

Eu conheço esse rosto: a necropolítica presente em sistemas de reconhecimento facial¹

Ana Beatriz Fonseca²
Vinícius da Rosa³
Júlia Duarte dos Santos Silva⁴
Natália Santana Santiago de Oliveira⁵
Carolina Cassoli⁶
Universidade Federal do Rio de Janeiro - UFRJ

Resumo

O presente artigo trata-se de um estudo sobre o uso de inteligência artificial em sistemas de reconhecimento de facial e a discriminação algorítmica que instrumentos destinados à identificação estão suscetíveis a cometer. A pesquisa visa analisar o modo de operação de tecnologias de vigilância e seu direcionamento a grupos racializados. Nesse sentido, o trabalho é constituído por um levantamento de dados sobre a implementação dessas bases algorítmicas em sistemas de reconhecimento facial no Brasil e uma revisão bibliográfica para análise dos conceitos de sociedade de vigilância, racismo algorítmico e necropolítica. Isto posto, o estudo tem o objetivo de verificar os limites da neutralidade técnica no contexto de uma política de segurança discriminatória.

Palavras-chave: reconhecimento facial; comunicação; vigilância; racismo algorítmico; necropolítica.

Introdução

A expansão do uso de tecnologias de processamentos de dados permitiu a conectividade ampliada de sistemas computacionais. O grande volume de dados gerados — parte do fenômeno Big Data (Diebold, 2012) — são coletados e controlados de forma não transparente, permitindo que indivíduos sejam massificados, ranqueados, classificados e selecionados.

Neste ambiente progressivamente digitalizado, o desenvolvimento de tecnologias biométricas se insere como uma ferramenta de identificação, tornando possível uma vigilância, nos âmbitos público e privado, sobre os sujeitos. Essa vigilância é constante, exercida por meio de tecnologias digitais e tem se mostrado

1

¹Trabalho apresentado na IJ05 – Comunicação, Cultura Digital e Tecnologias, da Intercom Júnior – 21ª Jornada de Iniciação Científica em Comunicação, evento componente do 48º Congresso Brasileiro de Ciências da Comunicação ²Estudante de Graduação do 3º período do Curso de Jornalismo da Escola de Comunicação da Universidade Federal do Rio de Janeiro – UFRJ, e-mail: beatrizfonsecanovo@gmail.com

³Estudante de Graduação do 3º período do Curso de Jornalismo da Escola de Comunicação da Universidade Federal do Rio de Janeiro – UFRJ, e-mail: viniciusdarosaoliv@gmail.com

⁴Estudante de Graduação do 3º período do Curso de Jornalismo da Escola de Comunicação da Universidade Federal do Rio de Janeiro – UFRJ, e-mail: juliasduartesprofissional@gmail.com

⁵Estudante de Graduação do 3º período do Curso de Jornalismo da Escola de Comunicação da Universidade Federal do Rio de Janeiro – UFRJ, e-mail: natsantana2004@gmail.com

⁶ Mestranda em Comunicação e Cultura pelo PPGCOM/UFRJ. Orientadora do trabalho, e-mail: carol.cassoli@gmail.com



"uma tendência que já parece irresistível, comum aos mais diversos países" (Rodotà, 2008, p. 147).

Por "biometria" entende-se o reconhecimento automatizado de indivíduos com base nas suas características biológicas, como impressões digitais, traços do rosto, voz e íris do olho ou comportamento (Li; Jain, 2015). Essa tecnologia é responsável pela geração de dados, os quais devem ser coletados, processados e armazenados por uma Inteligência Artificial (IA). A partir desse tratamento, as informações brutas constituem um algoritmo, e criam-se padrões reconhecíveis para a IA.

Quanto à Inteligência Artificial, tem-se variadas definições (Kaufman, 2018; Russel, Norvig, 2013). No presente artigo, adotaremos a elaborada por Russel e Norvig (2013) de que seriam "agentes inteligentes capazes de perceber seu meio ambiente e de realizar ações com a expectativa de selecionar uma ação, que maximize seu desempenho". Elas funcionam com base em algoritmos, que podem ser entendidos como "[...] uma sequência de instruções determinadas para solucionar um problema, por meio de cálculos matemáticos, e são a base do processo de desenvolvimento de um software quando aplicado a lógica computacional" (Bona; Schons; Lopes-Flois, 2023, p. 227).

