RACISMO ALGORÍTMICO EM TECNOLOGIAS DE RECONHECIMENTO FACIAL: IMPACTOS NO SISTEMA PENAL BRASILEIRO

Anelize Fátima Almeida de Lara
Email: 23062862@uepg.br
Graduanda em Direito pela Universidade Estadual de Ponta Grossa – Paraná, Brasil.

Eduarda Hemeterio Bueno
Email: 23017562@uepg.br
Graduanda em Direito pela Universidade Estadual de Ponta Grossa – Paraná, Brasil.

Pedro Fauth Manhães Miranda
Email: pedromiranda.adv@gmail.com
Doutor em Direito pela Pontifícia Universidade Católica do Paraná – Paraná, Brasil.

Resumo: Os avanços da inteligência artificial e o consequente surgimento das tecnologias de reconhecimento facial, utilizadas na segurança pública e na persecução penal, trouxeram a discussão sobre o racismo algorítmico, uma nova manifestação do racismo estrutural. Os vieses raciais encontrados nessas ferramentas podem reproduzir preconceitos e discriminações já enraizados na sociedade, resultando na violação de direitos fundamentais. Diante desse cenário, o presente estudo tem como objetivo analisar a presença do racismo algorítmico em tecnologias de reconhecimento facial e seus reflexos no sistema penal brasileiro. Para tanto, adota-se o método indutivo, com base em uma pesquisa bibliográfica. A análise apontou a necessidade da atuação estatal na proteção dos grupos minoritários afetados por erros destes dispositivos e na criação de uma legislação específica que regulamente o uso da tecnologia no país.

Palavras-chave: Racismo Algorítmico, Reconhecimento facial, Sistema Penal.

Introdução

Os avanços da inteligência artificial no mundo contemporâneo possibilitaram a criação de novas ferramentas tecnológicas, como é o caso dos sistemas de reconhecimento facial. Atualmente, essas tecnologias estão sendo utilizadas na área da segurança pública e da persecução penal como instrumento para encontrar com mais agilidade criminosos, bem como solucionar crimes.

Todavia, não são raros os casos em que o sistema de reconhecimento facial demonstrou falibilidade e trouxe consequências indesejadas no âmbito do sistema penal, especialmente para as pessoas negras, considerando que os algoritmos presentes nessas tecnologias reproduzem vieses preconceituosos presentes na sociedade. Nesse sentido, enquanto problema de pesquisa o trabalho aponta o

racismo algorítmico presente em tecnologias de reconhecimento facial como produtor de desigualdades e injustiças no sistema penal brasileiro.

Diante desse contexto, os objetivos da pesquisa são explicar como o racismo algorítmico opera em tecnologias de reconhecimento facial; demonstrar os impactos no sistema penal brasileiro e explorar o dever do Estado diante de violações de direitos fundamentais.

A fim de atingir o propósito do trabalho, adota-se para a pesquisa o método indutivo, ancorado em uma pesquisa bibliográfica baseada em artigos científicos e livros relacionados ao tema, e coleta e análise de casos noticiados encontrados na mídia. Com base nos estudos de Tarcízio Silva (2022), o texto adota como referencial teórico o conceito de racismo algorítmico.

Na segunda parte do trabalho, far-se-á a apresentação da inteligência artificial e do sistema de reconhecimento facial, seu funcionamento e características técnicas. Na terceira parte, será apresentado o conceito de racismo algorítmico e sua relação com o sistema de reconhecimento facial. Em seguida, serão apresentados os impactos no sistema penal brasileiro, acompanhados de relatos de casos reais. Por fim, a última parte do trabalho é dedicada a abordar o dever do Estado e trazer possíveis soluções para as problemáticas que envolvem o sistema de reconhecimento facial.

A pesquisa se mostra relevante em razão da necessidade de refletir criticamente sobre o uso das tecnologias de reconhecimento facial no sistema penal brasileiro, cuja aplicação tem revelado falhas técnicas e efeitos discriminatórios.

2 Inteligência Artificial e Sistema de Reconhecimento Facial

Atualmente, vivemos em uma Era da Informação, onde a sociedade é moldada por tecnologias digitais de informação e comunicação (MIRANDA; SCHNEIDER, 2020). Entre essas tecnologias, destaca-se a Inteligência Artificial (IA).

