RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA NO BRASIL: riscos e seletividade penal

FACIAL RECOGNITION IN PUBLIC SECURITY IN BRAZIL: risks and penal selectivity

RECONOCIMIENTO FACIAL EN LA SEGURIDAD PÚBLICA EN BRASIL: riesgos y selectividad penal

Danielly Garcia da Silva[1]

Lorena Gonçalves Oliveira[2]

Vinícius Pedro Teló[3]

RESUMO: O uso de tecnologias de reconhecimento facial na segurança pública brasileira tem se expandido rapidamente, com pelo menos 421 projetos ativos capazes de monitorar 87,2 milhões de pessoas, de acordo com o relatório "Mapeando a Vigilância Biométrica", elaborado pela Defensoria Pública da União (DPU) em parceria com o Centro de Estudos de Segurança e Cidadania (CESeC). Embora os investimentos já tenham superado a marca de R$ 160 milhões, o relatório aponta ausência de transparência, falta de evidências de eficácia e inexistência de controle público - fatores que ampliam o risco de violações aos direitos fundamentais. Busca-se, como problema de pesquisa, responder quais são os principais riscos sociais e jurídicos da adoção dessas tecnologias na segurança pública brasileira, analisar criticamente o uso delas avaliando seus impactos sobre os direitos fundamentais, além de mapear os projetos de reconhecimento facial em operação e os dados disponíveis sobre sua aplicação. A metodologia adotada será bibliográfica e documental. A pesquisa aponta para os riscos de acirramento da seletividade penal, com impactos desproporcionais sobre grupos vulneráveis e marginalizados.

PALAVRAS-CHAVE: : Direitos Humanos; discriminação algorítmica; reconhecimento facial; segurança pública; tecnologia.

[1] Danielly Garcia da Silva é estudante do curso de Direito na Faculdade Insted. E-mail: garcia_danielly@yahoo.com.br.

[2] Lorena Gonçalves Oliveira é professora do curso de Direito na Faculdade Insted. Mestranda em Ciências Criminais pela Pontifícia Universidade Católica do Rio Grande do Sul. Pós-graduada em Direito Penal e Criminologia pelo Introcrim/CEI. Graduada em Direito pelo Centro Universitário Unigran Capital. ORCID iD: https://orcid.org/0009-0006-1707-696X E-mail: lorenagoliveira15@gmail.com.

[3] Vinícius Pedro Teló é professor do curso de Direito na Faculdade Insted. Mestrando e pós-graduado em Ciências Criminais pela Pontifícia Universidade Católica do Rio Grande do Sul. Graduado em Direito pela Universidade Federal do Mato Grosso do Sul. ORCID iD: https://orcid.org/0009-0004-6944-175X E-mail: telo.vinicius@gmail.com.

ABSTRACT: The use of facial recognition technologies in Brazilian public security has expanded rapidly, with at least 421 active projects capable of monitoring 87,2 million people. This is according to the "Mapping Biometric Surveillance" report, prepared by the Public Defender's Office (DPU) in partnership with the Center for Security and Citizenship Studies (CESeC). This practice reflects a global scenario, considering that 70% of the world's police forces have access to some form of facial recognition technology (Bischoff, 2021). Although investments have already surpassed R$ 160 million, the report points to a lack of transparency, insufficient evidence of effectiveness, and absence of public control. These factors significantly increase the risk of fundamental rights violations. This research aims to answer what are the main social and legal risks of adopting these technologies in Brazilian public security,to critically analyze their use, evaluating their impacts on fundamental rights, to map operational facial recognition projects and available data on their application. The adopted methodology will be bibliographic and documentary. The research highlights the risks of exacerbating penal selectivity, with disproportionate impacts on vulnerable and marginalized groups.

KEYWORDS: Human Rights; Algorithmic discrimination; Facial recognition; Public security; Technology.

RESUMEN: El uso de tecnologías de reconocimiento facial en la seguridad pública brasileña se ha expandido rápidamente, con al menos 421 proyectos activos capaces de monitorear a 87,2 millones de personas, según el informe "Mapeando la Vigilancia Biométrica", elaborado por la Defensoría Pública de la Unión (DPU) en asociación con el Centro de Estudios de Seguridad y Ciudadanía (CESeC). Esta práctica refleja un escenario global, considerando que el 70% de las fuerzas policiales del mundo tienen acceso a algún tipo de tecnología de reconocimiento facial (Bischoff, 2021). Aunque las inversiones ya han superado los R$ 160 millones, el informe señala la ausencia de transparencia, la falta de evidencia de eficacia y la inexistencia de control público, factores que aumentan el riesgo de violaciones a los derechos fundamentales.El problema de investigación busca responder cuáles son los principales riesgos sociales y jurídicos de la adopción de estas tecnologías en la seguridad pública brasileña, analizar críticamente su uso evaluando sus impactos sobre los derechos fundamentales, además de mapear los proyectos de reconocimiento facial en operación y los datos disponibles sobre su aplicación. La metodología adoptada será bibliográfica y documental. La investigación apunta a los riesgos de agudización de la selectividad penal, con impactos desproporcionados sobre grupos vulnerables y marginados.

