
**O RECONHECIMENTO FACIAL NO SISTEMA PENAL BRASILEIRO: UMA
ANÁLISE SOBRE OS RISCOS DE PRISÕES INDEVIDAS E DISCRIMINAÇÃO
RACIAL**

**FACIAL RECOGNITION IN THE BRAZILIAN CRIMINAL JUSTICE SYSTEM: AN
ANALYSIS OF THE RISKS OF WRONGFUL ARRESTS AND RACIAL
DISCRIMINATION**

Kesia Santos Moreira¹
Shibelly Alves Correia²
Su Ellen Fernandes Ferraz³

Orientador: Prof. Dr. Williem da Silva Barreto Junior⁴

RESUMO

As inovações no campo da vigilância tecnológica têm alterado de maneira significativa a dinâmica da segurança pública e a interação entre o Estado e os cidadãos. O presente trabalho tem como tema o uso do reconhecimento facial no sistema penal brasileiro, com enfoque nos riscos e nas consequências jurídicas e sociais decorrentes de sua aplicação. O objetivo geral consiste em analisar criticamente essa tecnologia, identificando suas limitações técnicas, a relação com o racismo estrutural e os impactos nos direitos fundamentais, como a liberdade, a dignidade da pessoa humana e a presunção de inocência. Entre os objetivos específicos destacam-se a análise do funcionamento técnico dos sistemas, a investigação de casos concretos de prisões indevidas, a avaliação da responsabilidade do Estado e a discussão da compatibilidade do reconhecimento facial com os princípios constitucionais. A pesquisa apresenta natureza exploratória, descritiva e qualitativa, fundamentada em análise documental e de conteúdo. Foram considerados a legislação brasileira, jurisprudências, relatórios de organizações de direitos humanos e estudos de caso divulgados pela mídia. Os resultados indicam que o reconhecimento facial, quando aplicado de maneira acrítica e sem regulamentação específica, ocasiona erros graves, sobretudo em razão de vieses algorítmicos que atingem desproporcionalmente a população negra e reforçam a seletividade penal. Conclui-se que, embora a tecnologia possa oferecer potencial contribuição à segurança pública, seu uso atual no Brasil compromete garantias constitucionais, viola direitos fundamentais e exige regulamentação rigorosa, de

¹ Discente do curso de Direito do Centro de Excelência em Ensino Jurídico UNEX de Vitória da Conquista – BA (UNEX/BA), e-mail: kesiamoreira77@gmail.com.

² Discente do curso de Direito do Centro de Excelência em Ensino Jurídico UNEX de Vitória da Conquista – BA (UNEX/BA), e-mail: shibellycorreia@hotmail.com.

³ Discente do curso de Direito do Centro de Excelência em Ensino Jurídico UNEX de Vitória da Conquista – BA (UNEX/BA), e-mail: suferrazadv@gmail.com.

⁴ Professor Orientador do curso de Direito do Centro de Excelência em Ensino Jurídico UNEX de Vitória da Conquista – BA (UNEX/BA), e-mail: williem.junior@ftc.edu.br

modo a resguardar o Estado Democrático de Direito e a proteção contra práticas discriminatórias.

Palavras chave: Reconhecimento facial. Sistema penal. Racismo estrutural. Direitos fundamentais.

ABSTRACT

Innovations in technological surveillance have significantly altered the dynamics of public security and the interaction between the State and its citizens. This study focuses on the use of facial recognition in the Brazilian criminal justice system, emphasizing the risks and the legal and social consequences arising from its application. The general objective is to critically analyze this technology, identifying its technical limitations, its relation to structural racism, and its impacts on fundamental rights, such as liberty, human dignity, and the presumption of innocence. Specific objectives include analyzing the technical functioning of the systems, investigating concrete cases of wrongful arrests, assessing state responsibility, and discussing the compatibility of facial recognition with constitutional principles. The research is exploratory, descriptive, and qualitative in nature, based on documentary and content analysis. Brazilian legislation, case law, human rights organization reports, and media-reported case studies were considered. The results indicate that facial recognition, when applied uncritically and without specific regulation, causes serious errors, particularly due to algorithmic biases that disproportionately affect the Black population and reinforce penal selectivity. It is concluded that, although the technology has potential contributions to public security, its current use in Brazil compromises constitutional guarantees, violates fundamental rights, and requires strict regulation to safeguard the Rule of Law and protection against discriminatory practices.

Keywords: Facial recognition. Criminal justice system. Structural racism. Fundamental rights.

1. INTRODUÇÃO

O avanço tecnológico redefiniu as formas de controle social e de produção de prova no direito penal contemporâneo. Entre as inovações mais debatidas está o reconhecimento facial, ferramenta baseada em algoritmos de inteligência artificial destinada à identificação de pessoas por meio de características biométricas. Essa tecnologia, difundida por promessas de eficiência e segurança, tem sido incorporada a práticas policiais e judiciais sem um marco normativo sólido, o que suscita questionamentos sobre violação de direitos fundamentais e reprodução de desigualdades raciais.

Dessa forma, ao serem inseridas em um contexto permeado por desigualdade e seletividade penal, as tecnologias de vigilância, em vez de promover

justiça, acabam por espelhar os vieses estruturais que moldam a sociedade. Essa constatação torna-se ainda mais grave quando se observa que o reconhecimento facial opera com base em bancos de dados e parâmetros técnicos construídos sob lógicas eurocêntricas, frequentemente excludentes para corpos negros e periféricos. A promessa de neutralidade técnica se dissolve diante das evidências empíricas. Estudos como o de Buolamwini e Gebru (2018)⁵ demonstram que algoritmos de reconhecimento facial apresentam maior taxa de erro na identificação de pessoas negras e de mulheres, fenômeno que o pesquisador brasileiro Tarcízio Silva (2022) denomina racismo algorítmico.