A Inteligência Artificial pode ser descrita como uma máquina que tem a capacidade de se comportar como um ser humano inteligente (COSTA; KREMER, 2022). Essas máquinas passam por um processo de aprendizado, onde são alimentadas por dados que fornecem informações sobre diversos assuntos (CHAVES JUNIOR; GUASQUE; PADUA, 2023).

Não é possível discutir Inteligência artificial sem abordar sobre o algoritmo, ferramenta essencial para entender o funcionamento das máquinas de IA. Na obra “Racismo algorítmico: inteligência artificial e discriminação nas redes digitais”, Tarcízio Silva é claro e preciso ao definir o termo como “sistematizações de procedimentos encadeados de forma lógica para realizar tarefas em um espaço computacional” (2022, p. 60).

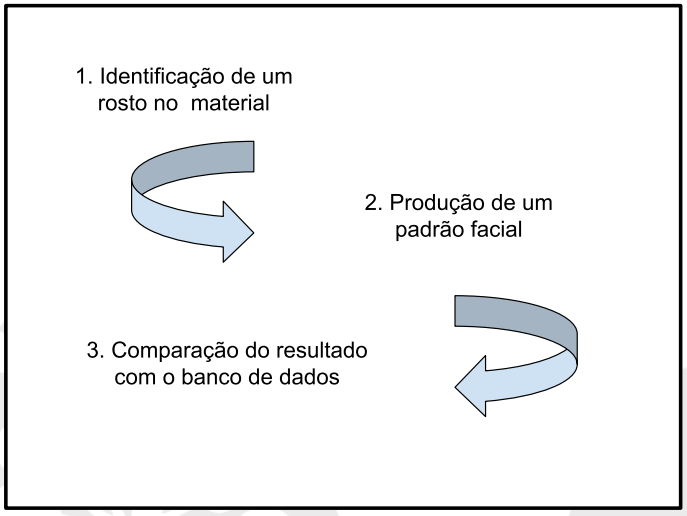
Os sistemas algorítmicos, presentes nas tecnologias de inteligência artificial, são responsáveis por cumprir uma sequência de instruções a fim de solucionar determinado problema. Alguns computadores e máquinas necessitam de algoritmos complexos capazes de executar tarefas específicas e produzir padrões. Nesses casos, a técnica utilizada é conhecida como aprendizado de máquina ou *machine learning*. O diferencial da técnica é a autonomia para desempenhar funções por conta própria, as quais consistem em aprender com os dados e identificar padrões (DA SILVA; ARAÚJO, 2020).

Os sistemas de reconhecimento facial são dotados de inteligência artificial para serem capazes de identificar pessoas, de modo que correspondem a uma ferramenta tecnológica que se comporta como uma atividade humana (COSTA; KREMER, 2022). Atualmente, este sistema está sendo ampliado no âmbito da segurança pública como instrumento de vigilância da sociedade.

Segundo o Instituto Igarapé (2019), o uso da tecnologia de reconhecimento facial no Brasil se tornou popular no ano de 2019, especialmente nos estados da Bahia e do Rio de Janeiro. A primeira etapa do sistema de reconhecimento facial é a identificação de um rosto na fotografia ou no vídeo em análise, retirada de uma câmara de segurança, por exemplo. A partir disso, o sistema escolhe pontos específicos da face, como olhos, boca e nariz, e realiza um cálculo matemático com base na distância entre eles para produzir um padrão facial. Após esse processo, é realizada uma comparação para verificar a compatibilidade entre o padrão facial e o registro cadastrado em um banco de dados (NUNES, 2019).

Em suma, podemos resumir as etapas de funcionamento do sistema de reconhecimento facial da seguinte forma:

Figura 1. Representação do funcionamento do sistema de reconhecimento facial



Fonte: Os autores

Na segurança pública, especificamente no policiamento, após o processo de cálculo e comparação do resultado, se houver um grau considerável de semelhança entre a filmagem da câmera e a imagem do banco de dados - no caso em tela, o mandado de prisão - é acionado um sinal de alerta para realizarem as diligências necessárias (NUNES, 2019).

