

10, 11 e 12 de novembro de 2025

POLITÉCNICO DO PORTO / ISCAP
PORTO - PORTUGAL

A controvérsia da utilização de Tecnologias de Reconhecimento Facial no Brasil

Letícia Vitoria Rodrigues Lima de Souza, IBICT/UFRJ, 0009-0009-9821-2901, Brasil,
leticiavrlsouza@gmail.com

Juliana Campos de Aguiar Mattos Ribeiro, IBICT/UFRJ, 0000-0003-1103-4671, Brasil,
jcampos.juridico@gmail.com

Antonio Mario Banchik, IBICT/UFRJ, 0009-0006-2281-6790, Brasil,
ambanchik10@gmail.com

Eixo: Impactos Sociais

1 Introdução

Nas últimas décadas, os acelerados avanços nas Tecnologias de Informação e Comunicação (TICs) promoveram profundas mudanças em diversos aspectos da sociedade, tanto no ambiente individual e privado quanto na esfera pública, que afeta a vida urbana e a sociedade. Nesse sentido, as inovações presentes nas TICs se consolidaram, a partir da adoção de ferramentas automatizadas aplicadas em diversas áreas como educação, saúde, mobilidade urbana e — em especial no contexto deste trabalho — segurança pública. A incorporação e proliferação de tecnologias nos aparatos públicos brasileiros se desdobrou em alguns outros fenômenos, como a datificação de cidadãos, a plataformação de órgãos e instituições, preocupação com a soberania de dados e ampla utilização de tecnologias de vigilância, esta última tendo como ponto de partida os esforços em segurança em grandes eventos.

No trabalho de Van Dijck (2017), há uma discussão importante no que diz respeito ao processo de datificação da sociedade, em que o autor aponta como este fenômeno é um novo paradigma na sociedade, em que a ação social se transforma em dados quantificáveis em ambiente *online*. Como consequência,

percebe-se que, desse modo, tais dados podem ser utilizados para monitoramento realizado em tempo real e, também, análise preditiva (Van Dijck, 2017, p. 41). Essa conjuntura oferece um momento específico dentro da história que pode proporcionar novos modos de enxergar e experienciar o mundo.

Como exemplo representativo disso, abordamos as Tecnologias de Reconhecimento Facial (TRFs), sistemas computacionais que permitem a identificação e verificação de pessoas a partir da análise biométrica de seus rostos a partir de fotos e vídeos. Sua aplicação tem sido amplamente empregada em diversas cidades brasileiras — com a justificativa de fortalecer a prevenção de crimes, apoiar investigações e promover maior eficiência na atuação das forças de segurança — porém está longe de ser um consenso, tanto política quanto socialmente. Por exemplo, em 2019 a Câmara de Deputados brasileira realizou audiência pública com diversos setores da sociedade para discutir a aplicação do reconhecimento facial para a manutenção da segurança pública (Almeida, 2022).

O emprego das TRFs no Brasil foi impulsionado a partir da realização da Copa do Mundo de 2014 e das Olimpíadas do Rio de Janeiro em

2016, eventos que demandaram um significativo aparato de segurança e vigilância digital, ampliando a aquisição de infraestrutura mais moderna entre aquelas que estavam disponíveis à época e a atuação de empresas especializadas no setor de segurança. Desde então, a utilização das TRFs tem se expandido de maneira significativa, sendo incorporada no setor público em diferentes estados e municípios — além de empresas privadas de segurança —, buscando ampliar ações de monitoramento em tempo real, sobretudo em áreas com grande circulação de pessoas.

Em um levantamento recente realizado por Picolo e Nunes (2024), os autores apontam que, atualmente, cerca de 37% da população brasileira está submetida a algum tipo de vigilância facial, muitas vezes sem ciência ou consentimento formal. Esse dado demonstra o alcance crescente dessas tecnologias e levanta questões importantes quanto à transparência e à governança das informações coletadas. Comumente, não realizamos tal reflexão crítica no dia a dia por conta da naturalização que as TICs se fazem presente. Entretanto, é importante observar que existe um discurso de segurança que embaça as fronteiras do que é ou não aceitável entre as TRFs no cotidiano.

Desde sua implementação para a abordagem e consequente prisão de suspeitos de crimes houve diversos casos de erros, acarretando em situações que vão de assédio estatal e constrangimento a consequências graves, como acusações criminais e detenções indevidas. Por outro lado, as forças de segurança afirmam que tais tecnologias auxiliam em investigações e economizam recursos públicos, considerando as taxas de erro como casos isolados. Entre os usos mais frequentes das TRFs no país, podemos destacar as operações de reconhecimento automático de foragidos da justiça, a integração com bancos de dados policiais e o uso em grandes eventos e espaços públicos. Na maioria das vezes, a aplicação ocorre por meio de sistemas que cruzam imagens captadas por câmeras de vigilância com bases de dados de mandados de prisão ou registros de pessoas procuradas. Outro exemplo é a matéria

publicada na página eletrônica da Prefeitura de Manaus (2025) que, em tom elogioso, indica como a implementação das TRFs auxiliará na segurança pública, sendo “um dos sistemas mais modernos de monitoramento e inteligência em segurança pública no Brasil”, divulgando a *Smart Sampa*, um sistema de vigilância implementado pela Prefeitura de São Paulo.

O que acaba ocorrendo na segurança pública é que pessoas são identificadas e mandados são expedidos mediante esta prova. Enquanto as forças de segurança se ancoram nos diversos mandados que foram cumpridos por meio dessas tecnologias — o que reforça a percepção institucional de sua eficácia —, registros públicos, entidades civis e reportagens jornalísticas revelam que o emprego das TRFs também ocasionam erros significativos de identificação, resultando em detenções indevidas, constrangimentos e danos individuais.