Em contexto nacional, essa problemática assume contornos dramáticos. Casos de prisões injustas baseadas em reconhecimento facial, como os registrados no Rio de Janeiro e na Bahia entre 2022 e 2025, evidenciam a ausência de critérios técnicos e de controle judicial efetivo. Tais episódios indicam que o sistema penal, longe de se modernizar de maneira igualitária, reforça a seletividade racial que historicamente o caracteriza. Conforme destaca Michelle Alexander (2017), a seletividade não é mero desvio, mas elemento essencial de um modelo penal que criminaliza a juventude negra e pobre.

A relevância deste estudo decorre da necessidade de reavaliar a compatibilidade entre inovação tecnológica e princípios constitucionais. A Constituição Federal de 1988 consagra como fundamentos da República a dignidade da pessoa humana, a igualdade e o devido processo legal, princípios que se mostram tensionados pela aplicação desregulada de sistemas algorítmicos. A ausência de regulamentação específica, somada à limitação da Lei 13.709/2018 (LGPD) no âmbito penal, cria zonas de incerteza jurídica e vulnerabilidade social.

Além dos riscos técnicos, a questão adquire dimensão epistemológica. A crítica de Lélia Gonzalez (1988) à hegemonia eurocêntrica do pensamento ocidental e sua defesa da amefricanidade, permite compreender como a tecnologia reproduz padrões de exclusão cognitiva. A contribuição de Livia Santana Vaz (2022) reforça essa leitura ao afirmar que a igualdade racial deve ser compreendida como processo ativo de reconstrução institucional, que exige o enfrentamento dos dispositivos de

⁵ BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, 2018. O estudo revelou o viés algorítmico em sistemas de reconhecimento facial, com erros de até 34,7% para mulheres negras e 0,8% para homens brancos, fenômeno denominado por Buolamwini de *Coded Gaze*.

poder que naturalizam a inferiorização racial. A interseção entre tecnologia e raça, portanto, impõe ao direito penal o desafio de reformular seus paradigmas probatórios para garantir efetividade aos direitos humanos.

A partir dessas premissas, o problema de pesquisa formulado é o seguinte: Como o uso do reconhecimento facial no sistema penal brasileiro contribui para a manutenção de práticas discriminatórias e para a ocorrência de prisões indevidas, especialmente de pessoas negras, e quais são as consequências jurídicas, constitucionais e sociais desse fenômeno?

A justificativa do estudo repousa sobre três eixos principais: constitucional, social e científico. No plano constitucional, impõe-se a reflexão sobre o equilíbrio entre segurança pública e direitos fundamentais, especialmente a liberdade e a dignidade da pessoa humana. No plano social, destaca-se a urgência de enfrentar as dinâmicas de exclusão racial que atravessam o sistema penal e se reproduzem nas novas tecnologias. E, no plano científico, o trabalho busca preencher lacuna teórica existente entre o campo jurídico e as ciências da computação, contribuindo para uma leitura interdisciplinar do fenômeno.

O objetivo geral consiste em analisar criticamente a utilização do reconhecimento facial no sistema penal brasileiro, investigando suas limitações técnicas e os impactos sobre a igualdade racial e os direitos fundamentais. A pesquisa utilizada no desenvolvimento deste artigo apresenta natureza exploratória, descritiva e qualitativa, adequada à análise crítica de um fenômeno contemporâneo ainda em consolidação normativa.

A abordagem exploratória permitiu delinear as principais dimensões do problema e identificar lacunas teóricas e legislativas sobre o uso do reconhecimento facial no sistema penal brasileiro. O caráter descritivo possibilitou sistematizar dados e casos concretos relacionados a prisões indevidas e erros de identificação. Já a abordagem qualitativa favoreceu a interpretação dos significados sociais e jurídicos subjacentes à aplicação da tecnologia, priorizando a compreensão crítica dos discursos e práticas institucionais.

Por fim, o artigo organiza-se em três seções principais: a primeira aborda os resultados e discussões, divididos em subcapítulos que tratam da técnica do reconhecimento facial, do racismo algorítmico, das garantias fundamentais e das propostas de regulação; e, por último, são apresentadas as considerações finais,

nas quais se sintetizam as conclusões e se reafirma a necessidade de controle ético e jurídico das tecnologias de vigilância.

1.2 METODOLOGIA

A coleta de dados ocorreu por meio de pesquisa documental e bibliográfica, realizada entre janeiro e agosto de 2025. Foram examinadas legislações nacionais (Constituição Federal de 1988, Código de Processo Penal, Lei 12.037/2009, Lei 13.709/2018 - LGPD, e Resolução CNJ nº 484/2022), bem como jurisprudências recentes do Superior Tribunal de Justiça (2024–2025) que trataram da nulidade de reconhecimentos fotográficos e faciais. Também foram analisados relatórios de organizações internacionais, como Human Rights Watch (2021) e Anistia Internacional (2023), estudos técnicos de universidades e publicações científicas de autores das áreas do Direito, Sociologia, Comunicação e Estudos de Vigilância.