Apesar de aparentar ser uma ferramenta tecnológica promissora ao lado do policiamento, os sistemas de reconhecimento facial podem apresentar uma outra faceta. Como todas as tecnologias, essas ferramentas não estão isentas de erros. O Coordenador de Pesquisa da Rede de Observatórios da Segurança, Paulo Nunes (2019, p. 68) explica que as ferramentas de reconhecimento facial podem gerar “constrangimentos, prisões arbitrárias e violações de direitos humanos”. Estes problemas podem ser explicados a partir do racismo algoritmo, fenômeno que surgiu a partir dos avanços tecnológicos da Inteligência Artificial.

3 Racismo algorítmico e o Sistema de Reconhecimento Facial

Com o avanço das tecnologias de Inteligência Artificial, a modernidade passou a expressar o racismo por meio de novas formas, possibilitando a discussão sobre o racismo algorítmico. Para compreender esse fenômeno, consideramos ser necessário apresentar, inicialmente, o que se entende por racismo.

Em seu livro “Racismo Estrutural”, o filósofo e professor Silvio Almeida define o racismo como

> [...] uma forma sistemática de discriminação que tem a raça como fundamento, e que se manifesta por meio de práticas conscientes ou inconscientes que culminam em desvantagens ou privilégios para indivíduos, a depender do grupo racial ao qual pertençam (2019, p. 23)

O caráter sistêmico do racismo não se refere somente a um caso isolado de discriminação ou a um conjuntos de casos, mas trata-se de um processo histórico onde as diferenças e privilégios baseadas na raça estão inseridas em todas as esferas sociais, econômicas ou políticas de uma sociedade (ALMEIDA, 2019).

A partir disso, os sistemas algorítmicos se tornam problemáticos no momento em que passam a reproduzir padrões preconceituosos e criar vieses racistas. Nessa razão, pesquisadores passaram a se aprofundar no estudo do racismo algoritmo, demonstrando como as suas consequências podem trazer danos para grupos minoritários.

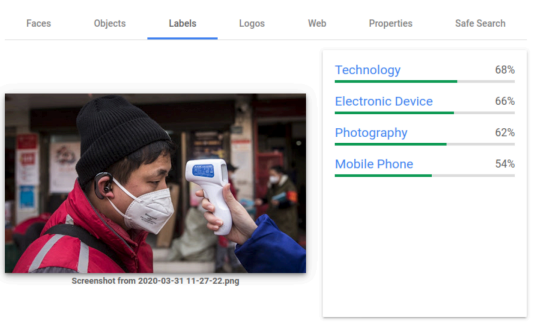
O racismo algorítmico pode ser definido como a perpetuação de preconceitos preexistentes na sociedade por meio de algoritmos e sistemas de inteligência artificial (DE ALMEIDA, et. al, 2025). Trata-se, portanto, de um desdobramento do racismo estrutural que permeia as instituições e as relações sociais. Nesse sentido, Da Silva e Araújo (2020) denominam o fenômeno como “racismo estrutural-algorítmico”, ressaltando o modo como os sistemas tecnológicos incorporam e reproduzem desigualdades já existentes.

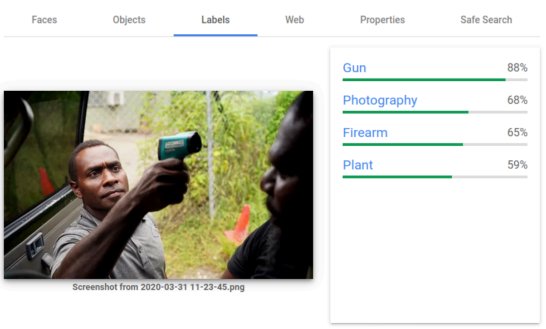
Um exemplo prático desse fenômeno ocorreu em 2019, quando a estudante e pesquisadora negra Joy Buolamwini testou uma ferramenta de reconhecimento facial em um laboratório de tecnologia, e constatou que a ferramenta não reconheceu rostos negros, embora tenha identificado com precisão rostos de pessoas brancas. O mais chocante foi quando Joy colocou uma máscara branca sobre a face e passou a ser reconhecida pela ferramenta. Ao analisar a tecnologia, a pesquisadora constatou que o banco de dados era composto, majoritariamente, por

imagens de pessoas brancas, em razão disso o dispositivo não aprendeu a reconhecer rostos como o dela (EloInsights, 2022).