Para ilustrar os potenciais danos causados pelo uso das TRFs, tomaremos o exemplo de um caso emblemático ocorrido no estado da Bahia. Um homem negro foi identificado por essa ferramenta durante uma festa junina — festividade que ocorre para comemorar os dias de Santo Antônio, São João e São Pedro, santos católicos — em 2022 e acusado de um crime de roubo ocorrido em 2012, ou seja, uma década antes. Conforme relatado, o verdadeiro infrator, detido em flagrante à época, utilizou o nome do vigilante para se identificar, sendo liberado em 2013, apesar de ter sido condenado a uma pena de cinco anos e quatro meses de reclusão. Posteriormente, um mandado de prisão foi emitido em nome do vigilante, o que resultou na sua detenção.

A imagem do vigilante, que estava presente no banco de dados utilizado pelo sistema, foi reconhecida com 95% de similaridade em relação à pessoa procurada, conforme a Secretaria de Segurança Pública da Bahia (SSP-BA). No entanto, a reportagem de Alencar (2023) ressalta que não foi esclarecido o motivo pelo qual a fotografia do vigilante estava armazenada nesse banco de dados, uma vez que ele nunca havia cometido infrações. A

equipe do portal buscou explicações do órgão governamental, mas não recebeu resposta.

Alguns aspectos adicionais merecem ressalva. O vigilante foi detido na presença de sua esposa e filho, o que ocasionou constrangimento e humilhação no contexto familiar. Ademais, a Defensoria Pública da Bahia (DPE-BA), que interveio no caso, destacou a ausência de identificação pessoal — ou seja, utilizando documentos com foto — do verdadeiro infrator durante sua detenção inicial, fator crucial para a injustiça experimentada pelo vigilante. Este episódio revela as falhas do sistema de reconhecimento facial, que não apenas culminaram na violação dos direitos do trabalhador, mas também corroboram críticas acerca da utilização ética e responsável dessa tecnologia.

Os erros de reconhecimento facial vêm sendo discutidos em diferentes ambientes acadêmicos e jurídicos, com destaque para estudos que apontam a maior taxa de falhas na identificação de pessoas negras, indígenas e de pele parda. Pesquisas nacionais e internacionais mostram que os algoritmos utilizados para treinamento dessas tecnologias, em sua maioria, são construídos com base em bancos de dados pouco diversos, o que afeta diretamente a acurácia das identificações quando aplicadas em países com alta diversidade racial e étnica, como é o caso do Brasil (Almeida, 2022). Assim, mesmo diante de justificativas operacionais, a aplicação prática das TRFs requer uma análise mais ampla sobre os efeitos que produz em diferentes segmentos sociais.

Outro aspecto relevante é o crescente envolvimento de empresas privadas no fornecimento e operação desses sistemas, muitas vezes por meio de contratos firmados sem licitação ou com pouca transparência. Em alguns estados, consórcios empresariais atuam diretamente na gestão das câmeras, manutenção dos sistemas e atualização dos bancos de dados. A relação entre o setor público e as empresas de tecnologia levanta questões sobre governança de dados, propriedade intelectual dos algoritmos e

fiscalização independente do uso das imagens captadas.

Para analisar o impacto da utilização dessas tecnologias no âmbito brasileiro, este trabalho funda-se na abordagem de cartografia de controvérsias (Venturini, 2009), procurando identificar quais são os atores envolvidos e afetados pela utilização dessas tecnologias no Brasil, suas posições nos conflitos provenientes e as complexas relações de poder relacionadas, posições de instituições públicas e privadas e dinâmicas sociais. A abordagem de cartografia de controvérsias tem se mostrado eficaz na análise de cenários marcados por disputas de narrativas e conflitos de interesse, como é o caso da adoção das tecnologias de reconhecimento facial. A escolha por essa abordagem está relacionada ao caráter multidimensional do tema, que envolve aspectos técnicos, jurídicos, administrativos, comunicacionais e sociais, sem que haja uma posição dominante ou consenso consolidado entre os diferentes setores envolvidos.

2 Referencial Teórico

O referencial teórico aborda criticamente a tecnologia de reconhecimento facial como instrumento de vigilância que reforça desigualdades raciais, sustentando-se na ideia de racismo algorítmico e opacidade institucional, com ênfase em como essas práticas afetam desproporcionalmente certas populações.

O debate sobre o uso de tecnologias de reconhecimento facial na segurança pública se intensificou nos últimos anos a partir das evidências produzidas de que tais sistemas apresentam diferentes níveis de desempenho em relação a diferentes grupos étnicos. O relatório produzido em 2022 pelo Conselho Nacional das Defensoras e Defensores Públicos-Gerais (CONDEGE) aponta que 83% das pessoas presas injustamente por meio de reconhecimento biométrico facial eram negras, a partir de dados de 2021. Ao considerar ainda que 9,4% dos registros sobre os casos não incluíam informações sobre raça, é possível que a porcentagem de pessoas negras afetadas seja ainda maior. O mesmo

relatório aponta que o tempo médio das prisões efetuadas injustamente foi de nove meses, o que demonstra ser um processo demorado.

Então, essa situação incita um justo questionamento sobre os critérios, práticas e estruturas que envolvem a utilização de TRFs em um país historicamente marcado por desigualdades e violência de cunho racial. Através de uma história marcada pela perseguição, levando em consideração cas pessoas negras que foram escravizadas durante mais de três séculos e intimidações posteriores, incluindo uma lei que criminalizava a capoeira, prática que tem raízes afro-brasileiras (Brasil, 1890).