As fontes jornalísticas utilizadas referem-se a casos amplamente noticiados de prisões injustas envolvendo reconhecimento facial, com verificação cruzada em diferentes veículos de comunicação para evitar distorções. Como instrumento de análise, aplicou-se o método de análise de conteúdo, conforme preconizado por Bardin (2011), que permite identificar padrões de sentido, recorrências temáticas e categorias interpretativas a partir do corpus documental. Essa técnica foi essencial para observar como os discursos institucionais e midiáticos sobre eficiência tecnológica ocultam as dimensões de racismo estrutural e seletividade penal. A triangulação entre dados normativos, empíricos e teóricos reforçou a validade interna do estudo.

A pesquisa ainda se insere em uma perspectiva interdisciplinar, situando-se entre o Direito Constitucional, o Direito Penal e os Estudos Críticos da Tecnologia. Essa opção metodológica decorre do reconhecimento de que o fenômeno analisado ultrapassa o campo jurídico tradicional, exigindo o diálogo com a sociologia do racismo, a filosofia da técnica e as epistemologias negras. Assim, a metodologia adotada buscou não apenas descrever a aplicação da tecnologia, mas compreender suas implicações éticas e políticas, evidenciando as tensões entre modernização tecnológica e os princípios do Estado Democrático de Direito.

2. A TECNOLOGIA DO RECONHECIMENTO FACIAL E O MITO DA NEUTRALIDADE

Atrelada ao preceito constitucional de que a segurança pública é um dever do Estado, é importante reconhecer que, atualmente, a tecnologia tornou-se parte integrante da vida cotidiana, sendo progressivamente incorporada aos instrumentos jurídicos e às práticas estatais. Um dos exemplos mais recentes dessa integração é o uso do reconhecimento facial, presente tanto em dispositivos pessoais, como celulares, quanto em iniciativas governamentais voltadas para a segurança e a prevenção de crimes.

Embora seu uso tenha se popularizado apenas nas últimas décadas, o reconhecimento facial é uma tecnologia que remonta aos anos 1960. Desenvolvida inicialmente por Woodrow Wilson Bledsoe, matemático e cientista da computação, a técnica consistia no mapeamento manual de cerca de vinte características faciais distintas, registradas em computadores rudimentares da época, conforme descrito no artigo A Facial Recognition Project Report (1963). Bledsoe cunhou o termo “mask” (máscara) para referir-se ao conjunto de medidas faciais únicas de cada indivíduo, que, ao serem armazenadas, permitiam a comparação entre rostos diferentes.

Com o avanço tecnológico, especialmente com a popularização de câmeras digitais e sistemas tridimensionais, o reconhecimento facial foi aperfeiçoado. Atualmente, são analisados de 80 a 150 pontos nodais de uma face, captados eletronicamente e processados por algoritmos sofisticados, para criar um “modelo matemático” de identidade. Essas informações são então organizadas em um “template”, modernização do conceito original da “mask”, que é confrontado em tempo real com registros armazenados em bases de dados públicas e privadas.

O funcionamento do reconhecimento facial baseia-se, portanto, na submissão de imagens a complexos algoritmos que identificam características únicas de cada rosto. Quando uma pessoa é capturada por uma câmera, o sistema busca, em alta velocidade, correspondências entre os pontos faciais coletados e aqueles armazenados previamente. Dependendo do software utilizado, diferentes graus de sofisticação podem ser empregados, envolvendo tecnologias como inteligência artificial, *machine learning*, automação e análise de *big data*. (Ramos, 2021)

Um aspecto importante a ser destacado é que, diferentemente de métodos biométricos como a leitura de impressões digitais ou da íris, o reconhecimento facial pode ser realizado de maneira não consentida, muitas vezes sem que o indivíduo sequer saiba que está sendo identificado. Esse método possibilita a varredura simultânea de múltiplos rostos em ambientes públicos, o que potencializa preocupações relativas à privacidade. (Requião, [2025?]. Texto não publicado. Documento obtido em acervo pessoal do autor.)

À primeira vista, o reconhecimento facial pode parecer uma ferramenta neutra e eficiente. Contudo, pesquisas recentes têm evidenciado problemas graves associados à sua aplicação. Estudos apontam que a falta de transparência dos sistemas, somada à opacidade dos algoritmos, dificulta a avaliação de sua eficácia e conformidade com os direitos fundamentais. Além disso, há relatos de altas taxas de falsos positivos, especialmente relacionados a vieses algorítmicos que refletem preconceitos sociais pré-existent. Esses erros não são meramente técnicos, tendo em vista que podem resultar em constrangimentos públicos, prisões injustas e outras formas de violação de direitos humanos fundamentais. (Requião, [2025?]. Texto não publicado. Documento obtido em acervo pessoal do autor.)⁶

A inteligência artificial (IA) tem sido incorporada em diferentes setores ao redor do mundo, apresentando resultados significativos e positivos em diversas áreas. No entanto, também se multiplicam os estudos que alertam para falhas, vieses e equívocos advindos da utilização dessas tecnologias, apontando, inclusive, para violações de direitos humanos e ameaças ao regime democrático em vários países. (Rocha, 2025)

Um dos campos que mais tem gerado preocupações é o reconhecimento facial, especialmente quando aplicado no âmbito do Direito Penal, para a identificação de indivíduos supostamente foragidos do sistema prisional. A experiência prática demonstra que o uso da IA nesse contexto não está isento de problemas sérios, que vão desde erros de identificação até abordagens discriminatórias. No contexto jurídico, sua aplicação no sistema penal brasileiro carece de regulamentação específica, sendo pautada por políticas locais e por contratos firmados com empresas de tecnologia, frequentemente sem transparência

⁶ O artigo foi gentilmente disponibilizado pelo autor, Luis Henrique Requião, professor do Curso de Direito da rede UniFTC, a partir de seu acervo pessoal, não tendo sido ainda publicado em periódico ou repositório institucional.

pública. Tal cenário contrasta com o princípio da legalidade estrita, que rege o processo penal e exige base normativa para a limitação de direitos fundamentais.