Dentre as tecnologias biométricas, o reconhecimento facial desponta como um interessante caso de estudo, devido à expansão de sua adesão ao sistema de segurança pública brasileira e a viabilidade de discriminações, especialmente as raciais, por meio da ferramenta.

O reconhecimento facial tem como especificidade o mapeamento das linhas faciais, que considera os pontos nodais — características que distingue uma pessoa —, como distância entre os olhos, largura do nariz e comprimento da linha da mandíbula. A relação entre essas particularidades individuais gera uma geometria espacial que é armazenada e processada pela Inteligência Artificial. É a partir destes dados que os *softwares* comparam imagens e identificam pessoas, processo explicado por Wechsler (2007). O reconhecimento facial pode ser feito sem que o indivíduo interaja com o sistema, através de câmeras de segurança, por exemplo. Além disso, os dados processados podem ser usados para uma extensa gama de propósitos (Nabeel, 2019).

O Brasil começou a integrar tecnologias de reconhecimento facial no sistema da segurança pública em 2019 devido à Portaria n° 793, de 24 de outubro de 2019, que estabelece a utilização de recursos do Fundo Nacional de Segurança Pública para



estimular a instalação de sistemas de videomonitoramento com reconhecimento facial, inteligência artificial ou outras tecnologias similares (Brasil, 2019), em um processo sem muita transparência nem debate público. Pablo Nunes, pesquisador coordenador do Panóptico, projeto do Centro de Estudos de Segurança e Cidadania (CESeC), aponta que "apesar do movimento mundial ser de crítica, banimento ou moratória ao uso do reconhecimento facial pelas polícias, no Brasil temos visto o movimento contrário" (Nunes, 2021).

Neste sentido, no presente artigo, delimitamos como objeto de estudo a biometria de reconhecimento facial, frente à ampliação de seu uso na segurança pública brasileira e a relevância do debate quanto às questões éticas atinentes, especialmente implicações racistas. A pesquisa envolveu levantamento de dados atualizados quanto ao uso de sistemas de reconhecimento facial no Brasil; bem como extensa análise de bibliografia, nacional e estrangeira, sobre a sociedade de vigilância na qual esta tecnologia se insere e sobre relações entre reconhecimentos discriminatórios e o racismo estrutural brasileiro.

Isto posto, nos voltamos ao debate se discriminações racistas por algoritmos biométricos são reflexos de estruturas mentais racistas pré-estabelecidas na sociedade ou carregam intencionalidade. A questão que se impõe a partir disto é se a responsabilização de "erros" racistas deve recair sobre a sociedade da qual deriva a base de dados dos algoritmos e na qual estão imersos os desenvolvedores da tecnologia ou deve recair sobre o projeto e o planejamento da expansão de Inteligência Artificial feitos e financiados por empresas com reconhecida capacidade de evitar tais "erros". Buscamos, a partir da elaboração do debate, verificar a hipótese de que a discriminação algorítmica seria instrumento de necropoder (Mbembe, 2018)

Os alvos e as vítimas da vigilância

O conceito da Sociedade de Controle estabelecido pelo filósofo Gilles Deleuze (2000) propõe uma evolução social da ideia analisada por teórico social Michel Foucault (1987) em relação à Sociedade Disciplinar. "As formas ultra rápidas de controle ao ar livre, que substituem as antigas disciplinas que operavam na duração de um sistema fechado." (Deleuze, 2000, p. 220). O controle social não se encontra mais nas estruturas físicas somente; não obstante, ele se complexifica e alcança novas



vertentes. Para Deleuze (2000, p. 216), ela se diferencia "não mais por confinamento, mas por controle contínuo e comunicação instantânea".