PALABRAS CLAVE: Derechos humanos; discriminacion algorítmica; reconocimiento facial; seguridad pública; tecnologia.

INTRODUÇÃO

> Art. 5º Para os fins desta Lei, considera-se:
>
> II- dado pessoal sensível: 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;

BRASIL, Lei nº 13.709, de 14 de agosto de 2018.

Vive-se, na atualidade, em uma sociedade da informação. As pessoas estão imersas em um ambiente de uso contínuo de diferentes tecnologias que estão em constante desenvolvimento. O acesso aos espaços e serviços digitais depende continuamente da disponibilização de dados pessoais. Nessa perspectiva, nota-se que esses dados têm sido utilizados por empresas e governos para diversas finalidades, a exemplo da segurança pública, em sentido amplo, que abarca tanto a persecução penal, atividade de investigação, quanto a segurança pública em sentido estrito, atividade de prevenção de crime[3].

O reconhecimento facial é uma tecnologia de identificação biométrica realizada a partir da coleta de dados faciais, que podem ser provenientes de fotografias ou segmentos de vídeos. Esses sistemas automatizados extraem representações matemáticas de traços específicos como, por exemplo, a distância entre os olhos ou o formato do nariz, produzindo o que é chamado de padrão facial. É justamente no processo de comparação desse padrão facial a outros padrões faciais contidos na base de dados prévia do sistema que a tecnologia identifica indivíduos desconhecidos,[4] e formam expressivos bancos de dados – big datas –que reúnem grandes volumes de dados biométricos, utilizados no processamento para identificação das pessoas.[5]

O cenário da segurança pública no Brasil, no que tange ao uso de tecnologias de reconhecimento facial, ecoa uma tendência global cada vez mais consolidada. A expansão acelerada dessas ferramentas em solo brasileiro se alinha com o que observamos internacionalmente, onde o reconhecimento facial tem se tornado uma peça central nas estratégias de policiamento.

[3] ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. Revista Brasileira de Segurança Pública, v. 16, n. 2, p. 264-283, 2022.
[4] KANASHIRO, Marta Mourão et al. Biometria no Brasil e o registro de identidade civil: novos rumos para a identificação. 2011. Tese de Doutorado. Universidade de São Paulo.
[5] COSTA, Ramon Silva; KREMER, Bianca. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. Revista Brasileira de Direitos Fundamentais & Justiça, v. 16, n. 1, 2022.

São crescentes os relatos de cidadãos presos, processados ou investigados com base em dados biométricos extraídos de bancos compartilhados entre diferentes instituições, sem critérios claros de acesso, revisão ou possibilidade de contestação. O reconhecimento facial, por sua vez, vem sendo empregado em espaços públicos e eventos de grande porte, suscitando debates sobre privacidade, segurança da informação, viés discriminatório e ausência de mecanismos eficazes de controle social.[6]

O presente artigo tem como objetivo oferecer um panorama sobre o uso do reconhecimento facial na segurança pública brasileira, analisando os valores investidos, o impacto sobre os direitos fundamentais e os desafios significativos quanto a precisão e segurança de grupos historicamente vulneráveis na sociedade, usando como texto base o relatório "Mapeando a Vigilância Biométrica" (DPU/CESeC).

Para elaboração desse relatório, a Defensoria Nacional de Direitos Humanos e do CESeC enviou às Secretarias de Segurança dos 26 estados da federação e do Distrito Federal ofícios que buscaram investigar e monitorar a adoção das TRF como política pública. Abrangendo aspectos relacionados à implementação dessas tecnologias, incluindo contratos firmados, empresas contratadas, orçamento envolvido em cada projeto, finalidades declaradas, medidas de proteção de dados sensíveis e mitigação de possíveis vieses discriminatórios.

O problema de pesquisa que orienta este estudo consiste em compreender quais são os principais riscos sociais e jurídicos associados à adoção de tecnologias de reconhecimento facial na segurança pública brasileira.

O objetivo geral é analisar criticamente o uso do reconhecimento facial no contexto da segurança pública nacional, com ênfase nos impactos sobre direitos

[6] DEFENSORIA PÚBLICA DA UNIÃO; CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA (CESeC). Mapeando a vigilância biométrica: relatório sobre uso de reconhecimento facial na segurança pública brasileira. Brasília: DPU; Rio de Janeiro: CESeC, 2024.

fundamentais, em especial o direito à privacidade, à não discriminação e à igualdade perante a lei. Como objetivos específicos, pretende-se: (i) mapear os projetos de reconhecimento facial em operação no Brasil, identificando sua distribuição geográfica, volume de investimento e finalidade declarada; (ii) examinar a base legal que autoriza ou limita seu uso; (iii) avaliar possíveis vieses algorítmicos e suas repercussões para a seletividade penal.