A tecnologia de reconhecimento facial, segundo definição da empresa de segurança digital Kaspersky (s.d.), consiste em um sistema que identifica ou confirma a identidade de uma pessoa por meio de seu rosto. Esse sistema, organizado através de uma inteligência artificial (IA), pode identificar pessoas tanto em vídeo quanto em fotografias, inclusive em tempo real. Seu funcionamento ocorre em quatro etapas. A primeira delas é a detecção do rosto, em que a câmera localiza a imagem de um rosto, tanto sozinho quanto em uma multidão, tanto de frente quanto de perfil. Em seguida, na segunda etapa, há a análise do rosto. Após a captura e análise da imagem, o sistema faz uma leitura da geometria do rosto e, a partir de certos pontos de referência, separam certas características que distinguem um rosto dos demais. A terceira etapa é a conversão da imagem em dados, em que a imagem é transformada em informações digitais com base nas características distintivas do rosto capturado e analisado. Por fim, essa “impressão facial” (por isso, chamada de biometria facial) é procurada e localizada dentro de um ou mais banco(s) de dados para a realização de uma correspondência.

Apesar de ser apresentada como neutra, a tecnologia tem vieses de acordo com seus criadores e dados utilizados, assim, não opera isoladamente dos contextos sociais ocorrendo na sociedade. O conceito de “racismo algorítmico” é então apresentado no intuito de

descrever a forma como sistemas automatizados, como os de reconhecimento facial, podem reproduzir e reforçar desigualdades raciais. Tarcízio Silva (2022), na obra “Racismo Algorítmico: inteligência artificial e discriminação nas redes digitais”, vai definir o que é racismo algorítmico da seguinte forma: “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 detrimento de grupos minorizados”. Nesse sentido, o pesquisador brasileiro busca chamar a atenção sobre a maneira como as tecnologias podem servir como um novo lugar em que se perpetua o racismo e, desse modo, reproduzir ideologicamente os valores discriminatórios, que são imputados através dos processos de codificação e decodificação, para além dos valores já estabelecidos na sociedade brasileira racista.

Entende-se que o racismo algorítmico não se refere a uma intencionalidade programada, mas sim à forma como os sistemas tecnológicos refletem os padrões discriminatórios dos dados com os quais são treinados. Os algoritmos aprendem com bancos de dados historicamente enviesados, e acabam por perpetuar esses vieses de forma automatizada. Para Silva (2022) as tecnologias não são racistas por si mesmas, mas tornam-se instrumentos de discriminação ao serem alimentadas por práticas digitais já marcadas por desigualdades explícitas, como o racismo discursivo. Ou seja, existe um discurso que já é produzido historicamente que está presente e precede as relações sociais que são estabelecidas entre indivíduos e tecnologias algorítmicas.

Outro conceito importante de ser apresentado na discussão sobre a utilização das TRFs é o de “opressão algorítmica”, isso porque ele auxilia a compreender os mecanismos pelos quais os aparatos tecnológicos digitais reforçam estigmas e desigualdades raciais. A pesquisadora norte-americana Safiya Umoja Noble, em sua obra *Algorithms of Oppression: How Search Engines Reinforce Racism* (2018),

analisa como mecanismos de busca associam automaticamente termos relacionados a pessoas negras a conteúdos sexualizados ou violentos. O exemplo citado por Noble envolve a busca pelo termo “black girls”, que frequentemente retorna resultados com conteúdo pornográfico. Para a autora, esse tipo de associação não é acidental, mas sim resultado de uma lógica algorítmica baseada em padrões discriminatórios historicamente reforçados na internet e em bancos de dados comerciais.

Historicamente, a sociedade brasileira vive dentro de uma lógica que se baseia no mito da democracia racial – segundo a qual o Brasil seria uma sociedade miscigenada e livre de conflitos raciais, o que não é historicamente uma verdade, devido às relações de dominação estabelecida entre brancos e negros e indígenas, que tiveram de assumir um papel de subalternidade — e, assim, nega a existência de discriminações raciais, contribuindo para a reprodução silenciosa de práticas discriminatórias e dificultando seu reconhecimento, inclusive quando mediadas por tecnologias.

O processo de reconhecimento fotográfico, mesmo antes do advento dos sistemas automatizados, já demonstrava seletividade racial dos agentes de segurança. O relatório do CONDEGE (2022) cita casos em que, mesmo com impossibilidade de identificação segura por parte das vítimas (como em ambientes escuros), estas eram induzidas a realizar reconhecimentos baseados em fotografias previamente selecionadas por pessoas reais — não algoritmos —, prática que contribuiu para a prisão de pessoas inocentes, majoritariamente negras.

Em sua obra *Pele negra, máscaras brancas* (2020), Fanon analisa como o processo de racialização se impõe sobre pessoas negras, desumanizando-as e atribuindo a elas características que as distanciam da idealização da humanidade branca. Esse processo de desumanização é fundamental para entender como sistemas que supostamente tratam todos de maneira igual acabam por afetar negativamente grupos

racializados, já que o treinamento dos algoritmos é feito em bases de dados comerciais de pessoas majoritariamente brancas, assim, características físicas de pessoas racializadas são menos reconhecíveis. Tal prática pode ser vista como prática atualizada do que acontece desde as câmeras analógicas que, calibradas a partir de imagens de mulheres brancas, o que resultava em imagens ruins para tons de pele escura, ou seja, os padrões técnicos da fotografia não foram feitos para capturar com qualidade peles escuras (Roth, 2009) — sendo este mais um fato que corrobora para a tese de que tecnologias não são neutras e isentas de vieses.

Como afirma Jackie Wang (2022), “desde o final do século XIX, abordagens baseadas em dados estatísticos para entender o crime têm sido usadas para perpetuar a institucionalização da violência antinegro e legitimar o policiamento”. Importante destacar que a ciência tentou justificar as desigualdades entre raças através de pseudociências que ganharam força naquele referido período, indicando inferioridade de determinados grupos sociais, como pessoas negras, que seriam, supostamente, pessoas mais violentas ou com menor capacidade intelectual. Tal visão preconceituosa e estereotipada aparece em discursos que são produzidos em diversos âmbitos sociais. No contexto contemporâneo, o que há de novo, porém, é a confiança inferida à tecnologia servindo como salvaguarda desse processo, junto à velocidade com a qual se alastra mundialmente.