Dentre as formas de discriminação associadas ao uso da IA, destaca-se o chamado racismo algorítmico, fenômeno em que preconceitos estruturais da sociedade são, consciente ou inconscientemente, reproduzidos e potencializados pelos algoritmos. Ainda que muitas vezes esse viés se manifeste de forma não intencional, seus impactos são profundamente danosos, reforçando desigualdades e afetando de maneira desproporcional grupos historicamente marginalizados. (Rocha, 2025)

A literatura especializada em estudos da vigilância, representada por David Lyon (2018), alerta que a expansão de tecnologias de controle cria uma “sociedade da vigilância” na qual a coleta e o cruzamento de dados tornam-se mecanismos permanentes de governo das populações. O autor observa que, em regimes democráticos, a vigilância tende a se justificar pela promessa de segurança, mas frequentemente resulta em formas sutis de controle social e exclusão.

Esse fenômeno é ampliado pelo que Shoshana Zuboff (2020) denominou capitalismo de vigilância: um modelo econômico baseado na extração e comercialização de dados pessoais. Na esfera penal, esse modelo se manifesta quando o Estado delega a empresas privadas o processamento de dados biométricos, convertendo a identidade cidadã em mercadoria. A ausência de regulação efetiva expõe a população a um duplo risco: o da violação da privacidade e o da criminalização algorítmica.

Em tese, o reconhecimento facial apresenta vantagens operacionais, como a rapidez na identificação de suspeitos. No entanto, os estudos técnicos do Instituto Nacional de Padrões e Tecnologia (NIST Interagency Report 8280 – 2019 - e NIST Interagency Report 8429 - 2022) demonstram que as taxas de erro aumentam significativamente em imagens com baixa resolução, iluminação precária ou rostos com características fenotípicas distintas das usadas no treinamento do algoritmo, condições comuns em câmeras de segurança urbanas no Brasil.

Além da falta de transparência, há uma assimetria de poder evidente. Enquanto as empresas que desenvolvem esses sistemas detêm o conhecimento técnico e os bancos de dados, os indivíduos submetidos à vigilância não têm acesso a informações sobre como suas imagens são coletadas e utilizadas. Tal desequilíbrio afronta o princípio da autodeterminação informativa, previsto

implicitamente na Lei Geral de Proteção de Dados (LGPD) e reforçado pela doutrina de Danilo Doneda (2019).

O caráter político do reconhecimento facial também se manifesta na forma como ele seleciona corpos e territórios. As políticas de segurança que utilizam essa tecnologia concentram-se, majoritariamente, em áreas urbanas periféricas e em grandes eventos populares, refletindo uma geografia do controle marcada pela cor e pela classe. Essa constatação corrobora o argumento de que a tecnologia, ao contrário do que se alega, não opera em vácuo social, mas dentro de estruturas históricas de desigualdade e criminalização da pobreza. Em suma, o reconhecimento facial, quando incorporado sem regulação, converte-se em uma ferramenta de vigilância assimétrica que padroniza a exclusão. A ausência de protocolos técnicos auditáveis e de supervisão independente transforma a promessa de inovação em risco de violação de direitos fundamentais.

3. RACISMO ALGORÍTMICO E EPISTEMOLOGIA NEGRA

Robert Williams, um homem negro estadunidense, acusado de roubar uma loja luxuosa, foi abordado e algemado ao chegar em casa, em frente a suas duas filhas e sua esposa. A prisão foi efetuada após um sistema de reconhecimento facial cruzar a imagem da carteira de motorista de Williams com as gravações do assalto captadas pelas câmeras de segurança, gerando um alerta que motivou a abordagem policial. O “único detalhe” do caso é que Williams não cometeu o crime. As imagens do assalto à loja mostravam outro homem negro (Silva, 2022).

O erro de uma tecnologia de reconhecimento facial operada pela segurança pública causou a prisão de Robert Williams. A questão é que o erro não é eventual, muito menos aleatório. Joy Buolamwini e Timnit Gebru (2018) demonstraram como sistemas de verificação facial comerciais têm desempenho muito pior para identificar pessoas pretas, sobretudo mulheres pretas.

Viés racial é um nome técnico para o racismo no âmbito da Inteligência Artificial (IA) e, no caso do reconhecimento facial, suas consequências podem acarretar em prisões equivocadas de pessoas pretas com o selo da eficácia e da neutralidade tecnológicas. Tarcízio Silva (2022, p. 69) nomeia esse viés de racismo algorítmico, “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”. A noção de racismo algorítmico emerge como uma das contribuições centrais para compreender o impacto da tecnologia sobre populações racializadas.

No Brasil, há casos de prisões indevidas amplamente divulgados na mídia. Em um deles, uma mulher foi presa após ser identificada como foragida pelo sistema de reconhecimento facial em Copacabana⁷, na Zona Sul do Rio de Janeiro. Embora tenha sido liberada após policiais da 12ª DP (Copacabana) consultarem o Tribunal de Justiça e constatarem o erro, o constrangimento ilegal já havia ocorrido. Segundo o Tribunal de Justiça, o banco de dados correto para a consulta é o BNMP2.0, do Conselho Nacional de Justiça. Caso não tenha um mandado de prisão em aberto nesse sistema, "nenhuma ordem de prisão fora do banco poderia ser cumprida".