Metodologicamente, a pesquisa se vale de abordagem bibliográfica e documental, utilizando como principal referência o relatório *Mapeando a Vigilância Biométrica* (DPU/CESeC), complementado por legislação, jurisprudência e literatura acadêmica nacional e internacional.

O CENÁRIO DA VIGILÂNCIA BIOMÉTRICA NO BRASIL

> O videomonitoramento com software de reconhecimento facial tem recebido grande atenção de autoridades públicas, pesquisadores e organizações da sociedade civil. Entre 2018 e 2019, observou-se um aumento significativo nos casos de implementação dessa tecnologia por municípios e estados brasileiros e, com isso, uma maior preocupação com o modo como a tecnologia está sendo implementada e testada.
>
> INSTITUTO IGARAPÉ. *Videomonitoramento*[7].

A expansão das atividades de videomonitoramento urbano tem sido uma das principais respostas ao problema da violência na América Latina. Com frequência, essas tecnologias são utilizadas pelo setor público e ganham protagonismo na segurança pública. Nesse cenário, o discurso empregado é de que a sua utilização serve à prevenção ao crime quando empregada em conjunto com processos e práticas de policiamento[8].

Além do uso para monitoramento coletivo, o sistema de reconhecimento facial (RF) é capaz de identificar, seguir, destacar individualmente e rastrear indivíduos nos locais em que eles transitam, podendo, assim, exercer vigilância específica. A justificativa para sua implementação consiste na defesa da eficiência

[7] Ver infográfico em https://igarape.org.br/videomonitoramento-webreport/#publicacoes.
[8] REGULAÇÃO DO RECONHECIMENTO FACIAL NO SETOR PÚBLICO: avaliação de experiências internacionais. Disponível em https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf.

do sistema algorítmico, especialmente no que tange ao seu uso como suporte para o aprimoramento da vigilância social no âmbito da segurança pública[9].

Dados do projeto O Panóptico (CESeC) mostram que há 421 projetos ativos de reconhecimento para fins de segurança no Brasil, e aproximadamente 87,2 milhões de brasileiros estão potencialmente sob vigilância por câmeras de reconhecimento facial na segurança pública abrangendo todas as cinco regiões. No Centro-Oeste, há 93 projetos ativos, o Estado de Goiás é o estado com mais projetos ativos, 73 no total e cerca de 3 milhões de pessoas potencialmente vigiadas.[10]

O relatório "Mapeando a vigilância biométrica" evidenciou um movimento crescente na adoção da tecnologia, mas também desafios significativos quanto à transparência e à justificativa da implementação. Dos estados que responderam aos ofícios, 22% não enviaram informações detalhadas, o que impede um monitoramento adequado do uso de recursos públicos, enquanto quase 30% ainda avaliam a viabilidade do sistema sem um compromisso formal. A ausência de um padrão nacional de regulamentação amplia as preocupações sobre segurança de dados e proteção à privacidade, tornando essencial o debate sobre os impactos sociais da tecnologia.

Os investimentos em tecnologia de reconhecimento facial variam significativamente entre os estados, mas os valores disponíveis são apenas indicativos, podendo ser ainda maiores. Isso ocorre porque não foram enviados os contratos na íntegra, não há clareza se os montantes informados correspondem a valores anuais e alguns projetos não detalharam os investimentos realizados. Até o momento, mais de R$ 160 milhões já foram

[9] OLIVEIRA, Loryne Viana et al. Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil. **Revista Tecnologia e Sociedade**, v. 18, n. 50, p. 114-135, 2022.

[10] O PANÓPTICO. Monitoramento do uso de reconhecimento facial no Brasil. Disponível em:https://www.opanoptico.com.br/#regioes. Acessado em 28 de julho de 2025. Dado atualizado em 14/07/2025.

destinados para a implementação da tecnologia em diferentes unidades federativas.

A Bahia lidera os investimentos, com um contrato de aproximadamente R$ 66 milhões, enquanto o Pará alocou R$ 20 milhões para sistemas de monitoramento. Outros estados, como Piauí e Tocantins, também registram valores expressivos: R$ 33,6 milhões e R$ 15,8 milhões, respectivamente. Por outro lado, estados como Rio Grande do Sul e Rio de Janeiro não informaram valores exatos, enquanto Minas Gerais e Mato Grosso ainda estão em fase de planejamento, com orçamentos aprovados, mas sem implementação ativa.

Além disso, o relatório da DPU e CESeC destacou as lacunas observadas no processo de levantamento, como a ausência de resposta por parte de alguns estados, mesmo após sucessivas tentativas de contato. Essas omissões limitam a plena compreensão do cenário nacional, mas não impedem que as informações disponíveis sirvam como base para identificar pontos críticos e propor caminhos para a criação de protocolos e políticas que levem a uma governança que limite os potenciais ofensivos dessas tecnologias.