A psicóloga Daiane de Souza Mello relata ter sido abordada por policiais, em uma conferência, antes de iniciar sua jornada de trabalho, após seu rosto ter sido associado, por um sistema de reconhecimento facial, a uma mulher com mandado de prisão em aberto (Braga, 2024). Esse tipo de erro de identificação, também conhecido como “falso positivo”, é uma ocorrência comum em sistemas de reconhecimento facial que operam com baixa precisão em rostos de pessoas negras. Segundo Braga (2024), essa tecnologia já era utilizada em vinte estados brasileiros até 2021, e a quantidade de erros envolvendo

peças negras tem sido um dos principais pontos de contestação quanto à sua eficácia e justiça.

Para analisar as implicações sociais, morais e jurídicas do uso de sistemas automatizados em decisões que afetam a vida das pessoas, surge o campo de estudos da ética algorítmica. Para Bezerra e Costa (2022), é fundamental refletir sobre que tipo de ética deve guiar o desenvolvimento e a aplicação dos algoritmos: se uma ética voltada à proteção dos interesses corporativos ou uma ética baseada na justiça social e no bem comum. A falta de transparência nos algoritmos — talvez o ponto principal das críticas sobre o funcionamento dessa tecnologia —, bases de dados e processamentos utilizados dificulta a fiscalização e o debate público sobre seus impactos, o que beneficia as empresas de tecnologia desenvolvedoras em detrimento da proteção dos direitos fundamentais, que deveriam nortear o Estado.

Também com relação à ética de uso das TRFs, deve-se observar que a relação entre segurança pública e tecnologias de vigilância é também atravessada por interesses econômicos. Segundo dados citados na matéria de Alencar (2023), publicada no G1 e já mencionada neste trabalho, o governo da Bahia teria investido aproximadamente R\$ 700 milhões em sistemas de reconhecimento facial. Esse valor indica a consolidação de um mercado da vigilância, no qual empresas de tecnologia oferecem soluções voltadas à segurança urbana como produtos comercializáveis. A expansão desse setor, por sua vez, alimenta uma lógica de constante monitoramento da população, sem que existam garantias efetivas de que os sistemas em operação respeitem os princípios constitucionais de presunção de inocência, igualdade e não discriminação.

Outro problema relacionado às TRFs é o de consentimento e privacidade. Tais tecnologias, ao atuarem sobre imagens captadas em espaços públicos, muitas vezes operam sem o conhecimento prévio dos cidadãos e com armazenamento em bancos de dados que não têm controle social efetivo. Pensando no uso

ético de imagens e levando em consideração que elas são captadas aleatoriamente e sem solicitação dos indivíduos envolvidos, como é possível garantir a privacidade das pessoas envolvidas? Na matéria de Molina (2023), a *Google* foi condenada em R\$ 15 mil por expor a imagem de uma mulher de 61 anos que teve sua imagem publicada na ferramenta *Street View*, do *Google Maps*, sem seu consentimento, e a justiça brasileira estipulou um valor de reparação. Ela apareceu em uma das imagens da ferramenta da *Google*, trabalhando como diarista em uma casa e, após tentativa de contato, não obteve resposta e, por essa razão, processou a empresa. Após a ação judicial, que teve a decisão favorável à mulher que teve seu “patrimônio íntimo” violado como cidadã, também garantiu o desfoque da imagem.

Com o objetivo de tecer uma investigação sobre a vigilância de Estado, Bezerra (2020) aponta que o medo e a perspectiva de morte podem contribuir para um maior aceite da população em relação à pervasividade de sua privacidade, caso o processo viabilize maior sensação de segurança:

O recente aumento de práticas estatais de vigilância e sua aparente aceitação social é o fenômeno que motiva a escrita destas linhas, inspiradas pela percepção de que, em tempos de pânico social, a insegurança em relação à vida contribui para que governos implementem, sem grande resistência popular, medidas de vigilância e controle que ultrapassam o mero combate à “ameaça” em questão, venha de inimigo humano ou não humano (Bezerra, 2020, p. 34).

É importante ressaltar que a lei brasileira presume a inocência de qualquer pessoa acusada a não ser que se prove o contrário. Ao utilizar o reconhecimento facial mediado por uma tecnologia baseada em inteligência artificial, existe a probabilidade de erro por conta da falta de informações que consigam individualizar a imagem de pessoas negras, tratadas de forma semelhante e sem marcas

individuais que as destaquem uma das outras. A ocorrência de penalidades a pessoas inocentes acontece em uma maioria ampla, entre pessoas negras. Os problemas atrelados à falta de precisão mascaram o real problema que é a base racista de imputação de dados nesse tipo de tecnologia, que já foi sugerido anteriormente.

Rosa, Pessoa e Lima (2020) realizam uma crítica importante no que diz respeito ao lugar da suposta neutralidade tecnológica que reverbera entre aqueles que defendem o uso das tecnologias de reconhecimento facial, partindo do lugar do racismo. Em seu artigo, realizam um estudo que apontam para o lugar de vigilância e controle social que é estabelecido pelas tecnologias diante da realidade pandêmica da época e, diante dessas transformações sociais, o lugar da tecnologia precisa ser questionado diante da falta de isenção tecnológica, uma vez que o processo de programação tem potencial de ampliar o encarceramento em massa da população negra brasileira.

3 Procedimentos Metodológicos

Esta pesquisa adota como base metodológica a cartografia das controvérsias, compreendida aqui não apenas como um conjunto de técnicas de observação e descrição, mas como um verdadeiro dispositivo epistemológico que permite acessar as camadas profundas e instáveis da vida social. Desenvolvida a partir da Teoria Ator-Rede (ANT), e tendo em Bruno Latour e Tommaso Venturini alguns de seus principais expoentes, essa abordagem se mostra especialmente adequada para a investigação de temas atravessados por conflitos sociotécnicos e disputas de poder, como é o caso da implementação de (TRFs) na segurança pública brasileira.