Outro episódio emblemático envolvendo o uso do reconhecimento facial ocorreu durante as festividades juninas de 2022, em Salvador, Bahia. Um homem negro, acompanhado de sua esposa e filho, foi abordado no momento em que chegava ao Parque de Exposições da cidade para participar do evento. Sem que houvesse uma averiguação adequada, ele foi detido e permaneceu preso injustamente por 26 dias, acusado da prática de roubo. A infração que motivou sua prisão havia sido cometida em 2012, por outra pessoa. Na ocasião, o verdadeiro autor do crime, preso em flagrante, forneceu informações falsas, utilizando o nome do trabalhador e suas próprias impressões digitais para se identificar, o que originou a grave confusão e culminou na privação indevida de liberdade do inocente.

Esses casos evidenciam o risco da adoção acrítica dessas ferramentas tecnológicas. Além disso, estudos internacionais, como os realizados pelo Instituto Nacional de Padrões e Tecnologia dos EUA (NIST), apontam que o desempenho do reconhecimento facial varia de acordo com a origem geográfica dos desenvolvedores e os dados utilizados. Casos concretos, como os relatados no estudo CESeC/DPU (2025), revelam que a utilização do reconhecimento facial no Brasil resultou em prisões indevidas em ao menos sete estados, majoritariamente de pessoas negras e pobres. Tais falhas demonstram que a tecnologia, longe de corrigir desigualdades, as automatiza.

⁷ <https://oglobo.globo.com/rio/noticia/2024/01/04/mulher-identificada-pelo-sistema-de-reconhecimento-facial-em-copacabana-e-liberada-apos-ser-constatado-que-mandado-de-prisao-estava-no-sistema-por-erro.ghtml>

No livro “Racismo Algorítmico: inteligência artificial e discriminação nas redes digitais”, o pesquisador baiano Tarcízio Silva, mestre em Comunicação e doutorando em Ciências Humanas e Sociais, ressalta que a percepção da tecnologia como neutra é um equívoco grave. Para o autor, essa visão incorreta é agravada pela negação do racismo como elemento estrutural das relações e hierarquias sociais em países como o Brasil. Para o autor, algoritmos e sistemas de inteligência artificial, longe de serem neutros, reproduzem as hierarquias sociais existentes.

Essa constatação encontra fundamento na teoria do racismo estrutural, formulada por Silvio Almeida (2019), segundo a qual o racismo é elemento constitutivo das instituições e das relações de poder. Quando os algoritmos são treinados com dados históricos produzidos por sociedades racialmente desiguais, incorporam padrões discriminatórios e os projetam em escala digital. Trata-se, portanto, de uma continuidade tecnológica do racismo estrutural.

O impacto desse fenômeno é particularmente severo no contexto do sistema penal, já que o reconhecimento facial atua como extensão automatizada da seletividade penal. Como adverte Michelle Alexander (2017), o encarceramento em massa da população negra não é resultado de desvios individuais, mas de políticas de controle social travestidas de legalidade. A inteligência artificial, ao ser aplicada nesse mesmo ambiente, tende a naturalizar as desigualdades raciais sob a aparência de eficiência científica.

A crítica epistêmica de Lélia Gonzalez (1988) contribui para ampliar esse debate. Ao propor o conceito de amefricanidade, a autora defende uma epistemologia enraizada na experiência histórica afro-latino-americana, capaz de desafiar o universalismo eurocêntrico dominante. Sob essa ótica, o racismo algorítmico é também um problema de epistemologia tecnológica, tendo em vista que as bases de dados e os algoritmos são construídos a partir de critérios de representatividade que excluem corpos e experiências não brancas. A ausência de diversidade nos processos de criação e validação tecnológica reflete o que Gonzalez denominou de “silenciamento epistêmico”, isto é, a marginalização dos saberes produzidos fora da matriz colonial. Assim, a crítica à tecnologia deve ser acompanhada de uma crítica ao monopólio cognitivo que sustenta sua legitimação.

Nesse sentido, Livia Santana Vaz, em sua palestra “A Justiça é uma Mulher Negra”, ao discutir igualdade racial e justiça, enfatiza que o combate à discriminação requer a reconstrução institucional e a reformulação de práticas

decisórias que, mesmo sob aparência de legalidade, perpetuam a desigualdade racial. Aplicada ao contexto tecnológico, essa perspectiva implica reconhecer que a justiça algorítmica não será alcançada apenas com correções técnicas, mas por meio de mudanças estruturais nas relações de poder e no acesso à produção do conhecimento.

A literatura internacional reforça esse entendimento. Ruha Benjamin (2019), em *Race After Technology*, argumenta que as tecnologias digitais são “máquinas de inequidade” que automatizam a segregação. Da mesma forma, Safiya Noble (2018) demonstra, em *Algorithms of Oppression*, como sistemas de busca e plataformas digitais reproduzem estereótipos raciais e de gênero. Tais estudos convergem com o diagnóstico brasileiro ao apontar que a tecnologia opera como espaço de disputa racial e política.

No contexto do reconhecimento facial, essa disputa se manifesta nos próprios resultados dos algoritmos. O erro de identificação não é aleatório, uma vez que recai, sistematicamente, sobre pessoas negras. Isso ocorre porque os conjuntos de dados utilizados para treinamento são predominantemente compostos por rostos brancos. Como resultado, o sistema “aprende” a reconhecer melhor o que é considerado padrão hegemônico e a errar justamente nos corpos historicamente marginalizados.