De fato, o Brasil não é uma ilha neste contexto. Globalmente, a adoção dessas tecnologias por parte das forças de segurança é um fenômeno notável. Conforme dados citados por Bischoff (2021), 70% das forças policiais do mundo já possuem acesso a algum tipo de tecnologia de reconhecimento facial. Essa estatística sublinha a amplitude e a relevância dessa ferramenta no panorama da segurança internacional, servindo como um paralelo direto para compreender a crescente implementação no contexto brasileiro. A comparação permite perceber que a corrida por cidades e ambientes mais "inteligentes" e monitorados, impulsionada pela promessa de maior eficácia na prevenção e combate ao crime, é uma realidade que transcende fronteiras.[11]

[11] BISCHOFF, Paul. Facial recognition technology (FRT): 100 countries analyzed, 8 June 2021.

DIREITOS FUNDAMENTAIS EM RISCO?

O uso crescente da tecnologia de reconhecimento facial, especialmente em ambientes públicos e por órgãos estatais, levanta preocupações sobre a violação de direitos fundamentais garantidos pela Constituição Federal. Embora a tecnologia possa ser apresentada como uma ferramenta para segurança e eficiência, seu emprego indiscriminado ou sem regulamentação adequada pode ferir a privacidade, a liberdade, o princípio da não discriminação e o devido processo legal.

Dentre os principais desafios está a violação da privacidade dos cidadãos, direito fundamental assegurado pelo Artigo 5º, inciso X, da Constituição Federal, que afirma: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"[12]. No que diz respeito ao uso de dados pessoais, as imagens podem ser coletadas e armazenadas sem o seu consentimento em bancos de dados de segurança pública. Essa coleta e o armazenamento de informações sensíveis podem propiciar o uso indevido desses dados, além de falta de transparência em relação a como e por quem essas informações são acessadas e utilizadas.[13]

Atrelado ao tema, está o princípio do devido processo legal, previsto no Artigo 5º, incisos LIV e LV, da Constituição Federal. O uso dos dados sensíveis em investigações criminais ou processos judiciais, especialmente sem transparência sobre a tecnologia empregada por trás dos algoritmos, sua acurácia e metodologia, pode comprometer esse direito fundamental, sobretudo

[12] BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm . Acesso em: 16 de outubro de 2025.

[13] PEREIRA, Sara Matias Ferrari; OLIVEIRA, Tarsis Barreto. O uso da inteligência artificial no direito penal e seus reflexos sobre os direitos fundamentais da não discriminação e da privacidade. Revista do Instituto de Direito Constitucional e Cidadania, v. 9, n. 1, p. e099-e099, 2024.

diante da impossibilidade de contestar a validade e os parâmetros do algoritmo, o que pode prejudicar o direito à ampla defesa.

A ausência de clareza sobre como esses dados são armazenados, por quanto tempo, com quem são compartilhados e para quais finalidades, agrava a violação. A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) também é diretamente afetada, pois o reconhecimento facial lida com dados pessoais sensíveis (dados biométricos), exigindo consentimento específico e finalidade determinada para seu tratamento.

Outro pilar da Constituição em risco é a liberdade, em suas diversas dimensões, consagrada no Artigo 5º, *caput*, e em vários de seus incisos, como o direito de ir e vir (inciso XV). A vigilância constante por meio do reconhecimento facial pode gerar um efeito inibidor na sociedade. Cidadãos podem se sentir vigiados e, por consequência, autocensurar-se em suas ações, associações ou manifestações públicas, por medo de serem identificados, monitorados ou incorrerem em alguma forma de punição ou vigilância indevida. Esse cenário mina a liberdade de expressão, de reunião e de associação, essenciais para uma democracia.

Outro princípio vinculado ao tema é o da não discriminação, garantido pelo Artigo 3º, inciso IV, da Constituição, que estabelece como objetivo fundamental da República "promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação". A literatura especializada demonstra que algoritmos de reconhecimento facial podem apresentar vieses raciais e de gênero, sendo menos precisos na identificação de pessoas negras, mulheres e outras minorias.[14] Considerando que o Brasil não dispõe de uma política pública especificamente voltada para o tema do viés algorítmico, surge a

[14] Coalizão Direitos na Rede (Brasil): Diversos materiais sobre vieses e o uso do reconhecimento facial no país. https://direitosnarede.org.br/. Acessado em 01 de agosto de 2025.

preocupação de como conferir eficácia ao texto constitucional e garantir a não-discriminação no uso da inteligência artificial.[15]

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, representa um marco regulatório fundamental no Brasil, estabelecendo regras claras sobre a coleta, armazenamento, tratamento e compartilhamento de dados pessoais. Para garantir a efetividade de suas disposições e coibir condutas que violem os direitos dos titulares de dados, a LGPD prevê um conjunto de sanções administrativas que podem ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD).