Ao rejeitar qualquer forma de simplificação apriorística dos fenômenos sociais, a cartografia das controvérsias parte do princípio de que toda observação é necessariamente situada, e que a objetividade, longe de ser alcançada pela aplicação de um modelo teórico universal, só pode emergir da multiplicação dos pontos de vista. Venturini (s.d.) sustenta

que a imparcialidade não se dá por meio da distância, mas pela abertura à complexidade dos discursos e pela escuta atenta dos atores envolvidos. A cartografia, nesse sentido, não busca resolver controvérsias, mas torná-las mais visíveis, mais densas, mais discutíveis.

No caso específico desta pesquisa, a escolha metodológica pela cartografia se justifica pela necessidade de compreender como se constituem e se transformam as relações de poder em torno do uso de TRFs em contextos urbanos brasileiros. As tecnologias de reconhecimento facial não são aqui tratadas como instrumentos neutros, mas como dispositivos sociotécnicos que participam ativamente da constituição de subjetividades, da gestão de populações e da administração da insegurança. É nesse sentido que a cartografia permite analisar não apenas os argumentos em disputa, mas também os arranjos institucionais, os dispositivos técnicos, as alianças improváveis e os silenciamentos operados ao longo do conflito.

A pesquisa se estrutura a partir de três grandes frentes de observação: a análise de produções bibliográficas que tematizam a plataforma do Estado e a digitalização da saúde e da segurança; o acompanhamento de notícias veiculadas na mídia hegemônica e alternativa sobre o uso de TRFs; e a descrição dos atores e dispositivos envolvidos nas controvérsias analisadas. Trata-se de seguir o conselho de Venturini ao "mergulhar no magma" da vida social, buscando observar a controvérsia em sua dinâmica quente, ou seja, em seu momento de efervescência, quando as alianças ainda não estão estabilizadas e os sentidos ainda estão em disputa.

Seguindo a proposta de Latour e Venturini, todo elemento que faz diferença para a dinâmica da controvérsia é considerado um ator, independentemente de ser humano ou não-humano. Assim, algoritmos, bancos de dados, câmeras, softwares, discursos, legislações e mesmo ausências (como a exclusão de determinados grupos sociais do debate) são levados em conta na análise.

Outra dimensão importante do método diz respeito às formas de publicização e confinamento das controvérsias. Lemieux (2007) chama a atenção para a existência de uma tensão constante entre os esforços de restringir o conflito ao círculo de especialistas e aqueles que buscam ampliá-lo para o público leigo. Tal tensão foi particularmente observada nas disputas em torno das TRFs, em que determinados setores do Estado e da indústria tecnológica operam um discurso de técnica e inevitabilidade, enquanto movimentos sociais e defensorias públicas lutam para tornar visíveis os impactos discriminatórios dessas tecnologias.

O tratamento simétrico dos atores também constitui um eixo fundamental da abordagem adotada. O princípio de simetria, defendido por Bloor e retomado por Lemieux, exige que o pesquisador trate com igual seriedade os argumentos de todos os lados da controvérsia, mesmo quando existam assimetrias gritantes de poder entre os envolvidos. Tal postura não visa negar a existência de domínios e desigualdades, mas evitar que o próprio pesquisador as naturalize ou reproduza em sua análise.

A cartografia das controvérsias, por fim, não se apresenta apenas como um método de pesquisa, mas como uma postura política e epistemológica diante do mundo. Sua aposta é que, ao descrever com rigor e sensibilidade os conflitos que moldam o presente, podemos criar as condições para uma participação mais qualificada e democrática nos processos de definição coletiva da vida em comum. Ao se recusar a encerrar a controvérsia, a cartografia a torna compartilhável, inteligível e, sobretudo, discutível.

4 Resultados Parciais ou Finais

A partir da metodologia da cartografia de controvérsias, é possível compreender como se configuram os debates públicos, institucionais e técnicos acerca das Tecnologias de Reconhecimento Facial no Brasil, um assunto complexo, que envolve distintos interesses econômicos, políticos, sociais e éticos. De modo geral, a configuração analítica

dessa controvérsia pode ser representada por uma estrutura triádica, composta por três grandes conjuntos de atores: os defensores da adoção massiva das TRFs, os opositores críticos a essa implementação e a população brasileira, que ocupa um lugar ambíguo, ao mesmo tempo julgadora, afetada e parcialmente informada sobre o tema.

O primeiro grupo identificado na controvérsia é composto por atores que promovem e legitimam o uso crescente das TRFs na segurança pública. Entre esses atores estão representantes das forças policiais, setores do poder público, empresas de tecnologia e segurança, e determinados segmentos da classe política. Seu discurso é fortemente pautado pela noção de modernização tecnológica e pela promessa de eficiência e racionalidade na gestão da segurança pública em um país marcado por altos índices de criminalidade urbana.

O primeiro argumento apontado por esses atores é o processo natural e necessário de modernização das forças de segurança pública diante das transformações sociais e urbanas do Brasil. Argumenta-se que, diante do crescimento populacional nas grandes metrópoles e da escassez de recursos humanos e materiais nas forças de segurança, as TRFs tornam-se ferramentas indispensáveis para otimizar os processos investigativos, agilizar a identificação de suspeitos e fazer bom uso dos recursos. Há uma percepção de celeridade conferida através das tecnologias, algo que é altamente replicado no senso comum. Dito de outro modo, é como se as ferramentas de reconhecimento facial oferecessem um modo ágil de resolução de problemas de segurança, ainda mais diante de uma realidade considerada impune. De acordo com levantamento realizado pelo Instituto Sou da Paz (2024), com dados referentes ao ano de 2022, 6 em cada 10 homicídios não têm solução. Apoiados através dessa narrativa, o argumento da modernização em busca da celeridade dos processos investigativos, uma vez que a sensação de insegurança é fomentada através dessa realidade que é reforçada de tempos em tempos.