Esse cenário reitera a necessidade de compreender o reconhecimento facial não apenas como ferramenta técnica, mas como ato político de classificação social. A epistemologia negra, ao reivindicar pluralidade de olhares e democratização do saber, oferece caminhos para reconfigurar os fundamentos éticos e cognitivos da tecnologia. A inclusão de perspectivas afro-diaspóricas e de saberes periféricos na formulação de políticas tecnológicas pode mitigar o viés estrutural que hoje caracteriza a inteligência artificial.

4. COMPATIBILIDADE DO RECONHECIMENTO FACIAL COM OS DIREITOS E GARANTIAS FUNDAMENTAIS E A RESPONSABILIDADE DO ESTADO POR EVENTUAIS PRISÕES INDEVIDAS

A compatibilidade do uso do reconhecimento facial no sistema penal com os direitos e garantias fundamentais previstos na Constituição Federal de 1988 é um tema central no debate sobre o impacto das novas tecnologias no Estado

Democrático de Direito. A Constituição Federal de 1988 estabelece, em seu art. 1º, inciso III, a dignidade da pessoa humana como fundamento da República. Este princípio, aliado à igualdade (art. 5º, caput) e à presunção de inocência (art. 5º, inciso LVII), orienta a atuação do Estado na proteção dos direitos individuais frente ao poder punitivo. O uso indiscriminado de reconhecimento facial, especialmente quando resulta em prisões equivocadas, contraria frontalmente tais princípios.

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), estabelece, em seu artigo 4º, inciso III, alíneas "a" a "d", que suas disposições não se aplicam ao tratamento de dados pessoais realizado com finalidades específicas de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Diante desse dispositivo, é possível afirmar que, sob a ótica da LGPD, o uso do reconhecimento facial pelo Estado não encontra, em princípio, vedação normativa.

Entretanto, é necessário considerar que a Constituição Federal de 1988 assegura, como garantia fundamental, o direito de que aquele que já possui identificação civil regular não seja submetido a identificação criminal (artigo 5º, inciso LVIII), salvo nas hipóteses excepcionais previstas em lei específica, como a Lei nº 12.037/2009. Em outras palavras, se o indivíduo apresenta documento de identidade oficial válido, não pode ser compelido a fornecer dados biométricos adicionais, seja por meio da coleta de impressões digitais, seja através de registros faciais, como fotografias ou vídeos.

A jurisprudência brasileira tem evoluído para reconhecer a importância da proporcionalidade na produção de prova penal. A exemplo disso, o STJ, no julgado do AgRg no REsp 2040092, publicado em 10/03/2025, entendeu que o uso de tecnologias de identificação sem observância das garantias processuais viola o devido processo legal e pode ensejar nulidade da prova. Esse movimento indica um recuo jurisprudencial em favor das garantias individuais, embora ainda insuficiente para conter práticas abusivas.

O direito à liberdade, que está intrinsecamente relacionado à presunção de inocência, é um dos mais vulneráveis diante de falhas nos sistemas de identificação tecnológica. Como destaca a interpretação jurídica sólida e majoritária no Brasil, a utilização de provas tecnológicas sem a devida regulamentação e sem critérios rigorosos de validação pode levar a prisões injustas, ferindo direitos fundamentais e comprometendo a integridade do processo penal.

Portanto, evidencia-se que a identificação criminal deve ser tratada como medida de caráter excepcional, em conformidade com os princípios constitucionais. Como destaca Luiz Flávio Gomes, a prática da identificação criminal só deve ocorrer em situações rigorosamente previstas em lei e em respeito às garantias individuais, para que se evite a banalização de procedimentos que podem implicar restrições injustificadas à liberdade e à dignidade da pessoa humana.

Nesse tocante, afirma Luis Flavio Gomes:

[...] se existe dúvida fundada (séria) sobre a identificação civil do sujeito, nada mais ponderado que proceder à sua identificação criminal. [...] não existe poder discricionário da autoridade de identificar ou não (aliás, raciocinar-se assim, pode-se chegar a atos arbitrários). Seu ato é vinculado: cabe-lhe examinar os pressupostos fáticos da situação e agir dentro da lei, conferindo sempre ao interessado o prazo de 48 horas para a comprovação de sua identificação civil, a não ser que seja patente, por exemplo, a inexistência de qualquer identificação. (Revista Consulex - Ano V - nº. 99, Fevereiro de 2001).

Além disso, é importante recordar que o sistema constitucional brasileiro adota o princípio da não autoincriminação. Esse princípio, associado aos direitos à ampla defesa e à presunção de inocência, assegura a qualquer indivíduo investigado, processado ou mesmo testemunha o direito de não ser compelido a produzir provas contra si próprio.

Dessa forma, observa Renato Brasileiro de Lima que:

[...] em se tratando de prova invasiva ou que exija um comportamento ativo, não é possível a produção forçada da prova contra a vontade do agente. Porém, se essa mesma prova tiver sido produzida, voluntária ou involuntariamente pelo acusado, nada impede que tais elementos sejam apreendidos pela autoridade policial. Em outras palavras, quando se trata de material descartado pela pessoa investigada, é impertinente invocar o princípio *nemo tenetur se detegere*. Nesse caso, é plenamente possível apreender o material descartado, seja orgânico (produzido pelo próprio corpo, como saliva, suor, fios de cabelo), seja inorgânico (decorrentes do contato de objetos com o corpo, tais como copo, ou garrafas sujas de saliva etc.). Exemplificando, se não é possível retirar à força um fio de cabelo de um suspeito para realizar exame de DNA, nada impede que um fio de cabelo desse indivíduo seja apreendido em um salão de beleza. [...]. (Manual de direito processual penal. Salvador: juspodivm, 2016, p.80.).

