvolvimento, uso e regulação de sistemas de reconhecimento facial no Brasil. Para tanto, reúne capítulos de especialistas de diferentes áreas do conhecimento, de modo a cobrir as múltiplas práticas de gestão, governo e controle que foram impactadas pelas inovações recentes no campo da inteligência artificial aplicada às tecnologias de monitoramento biométrico. A proposta do livro não é trazer pesquisas empíricas inéditas, mas mapear, organizar e, fundamentalmente, pôr em diálogo abordagens sobre sistemas de reconhecimento facial que se encontram ainda compartimentalizadas nos campos do direito, da sociologia e dos estudos de ciência e tecnologia. Nesse sentido, o livro contribui com uma abordagem interdisciplinar sobre o tema, o que pode ser útil para profissionais da área de segurança pública, jornalistas, organizações da sociedade civil, estudantes e pesquisadores engajados nos temas do direito, tecnologia e sociedade.

KONRAD ADENAUER STIFTUNG

www.kas.de/brasil