Entretanto, a incidência do tratamento dos dados pessoais prevista na lei se encontra restrita ao âmbito cível, uma vez que, conforme previsão do art. 4°, inc. III, da Lei Geral de Proteção de Dados, a regulamentação trazida pelo diploma legal é expressamente vedada na seara penal, a dispor: investigação, repressão de infrações penais e segurança pública[16].

> Art. 4º. Esta Lei não se aplica ao tratamento de dados pessoais:
> III - 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;
>
> BRASIL. (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

Diante do exposto, vários questionamentos são suscitados sobre se o RF é uma tecnologia adequada a espaços democráticos diante da iminente possibilidade de violações de direitos fundamentais. Sendo possível a implementação de RF no âmbito da segurança pública, surge um debate sobre as maneiras de regular o RF de forma a ser uma tecnologia útil e que sua

[15] CARVALHO, Allan Pereira de. Viés algorítmico e discriminação: possíveis soluções regulatórias para o Brasil. 2020.
[16] OLIVEIRA, Luiza Kimura Cardoso. Direito Penal Interconectado: Análise Do Sistema Penal Na Rede Mundial De Computadores. Persecução penal e proteção de dados: limites entre a mitigação do direito à privacidade virtual em face do interesse público criminal no ordenamento jurídico. In: VELOSO FILHO, José Carlos. Direito Penal e Processual Penal em perspectiva: contribuições crítico-reflexivas para o avanço do Sistema de Justiça Criminal.

implementação esteja direcionada para a proteção de dados pessoais dos titulares que cometeram crimes ou não.[17]

A percepção do público em relação ao uso do reconhecimento facial é um tema que varia significativamente entre diferentes grupos sociais. Enquanto alguns indivíduos expressam preocupações sérias sobre a invasão de privacidade, destacando o potencial para abusos e vigilância excessiva, outros acreditam fortemente que a tecnologia pode trazer benefícios significativos para a segurança pública e para a prevenção de crimes (Lima, 2023)[18].

Os problemas técnicos endêmicos presentes nos sistemas de reconhecimento facial significam que falsos positivos continuarão a ser um obstáculo comum no futuro, o que sem dúvidas traz diversos questionamentos em relação à proteção de direitos inalienáveis presentes na nossa Constituição federal .[19] Isso porque o sistema, embora se apresente como neutro e infalível, demonstra imprecisões técnicas que podem levar ao falso reconhecimento de pessoas, especialmente vinculadas a grupos vulneráveis.

Essas falhas podem representar uma ameaça não apenas à dignidade humana dos indivíduos, mas também ao próprio âmago moral dos que se tornam vítimas de uma tecnologia imprecisa. O reconhecimento facial é suscetível a riscos que requerem uma avaliação cuidadosa e abordagens éticas para garantir que seu uso não comprometa injustamente os direitos individuais e a integridade moral daqueles afetados por sua aplicação imprecisa.[20]

No Brasil, quando se fala de vigilância pública e, consequentemente, em políticas criminais adotadas pelo Estado, é impossível deixar de falar sobre

[17] ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. Revista Brasileira de Segurança Pública, v. 16, n. 2, p. 264-283, 2022.
[18] *Apud* REIS, Sálvio Roberto Freitas. Desafios no uso de reconhecimento facial em sistemas de vídeo monitoramento no Brasil. Pag. 32, 2025.
[19] LIMA, Dayana dos Santos. Relação entre o reconhecimento facial e a sua responsabilidade jurídica: a luz dos direitos humanos essa tecnologia pode vir a enlear a dignidade humana? 2023.
[20] LIMA, Dayana dos Santos. Relação entre o reconhecimento facial e sua responsabilidade jurídica: a luz dos direitos humanos essa tecnologia pode vir a enlear a dignidade humana? Pag.24, 2023.

racismo e a seletividade do sistema penal no país. Amplamente baseado na busca por um determinado tipo criminoso e ainda com grande carga de preconceito racial deixada como marca dos tempos de escravidão, o sistema penal no Brasil atualmente afeta consideravelmente mais pessoas negras do que brancas[21]. Nesse sentido, a implementação de tecnologias de vigilância na segurança pública afeta desproporcionalmente a clientela preferencial do sistema punitivo.

De fato, o racismo algorítmico se manifesta quando as práticas contemporâneas de organização e classificação da informação em grandes conjuntos de dados geram resultados que produzem e disseminam desigualdades racistas, fortalecendo a opressão sobre pessoas negras e suas comunidades.[22]

DISCRIMINAÇÃO ALGORÍTMICA E SELETIVIDADE PENAL

A crescente integração de algoritmos nos sistemas de justiça criminal ao redor do mundo, embora prometa eficiência e imparcialidade, tem levantado sérias preocupações sobre a discriminação algorítmica e a consequente seletividade penal. A realidade é que essas ferramentas digitais frequentemente replicam e amplificam preconceitos sociais já existentes, impactando desproporcionalmente grupos minoritários. A idealizada "justiça cega" é obscurecida pelo fato de que os dados que alimentam esses algoritmos são produtos de um histórico de desigualdades sociais e sistêmicas[23].