Outro ponto central na argumentação pró-TRFs é o da eficácia no combate ao crime, facilitação e agilidade em investigações através da identificação de suspeitos foragidos em bancos de dados integrados, alimentados por diversas fontes. Diante daquele número exposto no levantamento do Instituto Sou da Paz (2024), o argumento da eficácia no combate aos crimes tornaria, aparentemente, os processos mais ágeis que os métodos tradicionais, o que poderia diminuir os erros operacionais. No entanto, não se leva em consideração as possíveis falhas que podem acontecer através do uso das tecnologias, algo que é possível de ocorrer, afinal, toda tecnologia é produzida através de mãos humanas e é possível de falhas. Conforme Rosa, Pessoa e Lima (2020), podemos observar que existem diversos erros diante de questões como falta de luz e necessidade de calibragem da captura de imagem.

O terceiro argumento se refere à otimização de recursos públicos. Com a automatização de processos e a integração entre bases de dados, os defensores afirmam que seria possível reduzir custos operacionais, garantindo eficácia e reduzindo prejuízos — tanto materiais quanto humanos — tanto ao Estado quanto à população. Essa lógica econômica de eficiência também é usada como justificativa ética: garantir a segurança da população com menor risco e menor custo seria, portanto, uma responsabilidade das instituições públicas. A narrativa da modernização é apresentada, então, não apenas como inevitável, mas como desejável, como um avanço civilizatório.

As últimas justificativas são interconectadas: a segurança reforçada em eventos culturais e esportivos que tem como consequência a melhoria econômica por meio do aumento de turistas nas principais cidades do Brasil, atraídos pelos grandes eventos culturais, turísticos e esportivos — pioneiros no uso de TRFs — e a sensação de proteção causada pela utilização de equipamentos de vigilância. Empresas fornecedoras de TRFs também participam ativamente da construção desse discurso, muitas vezes oferecendo seus

produtos a título experimental ou firmando parcerias com entes públicos. Há uma forte presença de marketing tecnológico, na qual a ideia de “cidade inteligente” é associada ao uso intensivo de vigilância automatizada. Essa associação, embora carregada de promessas, nem sempre se sustenta em evidências concretas, mas mobiliza um imaginário coletivo de progresso, ordem e previsibilidade. Assim, existe toda uma mobilização de sensações e percepções de segurança que reforça esse universo mais favorável à implementação das tecnologias de reconhecimento facial.

Já os opositores do emprego de tais tecnologias têm se mobilizado para contestar a implementação indiscriminada das TRFs, chamando atenção para seus riscos, limitações técnicas e implicações sociais e políticas. Com um pensamento menos otimista, nesse grupo encontram-se organizações da sociedade civil, pesquisadores acadêmicos, ativistas de direitos humanos, defensores públicos, coletivos antirracistas e representantes de movimentos sociais. A crítica formulada por esses atores não se resume a uma recusa das tecnologias em si — um pânico tecnofóbico, mas denuncia as formas específicas como essas ferramentas têm sido implementadas indiscriminadamente, com pouca regulação, transparência e comprovação de eficácia, e os efeitos desiguais que elas produzem. Essa posição crítica é fundamentada através de estudos e pesquisas e é mais questionadora da realidade em que as tecnologias estão presentes em nosso cotidiano.

Um dos principais pontos de contestação refere-se aos vieses contidos em softwares e bases de dados com pouca ou nenhuma transparência de fontes e tratamento, apresentando alto viés racial, com imprecisões que afetam principalmente a população negra. Estudos como o de Buolamwini e Gebu (2018) apontam que as taxas de erros são significativas na identificação de pessoas negras, especialmente mulheres negras, quando comparadas a indivíduos brancos. Conforme já apontado anteriormente em nosso trabalho, as imagens de pessoas negras

ou foram colocadas de lado ou apresentam dificuldade nas suas captações em tecnologias, desde a época do desenvolvimento da fotografia. No trabalho de Buolamwini e Gebru (2018), os dados apontam para números alarmantes, chegando a 34% na classificação de gênero para mulheres negras, enquanto para homens brancos a taxa de erro é menor que 1%. Essas informações demonstram como nessa realidade há uma profunda assimetria nos resultados produzidos pelos algoritmos, comprometendo sua confiabilidade e expondo grupos racializados a riscos de criminalização indevida — retomando o que foi dito anteriormente pelo histórico viés de aparatos tecnológicos. Ainda que exista a necessidade de tornar os processos mais eficazes, estes possíveis erros podem impossibilitar o sucesso na sua implementação.

Outro fator apontado pelos opositores das TRFs é a falta de transparência quanto à origem e ao tratamento das bases de dados utilizadas. Casos emblemáticos — como o da inclusão de uma foto do ator americano Michael B. Jordan como suspeito em uma investigação no Ceará (G1 CE, 2022) — colocam em cheque a verificação das fontes de suspeitos, apontando precariedade da verificação das fontes e a ausência de protocolos claros. A apuração dos fatos é uma questão muito importante, ainda mais em um contexto de grande profusão de dados e informações no contexto contemporâneo. As chances de erros se tornam maiores diante de processos que estremecem a integridade da informação. Assim, levando em consideração que o impacto em pessoas negras é maior do que quando comparados com pessoas brancas, a chance de gerar uma situação injusta é maior, o que, de acordo com os críticos do uso das TRFs, impossibilitaria a confiabilidade completa e unicamente ligada ao reconhecimento facial.

Em seguida são apresentados os argumentos que concernem aos riscos de criminalização de parcela já marginalizada da sociedade, reproduzindo práticas de apagamento, classificação e dominação de certos grupos, visto que mais de 90% das pessoas identificadas por TRFs no Brasil são negras

(Silva, 2023). Em vez de garantirem mais precisão, as TRFs, tal como vêm sendo implementadas, acabam produzindo novos erros, que incidem com maior intensidade sobre as populações negras e pobres. Nesse sentido, tais tecnologias não são apenas ferramentas técnicas, mas dispositivos de poder que reatualizam mecanismos coloniais de vigilância, dominação e exclusão. Ou seja, o uso dessa tecnologia pode reproduzir um controle sobre os corpos negros.