Foucault (1987), ao definir o conceito de panóptico como uma estrutura onde um vigia observa a todos sem ser visto, acaba por influenciar o que Lyon (1994) posteriormente classifica como "olho eletrônico", uma constante coleta de dados sobre os cidadãos pelo Estado e por empresas. Essa vigilância é caracterizada por Rouvroy e Berns (2013, apud Melo e Serra, 2022, p. 5) como governamentalidade algorítmica, ou seja, uma forma de governar que se dá principalmente por meio da coleta e análise de dados, facilitando prever e influenciar comportamentos de forma silenciosa, automática e, a princípio, com rigor técnico.

A vigilância pode ser justificada com o argumento da proteção. Segundo o cientista social brasileiro Edson Passetti (2004, p. 6), "os assujeitamentos na sociedade de controle formam subjetividades que defendem segurança". Desta forma, as câmeras aparecem como uma ferramenta para realizar a vigilância e impor a segurança, ao mesmo tempo, em que trazem o conforto para o indivíduo de que ele está seguro naquela sociedade. A constante presença de câmeras, aliadas ao reconhecimento facial e a instantaneidade da comunicação, impossibilitam escapar dos olhos vigilantes da sociedade.

O dispositivo de Reconhecimento Facial não apenas nos protege, mas nos intimida a uma conduta ideal. Qual é a sensação de ser vigiado? Não temos grades, mas câmeras. O século XXI incluiu, ao Panóptico, uma aparência tecnológica. (Magno; Bezerra, 2020 p. 6).

Esse questionamento levanta a dúvida sobre quem são os alvos dessa vigilância. Dados demonstram que esse olhar se volta a corpos racializados. Entre janeiro e junho de 2019, os estados brasileiros em que dispositivos de reconhecimento facial foram testados — Bahia, Rio de Janeiro, Santa Catarina e Paraíba — detiveram 108.395 pessoas com uso da tecnologia, das quais 66.419 eram negras ou pardas, de acordo com o Departamento Penitenciário Nacional. O que Browne (2015, p.114) chama "vigilância racial" coloca seus alvos na posição de suspeitos propícios, possibilitando que populações socialmente vulneráveis estejam sujeitas à automatização de constrangimentos e violências. Também reitera micro agressões já presentes na sociedade racista brasileira, como a "suposição de criminalidade", denominada por



Tarcízio Silva (2022, p.34). Essa suposição associa, de forma preconceituosa, pessoas racializadas à criminalidade ou à periculosidade. "Se a maioria da população carcerária é negra, todos os suspeitos também são. Os culpados já têm cor" (Magno; Bezerra, 2020, p.6).

A linguagem algorítmica como arma discriminatória

Além de uma vigilância racializada, os sistemas de reconhecimento facial operam contra populações negras e pardas quanto a suas identificações. Não são raros os casos de erros cometidos neste sentido.

Um caso emblemático é o de Robert Williams, um homem negro norteamericano que foi injustamente preso após um software de reconhecimento facial vinculá-lo erroneamente a imagens captadas por câmeras de segurança de uma joalheria. A identificação equivocada se deu porque outro homem negro foi confundido com ele (Silva, 2022).

A cientista de dados Cathy O'Neil (2016) demonstra como modelos são passíveis de erro, sendo modelos aqui entendidos como "a utilização de dados preexistentes para descrever certas regularidades, à medida que tais padrões podem ser aplicados em novas situações" (O'Neil, 2016). Para a autora, modelos como os algoritmos são incapazes de captar a realidade em toda sua complexidade e, por isso, fazem simplificações determinando aspectos mais relevantes de um determinado processo. Nessa classificação de informações válidas ou não para a máquina reside a influência dos desenvolvedores de um sistema.

Nesse sentido, os responsáveis pela coleta de informações detêm o poder sobre os dados coletados e de que forma serão utilizados.

Por trás de toda tecnologia existem sujeitos que as formataram. Há um discurso a ser veiculado. Se o dispositivo de reconhecimento facial seguir a lógica da criminalização adotada pelo Estado, em que negros são sempre culpados, uma parcela majoritária da população enfrentará novos desafios para sobreviver (Magno, Bezerra; 2020, p. 5).