No ano seguinte, em 2020, o pesquisador Nicolas Kayser-Bril testou a ferramenta Google Vision na plataforma Google, onde carregou duas fotos similares de pessoas segurando um termômetro. Na imagem do homem asiático, a ferramenta identificou o termômetro como uma “tecnologia” e um “dispositivo eletrônico” com 68% e 66% de precisão, respectivamente. Enquanto na imagem com o homem negro, a ferramenta apontou o termômetro como 88% de chances de ser uma “arma”, apesar da similaridadade dos objetos (SILVA, 2020).

Figuras 2 e 3: Testes do pesquisador Nicolas Kayser-Bril no Google Vision

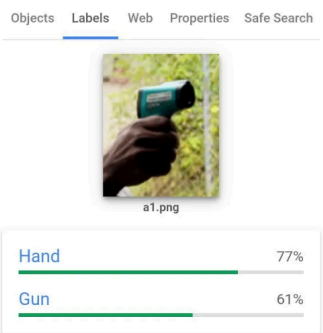


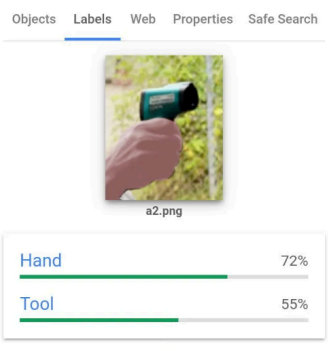


Fonte: SILVA, Tarcízio. Google acha que ferramenta em mão negra é uma arma. 02 abr. 2020. Disponível em: https://tarciziosilva.com.br/blog/google-acha-que-ferramenta-em-mao-negra-e-uma-arma/. Acesso em: 29 jul. 2025.

O pesquisador Bart Nagel também realizou o experimento, recortando a foto do homem negro e deixando somente a mão e o termômetro, com ajustes adicionais na iluminação para embranquecer a pele. O resultado constatou que a mão embranquecida reconheceu o termômetro como uma “ferramenta”, ao contrário da foto com a mão de pele negra, que reconheceu o objeto como uma “arma” (SILVA, 2020).

Figuras 4 e 5: Testes do pesquisador Bart Nagel no Google Vision





Fonte: SILVA, Tarcízio. Google acha que ferramenta em mão negra é uma arma. 02 abr. 2020. Disponível em: https://tarciziosilva.com.br/blog/google-acha-que-ferramenta-em-mao-negra-e-uma-arma/. Acesso em: 29 jul. 2025.

Observa-se que os experimentos realizados com a plataforma do Google Vision reforçaram o estereótipo racista que a sociedade criou de que pessoas negras seriam consideradas perigosas somente em razão da cor de pele.

Estes casos são exemplos da forma como o racismo algorítmico atua na prática, reproduzindo vieses raciais enraizados na sociedade. Tendo em vista que o reconhecimento facial se utiliza de algoritmos para o seu funcionamento, o problema do racismo algorítmico também é encontrado nessa tecnologia.

Destaca-se que o algoritmo não é o responsável por criar preconceitos, mas é capaz de reproduzir os padrões dos dados utilizados quando estes sistemas foram treinados. Ao treinar os algoritmos, os cientistas focam em dados com base em características de determinada raça (branca) e negligenciam as demais, o que significa que quando esses sistemas são aplicados na realidade, o reconhecimento facial de raças negligenciadas apresenta taxas muito mais altas de erros.

Em um estudo conduzido pelo NIST (Instituto Nacional de Padrões e Tecnologia), mencionado por Araújo, Cardoso e Paula (2021), foram examinados 189 algoritmos de reconhecimento facial desenvolvidos por 99 empresas distintas. Os resultados desse estudo revelaram uma desproporção alarmante: os sistemas investigados apresentaram uma taxa significativa de erros na identificação de pessoas negras e asiáticas em relação aos resultados alcançados com pessoas brancas.

É importante problematizar ainda a predominância de homens brancos na área da tecnologia e da Inteligência Artificial, e a sub-representatividade de mulheres e de pessoas negras. No Brasil, a pesquisa “Diagnóstico Comportamental dos Profissionais de TI” (IT Forum, 2024) apontou que os profissionais da área correspondem a 73% brancos, 20% pardos, 4% negros e 3% amarelos. A pesquisa também constatou que os homens correspondem a 86%, enquanto que as mulheres são apenas 12% dos indivíduos que trabalham nestes espaços. Esses dados são assustadores e representam a desigualdade e o atraso no desenvolvimento do setor.