Esses erros não são apenas efeitos colaterais, mas têm consequências materiais profundas: prisões injustas, perda de empregos, danos à reputação, traumas psicológicos e destruturação de vínculos familiares. Por isso, as consequências desproporcionais para pessoas negras e pobres identificadas erroneamente também são apontadas como ponto de atenção no uso amplo de TRFs. O exemplo do caso citado como ponto de partida é um exemplo das consequências possíveis: o vigilante perdeu seu emprego, ficou 26 dias encarcerado longe de sua família, com consequências psicológicas, econômicas e sociais não apenas para ele como para sua família. Tais impactos reverberam não somente ao caso do vigilante que, na verdade, torna-se um exemplo aos demais semelhantes a ele, sendo um símbolo do controle das TRFs.

As críticas às TRFs também abrangem a falta de transparência e regulamentação em todos os processos de implantação da tecnologia, como aquisições de ferramentas sem licitações claras, omissão de informações sobre garantia de segurança de dados sensíveis, violação da Lei Geral de Proteção de Dados (LGPD) principalmente no que concerne a dados biométricos de crianças e adolescentes e a falta de informação sobre quais tratamentos são aplicados nos dados. Há ainda sérias dúvidas sobre a soberania digital dos dados, visto que muitas das empresas responsáveis têm sedes ou servidores em outros países, sem garantias claras de que os dados dos cidadãos brasileiros não serão compartilhados ou utilizados indevidamente. Conforme apontado em outro momento em nosso trabalho, uma mulher teve sua imagem exposta através de uma

ferramenta da *Google*, o que demonstra a necessidade do respeito legal para garantia do respaldo ético e judiciário dos cidadãos.

Por fim, os opositores questionam a efetividade das TRFs como política de segurança pública. Apesar da promessa de modernização e eficiência, não há evidências robustas de que a presença dessas tecnologias tenha resultado em redução significativa da criminalidade. A sensação de segurança gerada pela vigilância pode, inclusive, mascarar práticas autoritárias e ampliar desigualdades, ao invés de resolvê-las. Para muitos críticos, o investimento em tecnologias de reconhecimento facial desvia recursos que poderiam ser destinados a políticas de prevenção, educação, moradia e saúde – áreas que, de fato, atuam nas causas estruturais da violência.

5 Considerações Parciais ou Finais

As TRFs podem ser identificadas como uma “tecnologia de poder” (Foucault, 2005), atuando como instrumento legitimador de hierarquias raciais sob o pretexto de maior segurança e eficiência num ciclo vicioso implementado desde a colonização no Brasil, em que o policiamento é orientado para as classes menos privilegiadas. A cartografia da controvérsia em torno das Tecnologias de Reconhecimento Facial no Brasil revela, então, um campo tensionado por interesses diversos, disputas narrativas e profundas assimetrias de poder. O que está em jogo são modelos de sociedade, formas de controle social, conceitos de segurança e justiça, e o próprio papel do Estado na mediação dos conflitos urbanos. Mapear essa controvérsia é, portanto, um passo fundamental para a construção de políticas públicas mais transparentes, participativas e orientadas por critérios de equidade. A adoção de qualquer tecnologia que interfira diretamente nos direitos fundamentais da população exige não apenas comprovação de sua eficácia, mas também garantias éticas, jurídicas e democráticas de sua utilização.

A falta de regularização e fiscalização intensas sobre a captação, uso e tratamento de dados

biométricos cria uma zona cinzenta de atuação, em que empresas privadas e órgãos estatais implementam tais tecnologias sem controle social devido, ampliando sua capacidade de intervenção sobre a população. É importante destacar nesse sentido que o avanço das TRFs se deu em um contexto de crescente investimento estatal em vigilância tecnológica, frequentemente associado à retórica da “modernização” da segurança pública. Essa narrativa é instrumentalizada por setores do Estado e por empresas privadas de tecnologia para justificar a adoção acelerada dessas ferramentas, mesmo diante da ausência de regulação clara, transparência nas aquisições e evidências robustas de efetividade.

Por outro lado, as forças de segurança brasileiras são constantemente cobradas por maior eficiência e a modernização é componente crucial para tal, a implementação do novo urbanismo militar é considerado um avanço e as TRFs se tornaram ferramentas de segurança pública vitais para o policiamento (Sousa et al., 2024). No entanto, a promessa de “eficiência” associada às TRFs, entretanto, revela-se problemática quando confrontada com os dados empíricos que apontam altos índices de erro, notadamente direcionados a pessoas negras, periféricas e socialmente vulnerabilizadas.

Além disso, pesquisa realizada procurou evidenciar o papel ambíguo ocupado pela população brasileira nesse debate. Enquanto parte da sociedade adere ao discurso da segurança - incitada pelo medo - e do progresso tecnológico, muitas vezes sem conhecimento pleno das implicações éticas e sociais das TRFs, outra parte vivencia diretamente os efeitos colaterais dessas práticas. Os contratos com empresas privadas, frequentemente firmados sem licitação e com cláusulas de sigilo sobre algoritmos e bases de dados, dificultam a fiscalização pública e inviabilizam o debate democrático. Ao invés de promover segurança, as TRFs acabam por aprofundar a desigualdade de acesso, além de restringir a possibilidade de contestação e responsabilização por seus erros.