Desta forma, se uma tecnologia é criada por indivíduos inseridos numa sociedade permeada, institucional e subjetivamente, por uma estrutura racista (Almeida, 2020), ela também é componente deste contexto e é atravessada pelo viés racista. Nesse sentido, Tarcízio Silva afirma que "o desenvolvimento de tecnologias algorítmicas se



alimenta do histórico social para oferecer uma pretensa inteligência artificial, que é comprometida com o patriarcado e o colonialismo" (Silva, 2022).

O enviesamento racista expresso pelas Inteligências Artificiais usadas em sistemas de reconhecimento facial torna relevante o apontamento, no presente artigo, do conceito de "racismo algorítmico". Elaborado pelo pesquisador e cientista social brasileiro Tarcízio Silva, o conceito trata das formas contemporâneas do racismo, seus impactos e os chamados "erros programados". Trata-se de uma atualização do racismo estrutural, que opera a partir do privilégio branco presente na sociedade e que, agora, se estende ao ambiente digital. Para além das microagressões que ocorrem no meio online, o racismo algorítmico baseia-se em uma perspectiva centrada no homem branco, promovendo padrões racistas que não se limitam somente à programação técnica dos sistemas tecnológicos.

Segundo o autor, as tecnologias digitais possuem "dualidades que podem pender para a opressão em sociedades marcadas pelas desigualdades" (Silva, 2022, p. 29). Dessa forma, a inteligência artificial se torna um espelho de uma sociedade racista, uma vez que é alimentada não apenas por dados e comandos, mas também por preconceitos e convenções discriminatórias que ajudam a perpetuar o privilégio branco em diferentes esferas.

A compreensão de muitas manifestações do racismo na forma de microagressões em práticas cotidianas é especialmente difícil quando se trata de tecnologias algorítmicas de comunicação, que trazem novas camadas de opacidade em seu funcionamento. Se a tecnologia é erroneamente enquadrada e percebida como neutra, a tal equívoco se soma à negação do racismo como fundante de relações e hierarquias sociais em países como o Brasil (Silva, 2022, p. 29).

Se há um padrão específico direcionado a um grupo social determinado, é ilógico atribuir neutralidade às ocorrências. Algoritmos são programados, programação é uma linguagem e linguagem não é neutra.

As manifestações do necropoder nas tecnologias de reconhecimento facial

Posterior às análises feitas pelo presente trabalho, o apontamento do enviesamento carregado por algoritmos de reconhecimento facial culminam na questão central da pesquisa: as identificações discriminatórias por inteligências faciais



biométricas são reflexos do racismo entranhado na sociedade ou são pensados intencionalmente para essa funcionalidade?

Para responder essa indagação é necessário compreender o conceito de necropolítica. Também conhecido como "política da morte" (Arendt,1951 apud Mbembe, 2018, p.18), trata-se do uso do poder político e social para designar quem deve morrer ou quem pode viver. Partindo da definição do cientista político camaronês Achille Mbembe (2018), a funcionalidade do racismo no controle de corpos em vulnerabilidade social é um projeto de poder que estabelece métricas aceitáveis para criar corpos matáveis. Os grupos racialmente excluídos das posições de poder são oprimidos por aparatos sociais que se justificam pela circunstância, como o combate à criminalidade:

O poder (e não necessariamente o poder estatal) continuamente se refere e apela à exceção, à emergência e a uma noção ficcional do inimigo. Ele também trabalha para produzir a mesma exceção, emergência e inimigo ficcional (Mbembe, 2018, p.17).

Nesse sentido, como já explicitado no tópico anterior, a programação de qualquer tecnologia prevê um treinamento do instrumento a partir dos conceitos de quem a cria. De acordo com o proposto com pesquisador em informática Geoffrey Bowker e a socióloga estadunidense Susan Leigh Star (2000), as opiniões, conceitos e os critérios de decisão são inseridos dentro do aparato tecnológico, fixando discursos em forma de códigos. Sendo assim, as câmeras de vigilância também estão suscetíveis a repetirem atos racistas.