As imprecisões algorítmicas se manifestam de diversas formas. Essa situação é frequentemente observada em relação a indivíduos pertencentes a comunidades negras, uma vez que as ferramentas de reconhecimento facial

[21] SILVA, R. L. D., & SILVA, F. D. S. R. D. (2019). Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. In *Congresso Internacional de Direito e Contemporaneidade, Santa Maria, RS, Brasil* (Vol. 5).

[22] COIMBRA, Jéssica Pérola Melo et al. Interseções entre racismo algorítmico, reconhecimento facial e segurança pública no Brasil. Revista Jurídica do Cesupa, v. 4, n. 2, p. 136-160, 2023.

[23] O'NEIL, Cathy. *Armas de Destruição Matemática: Como o Big Data Aumenta a Desigualdade e Ameaça à Democracia.*

tendem a apresentar taxa de falha desproporcional em relação a essa população.[24] Essa superestimação pode resultar em fianças mais altas, períodos de prisão preventiva mais longos e penas mais severas, mesmo quando não há evidências concretas que justifiquem tal disparidade. Mulheres também podem ser alvo de vieses, seja na avaliação de risco de violência doméstica ou em decisões sobre guarda de filhos, onde estereótipos de gênero podem influenciar as previsões dos algoritmos.[25]

Um dos principais problemas reside nos vieses inerentes aos dados de treinamento. Se um algoritmo é alimentado com um histórico de prisões e condenações que reflete a seletividade já presente no sistema penal – onde, por exemplo, indivíduos negros são desproporcionalmente detidos e condenados por crimes que outros grupos cometem com frequência similar –, ele aprenderá a associar certas características demográficas a um maior "risco" de criminalidade. Isso cria um ciclo vicioso: o algoritmo classifica erroneamente certos grupos como de alto risco, levando a um policiamento mais ostensivo e a sentenças mais severas para esses indivíduos, o que, por sua vez, gera mais dados enviesados para as futuras interações do algoritmo.[26]

É crucial reconhecer que a inteligência artificial não é intrinsecamente neutra. Ela reflete as escolhas de design, os dados utilizados e as prioridades dos seus criadores. A falta de transparência em muitos desses sistemas, que operam como "caixas pretas", dificulta a identificação e correção desses vieses.[27] A compreensão da seletividade penal demanda uma análise que transcende os

[24] LIMA, Dayana dos Santos. Relação entre o reconhecimento facial e a sua responsabilidade jurídica: a luz dos direitos humanos essa tecnologia pode vir a enlear a dignidade humana? Pag. 25, 2023.
[25] BAROCAS, Solon; SELBST, Andrew D. "Big Data's Disparate Impact." California Law Review, vol. 104, no. 3, 2016, pp. 671-730
[26] BENJAMIN, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*.
[27] PASQUALE, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information.*

aspectos meramente jurídicos, adentrando as dimensões históricas e sociais que sustentam práticas discriminatórias enraizadas no sistema penal brasileiro.[28]

Os bancos de dados de suspeitos usados no comparativo podem apresentar viés racial diante da problemática da seletividade notória contra pessoas negras no sistema penal brasileiro. As operações policiais movidas por um "sistema de caça de suspeitos", turbinadas pela tecnologia, podem atingir pessoas que sequer têm ciência de que estão sendo perseguidas até a abordagem policial, pois identificado o erro do sistema a ação é finalizada e sem registro de ocorrência. Assim, depreende-se como a falta de transparência retira a credibilidade das medidas de segurança pública principalmente envolvendo tecnologias, uma vez que os dados são essenciais para a criação de uma política pública, pois constituem a base de sua formulação e execução precisa[29].

Um caso expressivo de injustiça foi o do pedreiro José Domingos Leitão em dezembro de 2021, no Piauí, acordado por policiais civis durante a madrugada com gritos e chutes na porta de sua casa, após um programa de reconhecimento facial confundi-lo com o autor de um crime, que não cometeu, na cidade de Brasília, aproximadamente 1.200 quilômetros de distância de onde reside (R7, 2021).