Concluimos, portanto, que o debate sobre as Tecnologias de Reconhecimento Facial no Brasil é revelador de dilemas mais amplos sobre tecnologia, poder e justiça social. Sua utilização, nos moldes atuais, reforça desigualdades históricas e legitima práticas discriminatórias sob o pretexto da neutralidade técnica. Cabe à sociedade civil, à academia, aos órgãos de controle e às instituições públicas o papel de tensionar esse modelo, promover a escuta dos sujeitos afetados e garantir que o futuro digital seja construído a partir de princípios democráticos, inclusivos e transparentes.

Por fim, a abordagem de cartografia de controvérsias permite analisar com profundidade as relações de poder envolvidas na utilização de TRFs no Brasil, revelando interesses ocultos, assimetrias de acesso à informação e mecanismos utilizados pelos agentes que desejam legitimar ou contestar a implementação das ferramentas. Ao mapear agentes, conexões, interesses, narrativas e decisões, procura-se contribuir para um debate mais transparente.

6.1 Referências

- Alencar, I. (2023, setembro 1). Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por "racismo algorítmico"; inocente ficou preso por 26 dias. *G1*. <https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoas-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-preso-por-26-dias.ghtml>.
- Almeida, E. C. (2020). Os grandes irmãos: o uso das tecnologias de reconhecimento facial para perseguição penal. *Revista Brasileira de Segurança Pública*, 16(2), 264–283. <https://doi.org/10.31060/rbsp.2022.v16.n2.1377>.
- Bezerra, A. C. (2020). Do 11/9 à covid-19: a vigilância de estado na perspectiva da ética intercultural da informação. *Informação & Informação*, 25(4), 31–46. <https://doi.org/10.5433/1981-8920.2020v25n4p31>.
- Braga, N. (2024, julho 12). Erro em reconhecimento facial constrange psicóloga em conferência. *Defensoria Pública do Estado do Rio de Janeiro*. <https://defensoria.rj.def.br/noticia/detalhes/29955-Erro-em-reconhecimento-facial-constrange-psicologa-em-conferencia>.
- Brasil. (1890, outubro 11). Decreto nº 847, de 11 de outubro de 1890: Dispõe sobre a liberdade de cultos religiosos. *Câmara dos Deputados*. <https://www2.camara.leg.br/legin/fed/decret/1824-1899/decreto-847-11-outubro-1890-503086-publicacaooriginal-1-pe.html>.
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In S. A. Friedler & C. Wilson (Eds.), *Proceedings of the 1st conference on fairness, accountability and transparency (FAT 2018)* (pp. 77–91). PMLR.
- CONDEGE. (2022). *Relatório sobre reconhecimento fotográfico em sede policial*. <https://www.condege.org.br/wp-content/uploads/2022/02/Relatorio-CONDEGE-DPERJ-reconhecimento-fotografico.pdf>.
- Faustino, D., & Lippold, W. (2023). Racismo algorítmico ou racialização digital? In *Colonialismo digital: por uma crítica hacker-fanoniana* [Recurso eletrônico]. Boitempo.
- Fanon, F. (2020). *Pele negra, máscaras brancas*. Ubu Editora.
- Foucault, M. (2012). *Em defesa da sociedade*. Martins Fontes.
- G1 CE. (2022, janeiro 7). *Foto de astro do cinema Michael B. Jordan aparece em lista de procurados pela polícia do Ceará*. <https://g1.globo.com/ce/ceara/noticia/2022/01/07/astro-do-cinema-michael-b-jordan-appece-em-lista-de-procurados-pela-policia-do-ceara.ghtml>.
- Instituto Sou da Paz. (2024, novembro 13). *Indicador nacional de esclarecimento de homicídios tem leve crescimento e registra 39% para esse tipo de crime ocorrido em 2022*. <https://soudapaz.org/noticias/indicador-nacional-de-esclarecimento-de-homicidios-tem-leve-crescimento-e-registra-39-para-esse-tipo-de-crime-ocorrido-em-2022/>.
- Kaspersky. (n.d.). *O que é reconhecimento facial – definição e explicação*. <https://www.kaspersky.com.br/resource-center/definitions/what-is-facial-recognition>.

- Lemieux, C. (2007). À quoi sert l'analyse des controverses? Mil neuf cent. *Revue d'histoire intellectuelle*, 25, 191–212. (R. Cantu, Trad.). Para que serve a análise de controvérsias?
- Molina, T. (2023, setembro 23). Google é condenado em R\$ 15 mil por expor imagem de mulher no Maps. *Metrópoles*. <https://www.metropoles.com/sao-paulo/google-e-condenado-em-r-15-mil-por-expor-imagem-de-mulher-no-maps>.
- Piccolo, C., & Nunes, P. (2024). Vigilância por lentes opacas: mapeamento da transparência e responsabilização de projetos de reconhecimento facial no Brasil. LAPIN.
- Prefeitura de Manaus. (2025, fevereiro 6). *Prefeitura de Manaus implementará tecnologia de reconhecimento facial para auxiliar na segurança pública*. <https://www.manaus.am.gov.br/noticia/seguranca-publica/tecnologia-reconhecimento-facial/>.
- Roth, L. (2009). Looking at Shirley, the ultimate norm: Colour balance, image technologies, and cognitive equity. *Canadian Journal of Communication*, 34(1), 111–136. <https://cjc-online.ca/index.php/journal/article/view/2199>.
- Sousa, R., Lima, J., & Moreira, F. (2024). Esporte, dados e direitos: o uso de reconhecimento facial nos estádios brasileiros. *Centro de Estudos de Segurança e Cidadania*.
- Van Dijck, J. (2017). Confiamos nos dados? As implicações da datificação para o monitoramento social. *Matrizes*, 11(1), 39–59. <https://www.redalyc.org/articulo.oa?id=143050607004>.
- Venturini, T. (2009). Diving in magma: How to explore controversies with actor-network theory. *Public Understanding of Science*, 19(3), 258–273. (Trad. Mergulhando em magma: como explorar controvérsias com teoria ator-rede).
- Wang, J. (2022). *Capitalismo carcerário*. Igra Kniga.