A materialidade dessas políticas segregacionistas é compreendida mediante dados do Colégio Nacional dos Defensores Públicos Gerais que, em 2021, divulgou que 83% dos presos injustamente por reconhecimento fotográfico no Brasil eram negros. À guisa de exemplo, menciona-se o caso do educador Daniel Félix, acusado três vezes por meio de reconhecimento facial, em Niterói, Região Metropolitana do Rio de Janeiro. O jovem negro, de 26 anos, foi absolvido em três acusações diferentes que utilizaram o reconhecimento facial como prova de indiciamento. 8

⁷"Relatórios indicam prisões injustas após reconhecimento fotográfico". CONDEGE, 19/04/2021. Disponível em: https://www.condege.org.br/arquivos/1029. Acesso em: 07 maio /2025.

⁸ "RJ: Jovem negro acusado por reconhecimento facial é inocentado pela terceira vez". Brasil de Fato, 06/10/2023. Disponível em: https://www.brasildefato.com.br/2023/10/06/rj-jovem-negro-acusado-por-reconhecimento-facial-e-inocentado-pela-terceira-vez/. Acesso em: 07 maio 2025.



A organização do "necropoder" (Mbembe, 2018, p.38) é mais expansiva do que a determinação dos corpos elimináveis de uma sociedade, mas também, os corpos possíveis de punição e controle mais que outros. Sob a lógica dessa política de vigilância, é possível afirmar que é "a inserção deste projeto no espectro da política criminal brasileira que tem enfatizado uma atuação da polícia caracterizada pela repressão e opressão de negros sob o pretexto de reforço aos instrumentos de segurança pública" (Ferreira, 2024, p.28).

Considerações finais

Sistemas de reconhecimento facial vêm sendo implementados na segurança pública brasileira como ferramenta de vigilância. Tratamos de como essa vigilância é direcionada a corpos racializados, aplicando a "suposição de criminalidade" (Silva, 2022).

Esta tecnologia biométrica é firmada em algoritmos, os quais — como discutimos — essencialmente carregam vieses da sociedade da qual derivam. Neste sentido, a ausência de neutralidade nos algoritmos possibilita identificações discriminatórias, exemplificadas aqui. O racismo expresso nestes supostos erros pode ser lido como reflexo da sociedade brasileira.

No entanto, é válido pontuar que o investimento anual em reconhecimento facial no mundo está em crescimento: em 2024, o mercado de reconhecimento facial foi estimado em 6,61 mil milhões de dólares, com projeções para atingir 14 mil milhões de dólares em 2029, segundo relatório da empresa Mordor Intelligence. Assim, se a indústria tecnológica realiza investimentos de tal grandeza, elas reconhecidamente têm o recurso financeiro, humano e técnico de desenvolver os algoritmos de modo a evitar a discriminação racial. Todavia, não o fazem. Seja por negligência, seja intencionalmente, a ausência de ação por parte da indústria no sentido de mitigar o problema torna a tecnologia de reconhecimento facial em uma parte dele.

Propusemos como questão motriz do presente artigo: o racismo algorítmico é um produto do racismo pré-existente na sociedade ou é um instrumento de uma estrutura racializante? Frente a tudo apresentado até aqui, é possível deduzir que o reconhecimento facial é um instrumento de necropoder por viabilizar a identificação e a violação de direitos dos corpos mais passíveis de punição e controle: corpos racializados. A responsabilização do racismo automatizado deve recair, portanto, sobre

Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação 48º Congresso Brasileiro de Ciências da Comunicação – Faesa – Vitória – ES De 11 a 16/08/2025 (etapa remota) e 01 a 05/09/2025 (etapa presencial)

as empresas financiadoras e desenvolvedores que não agem em prol da reversão do problema, apesar de possuírem condições de o fazer.

Referências

ALMEIDA, Sílvio Luiz de. Racismo estrutural. São Paulo: Jandaíra, 2020.

BONA, Celito de; SCHONS, Eduarda Arruda; LOPES-FLOIS, Luiza. **Inteligências artificiais**: existe ética na implementação de algoritmos? Ciências Sociais Aplicadas em Revista, Marechal Cândido Rondon, v. 25, n. 45, p. 225-246, 2023.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria N.o 793, de 24 de outubro de 2019. **Diário Oficial da União**: seção 1, Brasília-DF, edição 208, p. 55, 24 de out. 2019. Disponível em: https://in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575. Acesso em: 13 maio 2025.