Tanto o autor do crime quanto José tinham um elemento em comum: eram homens negros. Os vieses raciais contidos nos algoritmos de reconhecimento facial ganham outros contornos no campo da segurança pública. E as condições atuais de produção, armazenamento e atualização das bases de dados desses sistemas pelo setor público são uma verdadeira caixa preta. Somado a isso, no contexto regulatório brasileiro, ainda não existe uma legislação

[28] NUNES, Ámon Gabriel Guimarães et al. A seletividade penal e o encarceramento em massa no brasil: Criminal selectivity and mass incarceration in brazil. RCMOS-Revista Científica Multidisciplinar O Saber, v. 1, n. 1, 2025.
[29] LIMA, Bruna Dias Fernandes. Racismo algorítmico: o enviesamento tecnológico e o impacto aos direitos fundamentais no Brasil. Pag. 45,2022.

que regulamente o uso de reconhecimento facial e outras técnicas de inteligência artificial.[30]

No Brasil, de acordo com o relatório "Mapeando a Vigilância Biométrica", as investigações indicam que mais da metade das abordagens policiais motivadas por reconhecimento facial resultaram de identificações equivocadas, evidenciando o risco de prisões indevidas e reforço de padrões históricos de seletividade penal.

Apesar dos casos que podem ser vistos como positivos para a segurança pública e investigação criminal, as tecnologias de reconhecimento facial possuem uma face nebulosa em sua aplicação no Brasil, que antecede a própria tecnologia, o racismo. Não são raros os casos de pessoas inocentes sendo presas por crimes que não cometeram.

O problema é que as máquinas utilizadas no reconhecimento facial carregam as percepções de quem as produzem e do tratamento fornecido aos bancos de dados que as alimentam. Portanto, há grandes chances de erros como esses se tornarem mais comuns por meio do reconhecimento facial. Isso porque existem questões estruturais sobre como a sociedade e o Estado leem quem são os indivíduos que devem ser vigiados, perseguidos, ou seja, sobre quem são as pessoas que oferecem perigo e devem ser detidas.[31]

Diante desse cenário, torna-se imperativo questionar o entusiasmo acrítico com que tecnologias de reconhecimento facial e outros sistemas algorítmicos vêm sendo incorporados às práticas de segurança pública e justiça criminal. Sem mecanismos robustos de transparência, auditoria independente e controle social, tais ferramentas correm o risco de perpetuar e até aprofundar desigualdades históricas, travestindo discriminação de neutralidade tecnológica. A promessa de

[30] COSTA, Ramon Silva; KREMER, Bianca. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. Revista Brasileira de Direitos Fundamentais & Justiça, v. 16, n. 1, 2022.
[31] COSTA, Ramon Silva; KREMER, Bianca. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. Revista Brasileira de Direitos Fundamentais & Justiça, v. 16, n. 1, 2022.

eficiência e precisão não pode se sobrepor à necessidade de garantir direitos fundamentais e preservar a dignidade humana. Em última instância, a adoção indiscriminada dessas tecnologias, sem regulamentação específica e salvaguardas efetivas, compromete não apenas a legitimidade do sistema penal, mas também o próprio ideal democrático que deveria orientá-lo.

CONCLUSÃO

O presente estudo teve como objetivo analisar criticamente o uso de tecnologias de reconhecimento facial na segurança pública brasileira, à luz de seu potencial impacto sobre direitos fundamentais e da possibilidade de acirramento da seletividade penal. A pesquisa, de natureza bibliográfica e documental, identificou que a implementação dessa tecnologia no país ocorre de forma acelerada, com mais de 421 projetos ativos, mas carece de transparência, regulamentação específica e mecanismos de controle social adequados.

Os resultados apontam que, embora apresentadas como instrumentos de eficiência na prevenção e repressão de crimes, as tecnologias de reconhecimento facial, quando aplicadas sem salvaguardas normativas e técnicas, tendem a reproduzir e amplificar desigualdades históricas, atingindo de forma desproporcional grupos vulnerabilizados, especialmente pessoas negras. Ademais, constatou-se a inexistência de evidências empíricas consistentes que demonstrem a efetividade da ferramenta na redução da criminalidade, o que reforça a necessidade de avaliações rigorosas antes de sua adoção em larga escala.

Como limitação, destaca-se a restrição dos dados disponíveis, decorrente tanto da opacidade na gestão pública quanto da ausência de padronização nas informações fornecidas pelos órgãos de segurança. Essa limitação reforça a urgência de maior transparência e de auditorias independentes para aferir a acurácia e a confiabilidade dos sistemas.

Conclui-se que a incorporação do reconhecimento facial à segurança pública brasileira deve estar condicionada ao cumprimento estrito dos princípios de legalidade, proporcionalidade e necessidade, aliados à proteção de dados pessoais sensíveis e à mitigação de vieses discriminatórios.

REFERÊNCIAS

ALMEIDA, Eduarda Costa. **Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal.** Revista Brasileira de Segurança Pública, v. 16, n. 2, p. 264-283, 2022.

BAROCAS, Solon; SELBST, Andrew D. **"Big Data's Disparate Impact."** California Law Review, vol. 104, no. 3, 2016, p. 671-730.

BISCHOFF, Paul. **Facial recognition technology (FRT):** 100 countries analyzed, 8 June 2021. Disponível em: https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/. Acesso em: 24 mar. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 jul. 2025.