Como consequência do racismo algorítmico, o sistema de reconhecimento facial pode ser recorrente na produção de falsos positivos, sendo grandes as

chances disso ocorrer caso o grau de semelhança seja menor que 90% (NUNES, 2019). Desse modo, além do constrangimento e da violência, esses falsos positivos reforçam a criminalização em massa de grupos minoritários que historicamente foram - e ainda são vítimas do sistema penal brasileiro.

Como apontam Miranda e Schneider (2020, p. 12):

> Na modernidade líquida, estigmas e preconceitos se naturalizaram e se institucionalizaram. Indivíduos de determinado perfil étnico e social, quando submetidos aos sistemas de controle e segurança, permanecem em secular desvantagem, perpetrada pelo próprio Estado, ainda detentor do poder de rotular e segregar.

Nesse sentido, a concepção de que as ferramentas de inteligência artificial, como as de reconhecimento facial, são neutras e imparciais, não é verídica. Acreditar que esses sistemas são dotados de neutralidade encoberta as dimensões sociais e dificultam a apresentação de propostas para combater o problema. Essas tecnologias são criadas por seres humanos que ainda carregam pensamentos preconceituosos e praticam discriminações, de modo que a sociedade não se desvinculou de comportamentos coloniais. Considerando que os algoritmos são treinados de forma limitada, sem considerar a diversidade de uma sociedade, os vieses raciais e preconceituosos são reproduzidos, conscientemente ou não, a partir do aprendizado de máquina, construindo uma tecnologia racializada e baseada na lógica da supremacia branca.

4 Os impactos no sistema penal brasileiro

O crescente desenvolvimento de Inteligências Artificiais de reconhecimento facial tem promovido intensas discussões sobre suas implicações éticas, sociais e jurídicas, especialmente quando aplicadas ao sistema penal. Apesar dessas ferramentas prometerem otimizar processos da segurança pública e da persecução penal, uma análise crítica e fundamentada em estudos acadêmicos revela que, ao invés de promover justiça, elas frequentemente perpetuam desigualdades históricas e promovem erros que afetam diretamente a liberdade e dignidade de pessoas inocentes. A presença de vieses algorítmicos, a ausência de regulamentação específica e a histórica seletividade penal brasileira tornam o uso do reconhecimento facial uma prática que demanda urgente reavaliação.

Em primeiro lugar, para compreender inteiramente o impacto desses sistemas no direito penal brasileiro, é preciso reconhecer que a aplicação do direito penal é seletiva, bem como que o sistema penal brasileiro carrega em sua estrutura a marca histórica da exclusão e da violência racial. Desde o período colonial, passando pela escravidão, e mesmo após a abolição formal, a população negra seguiu sendo alvo de políticas de criminalização, controle e invisibilização social.

A suposta transição para um Estado de Direito democrático nunca rompeu, de fato, com os padrões institucionais herdados do período escravocrata, pelo contrário, reconfigurou práticas de exclusão em novas formas de atuação estatal, com destaque para o uso seletivo da lei penal e o encarceramento em massa de pessoas negras. Essa realidade é evidenciada por dados como os do Atlas da Violência (CERQUEIRA; BUENO, 2024) o qual aponta que, em 2023, mais de 76,5% das vítimas de homicídio no Brasil foram negras; e do INFOPEN (BRASIL, 2024), segundo os quais a população negra representa 70% do total de pessoas encarceradas no Brasil. Tais dados não são apenas simples números, mas sim o retrato de um legado contínuo de dominação e repressão, que persiste até os dias atuais.

Proposta por Achille Mbembe (2016), a ideia de necropolítica exposta pelo autor é fundamental para entender como o sistema penal opera até os dias atuais. Mbembe argumenta que o poder soberano não se trata tão somente do direito de matar, mas sim refere-se ao poder de decidir quem tem direito à vida e quem será exposto à morte.

No contexto brasileiro, essa lógica se evidencia por meio da exclusão simbólica e material que atinge em massa a população negra, historicamente marginalizada e criminalizada. Essa dinâmica manifesta-se através da invisibilização e da violência sistemática contra esse grupo. Diante desse pano de fundo, o sistema penal opera como uma ferramenta de controle social, produzindo desigualdades e deixando de cumprir sua função de promover justiça.