BROWNE, S. **Dark matters**: on the surveillance of blackness. London: Duke University Press, 2015

DELEUZE, Gilles. Conversações. 1. ed., 3. reimpr. Rio de Janeiro: Editora 34, 2000.

DIEBOLD, Francis X. On the Origin(s) and Development of the Term "Big Data". Penn Institute for Economic Research. University of Pennsylvania. 2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152421https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152421 Acesso em: 15 maio 2025. 2025.

DUARTE, Daniel Edler; NUNES, Pablo; LIMA. Thallita G. L. **Estudos de vigilância**. Coleção Panorama. Rio de Janeiro: CESeC, 2023

FERREIRA, Pedro Paulo da Cunha. **Direito, raça e castigo:** criminologia do preconceito e a (necro)política criminal de aprisionamento racial no Brasil. Boletim IBCCRIM, [S. 1.], v. 30, n. 361, p. 27–29, 2024.

FOUCAULT, Michel. **Vigiar e punir:** nascimento da prisão. 20. ed. Petrópolis: Editora Vozes, 1987.

KAUFMAN, Dora. A inteligência artificial irá suplementar a inteligência humana?. Barueri, SP: Estação das Letras e Cores, 2018.

LI, Stan Z; JAIN, Anil K. (eds.). Encyclopedia of Biometrics. 2nd ed. [Nova Iorque]: Springer US, 2015. Disponível em:

https://www.researchgate.net/publication/280722044_Encyclopedia_of_Biometrics Acesso em: 13 maio 2025

LYON, David. **The electronic eye:** the rise of surveillance society. Minneapolis: University of Minnesota Press, 1994.

MAGNO, Madja Elayne da Silva Penha; BEZERRA, Josenildo Soares. Vigilância negra: o dispositivo de reconhecimento facial e a disciplinaridade dos corpos. Revista Novos Olhares, v.9, n.2, ago./dez. 2020. Disponível em:

https://www.revistas.usp.br/novosolhares/article/view/165698. Acesso em: 13 maio 2025.



Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação 48º Congresso Brasileiro de Ciências da Comunicação – Faesa – Vitória – ES De 11 a 16/08/2025 (etapa remota) e 01 a 05/09/2025 (etapa presencial)

MBEMBE, Achille. **Necropolítica:** biopoder, soberania, estado de exceção, política da morte. São Paulo: n-1 Edições, 2018.

MELO, Paulo Victor; SERRA, Paulo. **Tecnologia de reconhecimento facial e segurança pública nas capitais brasileiras:** apontamentos e problematizações. Comunicação e Sociedade, v. 42, p. 205-220, 2022.

NABEEL, Fahad. Regulating Facial Recognition Technology in Public Places. Centre for Strategic and Contemporary Research, 2019. Disponível em: https://www.academia.edu/39871139/Regulating_Facial_Recognition_Technology_in_Public_P laces. Acesso em: 13 maio 2025.

NUNES, Pablo. O algoritmo e racismo nosso de cada dia. Revista Piauí, 02 jan. 2021. Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia/. Acesso em: 13 maio 2025

O'NEIL, Cathy. **Weapons of math destruction:** how big data increases inequality and threatens democracy. Nova York: Crown, 2016.

PASSETTI, Edson. **Segurança, confiança e tolerância:** comandos na sociedade de controle. São Paulo em Perspectiva, v. 18, n. 1, p. 151–160, jan. 2004.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROUVROY, A.; BERNS, T. **Gouvernementalité algorithmique et perspectives d'émancipation:** Le disparate comme condition d'individuation par la relation? Réseaux, 1(177), 163–196. 2013.

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence:** A Modern Approach. tradução Regina Célia Simille. Rio de Janeiro: Elsevier, 2013.

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

WECHSLER, H. **Reliable face recognition methods:** system design, implementation and evaluation. Springer, 2007.