Outro ponto a destacar é que a violação de direitos decorrente de falhas tecnológicas implica, ainda, responsabilidade civil objetiva do Estado, prevista no art. 37, §6º, da Constituição Federal. Quando um cidadão é preso indevidamente em razão de erro de identificação automatizada, há dano moral e material indenizável,

independentemente de culpa do agente público. A responsabilidade estatal é condição necessária para garantir confiança nas instituições e para desestimular a banalização do uso de tecnologias de alto impacto social.

A discussão sobre o reconhecimento facial não se encerra na constatação de seus riscos. Para além disso, demanda a construção de estruturas de regulação e *accountability* que garantam controle público e transparência. A regulação deve combinar instrumentos jurídicos, técnicos e éticos, de forma a assegurar que a tecnologia opere de forma compatível com os princípios do Estado Democrático de Direito.

É imprescindível estabelecer um marco legal específico para o uso dessa tecnologia no sistema penal, disciplinando critérios de coleta e exclusão de dados, consentimento dos cidadãos, auditorias independentes e responsabilidade das empresas contratadas. Também se propõe a criação de um órgão nacional de supervisão algorítmica, vinculado à ANPD - Agência Nacional de Proteção de Dados, e a adoção de políticas de diversidade nos bancos de dados, a fim de reduzir vieses raciais e de gênero, conforme demonstram Ruha Benjamin (2019) e Safiya Noble (2018). A regulação deve ainda incorporar o princípio da transparência algorítmica e prever avaliações prévias de impacto antes da adoção de novas tecnologias.

Além da regulação estatal, é essencial promover uma cultura de responsabilidade social corporativa entre as empresas desenvolvedoras de inteligência artificial, exigindo certificações éticas e garantias de não discriminação. No campo acadêmico e social, deve-se fomentar o debate interdisciplinar sobre justiça algorítmica e democracia digital, com participação de especialistas, comunidades negras e movimentos sociais. Essa perspectiva, inspirada na amefricanidade de Lélia Gonzalez, propõe integrar saberes diversos e experiências históricas de resistência à formulação de políticas públicas. Assim, a regulação do reconhecimento facial deve transcender a dimensão técnica, assumindo caráter ético, político e inclusivo, em defesa da igualdade e da dignidade humanas.

5. CONSIDERAÇÕES FINAIS

A incorporação de tecnologias de reconhecimento facial no sistema penal brasileiro tem sido apresentada como avanço em eficiência investigativa e

modernização da segurança pública. Entretanto, a análise empreendida revela que o uso dessa ferramenta, em um contexto de racismo estrutural e ausência de regulação jurídica, compromete gravemente os direitos e garantias fundamentais assegurados pela Constituição Federal.

Os resultados demonstram que a tecnologia, quando aplicada sem critérios técnicos rigorosos e sem controle institucional, reproduz as desigualdades históricas do sistema de justiça criminal. O fenômeno identificado como racismo algorítmico manifesta-se na própria base de dados e nos parâmetros de funcionamento dos algoritmos, refletindo a seletividade racial que marca o sistema penal. Assim, longe de representar uma ruptura com práticas discriminatórias, o reconhecimento facial atualiza e automatiza a seletividade penal.

Constatou-se, também, que a inexistência de normas claras e de auditoria independente sobre os algoritmos utilizados gera insegurança jurídica e risco de prisões indevidas, como demonstram os casos analisados. A jurisprudência recente do Superior Tribunal de Justiça, ao invalidar condenações baseadas unicamente em reconhecimento facial ou fotográfico irregular, sinaliza um movimento de reafirmação das garantias processuais, mas ainda insuficiente para conter os efeitos estruturais da tecnologia aplicada de modo acrítico.

A análise crítica, amparada em autores como Silvio Almeida, Lélia Gonzalez e Lívia Santana Vaz, permitiu compreender que o racismo tecnológico não é apenas questão de dados enviesados, mas de epistemologias excludentes. A ausência de diversidade na formulação de políticas tecnológicas e na produção científica reproduz o silenciamento histórico das vozes negras e periféricas, o que reforça a necessidade de uma epistemologia amefricana capaz de reorientar a construção do conhecimento técnico-científico em direção à pluralidade e à justiça social.

Em termos jurídicos, verificou-se que a tecnologia de reconhecimento facial, na forma como é utilizada atualmente, viola princípios constitucionais basilares, como a dignidade da pessoa humana, a liberdade individual, a igualdade e o devido processo legal. Além disso, a Lei Geral de Proteção de Dados (LGPD), ao excluir a persecução penal de seu campo de aplicação, deixa o cidadão exposto a práticas de vigilância sem garantias adequadas. A responsabilidade do Estado por prisões indevidas decorrentes de erro tecnológico é objetiva e deve ser rigorosamente aplicada, conforme dispõe o art. 37, §6º da Constituição. A reparação

das vítimas é requisito de justiça, mas não substitui a necessidade de prevenção. Por essa razão, a criação de marcos regulatórios específicos e de mecanismos de *accountability* algorítmica é imperativa.

O debate sobre reconhecimento facial ultrapassa o campo técnico e atinge o núcleo ético e político do Estado Democrático de Direito. O desafio contemporâneo é equilibrar inovação tecnológica e proteção de direitos humanos, assegurando que a busca por segurança não se converta em instrumento de exclusão. O Estado, enquanto garantidor dos direitos fundamentais, deve promover políticas públicas de tecnologia baseadas em transparência, representatividade e controle social.