CARVALHO, Allan Pereira de. **Viés algorítmico e discriminação:** possíveis soluções regulatórias para o Brasil. (Trabalho de Conclusão de Curso de Graduação) - Universidade Federal do Rio Grande do Sul. Faculdade de Direito. Curso de Ciências Jurídicas e Sociais, 2020.

Coalizão Direitos na Rede (Brasil): **Diversos materiais sobre vieses e o uso do reconhecimento facial no país.** https://direitosnarede.org.br/ . Acessado em 01 ago. 2025.

COIMBRA, Jéssica Pérola Melo et al. **Interseções entre racismo algorítmico, reconhecimento facial e segurança pública no Brasil.** Revista Jurídica do Cesupa, v. 4, n. 2, p. 136-160, 2023.

COSTA, Ramon Silva; KREMER, Bianca. **Inteligência artificial e discriminação:** desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. Revista Brasileira de Direitos Fundamentais & Justiça, v. 16, n. 1, 2022.

DEFENSORIA PÚBLICA DA UNIÃO; Centro De Estudos De Segurança E Cidadania (CESeC). **Mapeando a vigilância biométrica:** relatório sobre uso de reconhecimento facial na segurança pública brasileira**.** Brasília: DPU; Rio de Janeiro: CESeC, 2024. Disponível em: https://direitoshumanos.dpu.def.br/relatorio-da-dpu-e-cesec-alerta-para-riscos-do-reconhecimento-facial-na-seguranca-publica/. Acesso em: 9 maio 2025.

FRANCISCO, Pedro Augusto P; HUREL, Louise Marie; RIELLI, Mariana Marques. "**Regulação Do Reconhecimento Facial No Setor Público:** avaliação de experiências internacionais". In: *https://igarape.org.br/.* Disponível em: (https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-egula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf). Acesso em 17 jul. 2025.

LIMA, Bruna Dias Fernandes. **Racismo algorítmico:** o enviesamento tecnológico e o impacto aos direitos fundamentais no Brasil. Dissertação (mestrado em Direito) – Universidade Federal de Sergipe, 2022.

LIMA, Dayana dos Santos. **Relação entre o reconhecimento facial e a sua responsabilidade jurídica:** a luz dos direitos humanos essa tecnologia pode vir a enlear a dignidade humana?, 2023.

LIMA, Leonardo Bruscagini de. **Detecção De Anomalias Em Tempo De Resposta De Servidores Web:** Uma Abordagem Automatizada Para Aprimorar A Segurança E A Eficiência. Tese (Doutorado) — Dissertação de Engenharia Elétrica e de Computação 2023.

MAINERI, Julia Chassot Loureiro. **Responsabilização civil na discriminação algorítmica racial na tomada de decisões automatizadas.** (Trabalho de Conclusão de Curso) - Faculdade de Direito da Universidade Federal do Rio Grande do Sul. 2024.

MELO, Rafael Augusto de Almeida. **A LGPD no cenário digital:** os impactos da Lei Geral de Proteção de Dados. SciELO, 2019. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/. Acesso em: 22 jul. 2025.

O PANÓPTICO. **Monitoramento do uso de reconhecimento facial no Brasil.** Disponível em:https://www.opanoptico.com.br/#regioes. Acessado em 28 de julho de 2025. Dado atualizado em 14/07/2025.

OLIVEIRA, Loryne Viana et al. **Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil.** Revista Tecnologia e Sociedade, v. 18, n. 50, p. 114-135, 2022.

OLIVEIRA, Luiza Kimura Cardoso. **Direito Penal Interconectado: Análise Do Sistema Penal Na Rede Mundial De Computadores. Persecução penal e proteção de dados:** limites entre a mitigação do direito à privacidade virtual em face do interesse público criminal no ordenamento jurídico. In: VELOSO FILHO, José Carlos. **Direito Penal e Processual Penal em perspectiva**: contribuições crítico-reflexivas para o avanço do Sistema de Justiça Criminal – Brasília: CEUB, 2025.

PASQUALE, Frank. **The black box society: The secret algorithms that control money and information**. Harvard University Press, 2015.

PEREIRA, Sara Matias Ferrari; OLIVEIRA, Tarsis Barreto. **O uso da inteligência artificial no direito penal e seus reflexos sobre os direitos fundamentais da não discriminação e da privacidade.** Revista do Instituto de Direito Constitucional e Cidadania, v. 9, n. 1, p. e099-e099, 2024.

REIS, Sálvio Roberto Freitas. **Desafios no uso de reconhecimento facial em sistemas de vídeo monitoramento no Brasil.** (Dissertação de Mestrado) - Universidade Federal De Sergipe, Centro De Ciências Exatas e Tecnologia, 2025.

SILVA, Rosane Leal da; SILVA, Fernanda dos Santos Rodrigues da. **Reconhecimento facial e segurança pública:** os perigos do uso da tecnologia no sistema penal seletivo brasileiro. In: Congresso Internacional de Direito e Contemporaneidade, Santa Maria, RS, Brasil. 2019.