Diante disso, inteligências artificiais que prometem eficiência e modernização do sistema de justiça, como os sistemas de reconhecimento facial, precisam ser analisadas de forma crítica. É preciso reconhecer que o reconhecimento facial não é uma tecnologia neutra, tendo em vista que são construídos a partir de dados coletados e processados por seres humanos que, conscientes ou não, reproduzem no algoritmo os preconceitos estruturais da sociedade. Essas tecnologias, ao se

desenvolverem em contextos racializados como o brasileiro, tendem a associar erroneamente indivíduos negros a atividades criminosas com muito mais frequência do que fazem com indivíduos brancos, como demonstram os casos de erros de sistema facial ocorridos no Brasil.

Os casos de prisões injustas de inocentes identificados incorretamente por sistemas de reconhecimento facial são um dos impactos mais preocupantes dessa tecnologia. No Rio de Janeiro, o jovem negro Danilo Félix, de 26 anos, já foi preso 3 vezes devido a erros em sistemas de reconhecimento facial. No primeiro caso, Danilo ficou preso preventivamente durante 55 dias aguardando a audiência de instrução, e na ocasião, a vítima confirmou que Danilo não foi o responsável pelo crime. No segundo caso, a vítima fez a identificação a partir do banco de dados da polícia e, após o reconhecimento presencial, afirmou que Danilo não era o responsável. Por fim, no caso mais recente, Danilo foi reconhecido erroneamente como autor de um crime que não cometeu, novamente a partir do banco de dados da polícia (MESQUITA, 2023).

Outro caso ocorreu na Bahia, onde um homem negro foi passear com a sua família em um evento, ocasião em que foi detido pela polícia e permaneceu preso injustamente durante 26 dias, em razão de erro do sistema de reconhecimento facial. (ALENCAR, 2023).

Em Sergipe, o personal trainer João Antônio Trindade Bastos assistia uma partida de futebol quando foi surpreendido por policiais militares que o confundiram com um foragido, com base no sistema de reconhecimento facial. João foi conduzido e levado até uma sala da PM, onde os policiais militares o interrogaram. Somente após apresentar o seu documento e se identificar ele foi liberado. João relata que se sentiu “com muito medo, frustrado e constrangido” diante da situação (FANTÁSTICO, 2024).

Todos esses casos são evidências do racismo estrutural-algorítmico presente nas tecnologias de reconhecimento facial. As situações de uma prisão arbitrária devido a um erro de reconhecimento facial não se limitam a um mero aborrecimento ou um breve constrangimento, mas violam direitos fundamentais como a presunção de inocência e a dignidade da pessoa humana. Para além do dano jurídico, às vítimas desses erros ainda precisam lidar com os traumas psicológicos, preconceitos e humilhação de serem confundidas e tratadas como criminosas. A falta de responsabilização por parte do Estado agrava ainda mais a dor e a humilhação.

5 Dever do Estado no Enfrentamento do Racismo Algorítmico: Propostas e Perspectivas

Os sistemas de reconhecimento facial têm sido uma promessa no contexto da segurança pública e do processo penal, ao mesmo tempo em que populações desprotegidas têm sido afetadas com o uso desses sistemas, como já exposto nos capítulos anteriores. Diante dessa falibilidade dos sistemas de reconhecimento facial e seus impactos no âmbito penal, surgem propostas e possíveis soluções para enfrentar o problema do racismo algorítmico.

Primeiramente, é necessário trabalhar com o senso de responsabilidade das equipes envolvidas no desenvolvimento das tecnologias, especialmente na área de reconhecimento facial. O primeiro passo começa pela conscientização, compreendendo que vivemos em uma sociedade plural e nem todos os grupos sociais estão inclusos no mercado tecnológico (EloInsights, 2022). Assim, o Estado deve promover políticas públicas de incentivo à contratação de mulheres e pessoas negras, além de garantir que estes profissionais ocupem cargos de liderança e de desenvolvimento das tecnologias, especialmente as de reconhecimento facial (TAVARES, 2024). Com isso, a diversidade de uma equipe pode fazer a diferença no treinamento dos modelos de inteligência artificial, e neutralizar a presença de vieses raciais nos algoritimos.