A consolidação de uma regulação voltada à justiça algorítmica deve incluir auditorias externas obrigatórias, diversidade nos bancos de dados, fiscalização por órgãos autônomos e mecanismos de revisão judicial das decisões automatizadas. A transparência dos algoritmos e a participação de comunidades vulnerabilizadas nos processos decisórios representam não apenas medidas técnicas, mas exigências democráticas.

O estudo conduzido evidencia, portanto, que o reconhecimento facial, se mantido sob o paradigma atual, contraria os princípios do Estado de Direito e aprofunda as desigualdades raciais. A adoção de políticas inclusivas, baseadas em epistemologias plurais e no controle público da tecnologia, é caminho necessário para transformar a inteligência artificial em instrumento de justiça e não de opressão.

Em síntese, conclui-se que o reconhecimento facial, enquanto prática probatória e de vigilância, só poderá ser compatível com a Constituição se submetido a regulação estrita, controle democrático e revisão crítica de suas bases epistemológicas. O enfrentamento do racismo algorítmico não é apenas tarefa técnica, mas projeto ético de reconstrução social, que demanda coragem institucional e compromisso com a igualdade substantiva.

REFERÊNCIAS

ALEXANDER, Michelle. **The New Jim Crow: Mass Incarceration in the Age of Colorblindness**. New York: The New Press, 2017.

ALMEIDA, Silvio. **Racismo Estrutural**. São Paulo: Editora Pólen, 2019. ISBN: 978-85-98349-74-9.

BADARÓ, Gustavo Henrique Righi Ivahy. **A nova regulamentação da identificação criminal**. Boletim IBCCRIM. São Paulo, v.8, n.100, p. 9-10, mar. 2001.

BENJAMIN, Ruha. **Race After Technology: Abolitionist Tools for the New Jim Code**. Cambridge: Polity Press, 2019.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República,. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 04 de abril de 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 04 de abril de 2025.

BUOLAMWINI, Joy & GEBRU, Timnit (2018, February). **Gender shades: Intersectional accuracy disparities in commercial gender classification**. In **Conference on fairness, accountability and transparency (pp. 1-15)**. Proceedings of Machine Learning Research, 2018. Disponível em: <<http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>> Acesso em 04 de abril de 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

GOMES, Luiz Flávio. **Revista Consulex** - Ano V - nº. 99, Fevereiro de 2001.

GONZALEZ, Lélia. **Por um Feminismo Afro-Latino-Americano**. In: _____. **Primavera para as Rosas Negras: Lélia Gonzalez em primeira pessoa**. São Paulo: Diáspora Africana, 2018.

HUMAN RIGHTS WATCH. **World Report 2021**: Brazil. Human Rights Watch, 2021.

KOCH, Willian; LOPES, Rafael V. de M. **Do reconhecimento facial a partir da inteligência artificial: a possibilidade de sua utilização como prova no processo penal brasileiro**. Jusbrasil, 2025. Disponível em: <https://www.jusbrasil.com.br>. Acesso em: 14 abr. 2025.

LIMA, Renato Brasileiro de. **Manual de direito processual penal**. Salvador:

juspodivm, 2016, p.80;

LYON, David. **Surveillance Studies: An Overview**. Cambridge: Polity Press, 2018.

NOBLE, Safiya Umoja. **Algorithms of Oppression: How Search Engines Reinforce Racism**. New York: New York University Press, 2018.

NUCCI, Guilherme de Souza. **Código de Processo Penal comentado**. 18. ed. São Paulo: Forense, 2022.

NUNES, Pablo et al. **Mapeando a vigilância biométrica [livro eletrônico]: levantamento nacional sobre o uso do reconhecimento facial na segurança pública**. Rio de Janeiro: CESeC, 2025.

O'NEIL, Cathy. **Algoritmos de destruição em massa. Como o big data aumenta a desigualdade e ameaça a democracia**. São Paulo: Editora Rua do Sabão, 2020.

RAMOS, Lucas Cabral de Souza. **Reconhecimento Facial: do uso privado aos blocos de carnaval**. 2021. 39 f. Trabalho de Conclusão de Curso (Análise e Desenvolvimento de Sistemas) – Faculdade de Educação Tecnológica do Estado do Rio de Janeiro, 2021.

REQUIÃO, Luis Henrique. **O direito criminal e as novas formas de investigação criminal: Análise sobre o Reconhecimento Facial para fins penais**. [S.l.: s.n.], [2025?]. Texto não publicado. Documento obtido em acervo pessoal do autor.

RIO DE JANEIRO. **Mulher identificada pelo sistema de reconhecimento facial em Copacabana é liberada após ser constatado que mandado de prisão estava no sistema por erro**. O Globo, Rio de Janeiro, 4 jan. 2024. Disponível em: <https://oglobo.globo.com/rio/noticia/2024/01/04/mulher-identificada-pelo-sistema-de-reconhecimento-facial-em-copacabana-e-liberada-apos-ser-constatado-que-mandado-de-prisao-estava-no-sistema-por-erro.ghhtml>. Acesso em: 05 abr. 2025.

ROCHA, Heloisa Rodrigues da. **Regulação da inteligência artificial generativa e racismo algorítmico no reconhecimento facial**. São Paulo: Editora Dialética, 2025. ISBN 978-65-270-5810-3

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

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância: A Luta por um Futuro Humano Frente às Novas Fronteiras do Poder**. Rio de Janeiro: Intrínseca, 2021. E-ISBN 978-65-5560-145-9