Cabe ainda ao Estado assegurar os direitos básicos dos cidadãos, como o respeito, a igualdade, a liberdade e a proteção. Considerando as graves violações desses direitos e os diversos casos de prisões de inocentes, convém destacar o previsto no artigo 37, §6° da Constituição Federal de 1988:

> As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

O artigo dispõe que o governo deve responder pelos danos que os seus agentes causarem aos cidadãos. Nesse sentido, a interpretação do texto deve abarcar também o uso indevido de tecnologias, como as de reconhecimento facial, que podem levar a prisões injustas ou abordagens discriminatórias. Nessas situações, impõe-se ao Estado o dever de indenizar quem foi preso ou acusado injustamente, revisar os processos baseados em identificações tecnológicas e

responsabilizar os agentes envolvidos. Sendo assim, é essencial que o governo promova a educação digital da população, visando a compreensão sobre essas novas tecnologias, seus riscos e como exigir seus direitos diante de uma possível falha do Estado. Dessa forma, o governo deve agir com responsabilidade, cautela e transparência, uma vez que o reconhecimento facial exige regulação, diálogo com a sociedade e respeito aos direitos humanos.

No que diz respeito à transparência, é essencial garantir o acesso da população às informações sobre os contratos de sistemas de reconhecimento facial. Muitas vezes, pode ocorrer a contratação de empresas para fornecer softwares, mas sem informar para a sociedade os critérios, a forma de tratamento dos dados e a taxa de erro desses sistemas, o que impede o controle social e afeta a confiança da sociedade.

Além disso, quando tratamos de sistema de dados, podemos pensar primeiramente na Lei Geral de Proteção de Dados (Lei nº 13.709/2018), responsável por limitar o uso de dados pessoais, como imagens e dados biométricos. Embora exista exceção para os ramos da segurança pública, defesa nacional, segurança do Estado e investigação criminal (art. 4º, III), o §1º do mesmo artigo exige que essas atividades sigam os princípios de proteção de dados, como finalidade, necessidade, transparência, segurança e responsabilização. Se um sistema tecnológico coleta dados faciais sem controle, o governo pode estar infringindo princípios. Portanto, se mostra necessário revisar a Lei Geral de Proteção de Dados (LGPD) para abordar melhor o uso de tecnologias de vigilância, como o reconhecimento facial.

Apesar da importância, os princípios gerais previstos na LGPD – como finalidade, necessidade, transparência, segurança e responsabilização – podem não ser suficientes diante da complexidade dessas ferramentas. Nesse sentido, uma alternativa seria a criação de uma lei específica para regular o uso de sistemas de reconhecimento facial e outras tecnologias biométricas pelo governo. Essa lei deve definir critérios técnicos, limites legais, garantias processuais e mecanismos de controle e responsabilização.

Diante desse cenário, cabe destacar três propostas legislativas com objetivos parecidos, mas conteúdos completamente distintos: o Projeto de Lei 2338/2023, de autoria do Senador Rodrigo Pacheco, o Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal (APL), elaborado por uma

comissão de juristas, e o Projeto de Lei 1515/2022, de autoria do deputado Coronel Armando. Ambos os projetos visam normatizar o tratamento de dados pessoais no contexto da segurança pública, contudo, partem de princípios e visões políticas diferentes.

O Projeto de Lei 2338/2023 deixa claro a obrigação do Estado em promover uma legislação responsável sobre os sistemas de inteligência artificial, especialmente os sistemas de alto risco, como é o caso dos sistemas de reconhecimento facial, bem como prevê em seu artigo 5° o direito à informação, privacidade e não discriminação. O PL ainda classifica em seu artigo 14, XI, os sistemas de identificação - sistemas de reconhecimento facial, por exemplo - como tecnologias de alto risco.

Por sua vez, o Anteprojeto busca assegurar os direitos fundamentais e processuais dos cidadãos, bem como harmonizar os deveres do Estado na segurança pública, partindo do princípio de que o tratamento de dados no contexto do sistema penal necessita de limites bem definidos, principalmente por se tratar de uma área em que o Estado detém o poder de restringir liberdades.

Como consta no Anteprojeto (2019, p. 2), o seu intuito é:

> [...] disciplinar os princípios, as diretrizes e as linhas mestras da proteção de dados no referido âmbito. Busca-se, portanto, harmonizar, de um lado, os deveres do Estado na prevenção e na repressão de ilícitos criminais, protegendo a ordem pública; de outro, assegurar a observâncias das garantias processuais e as prerrogativas fundamentais dos cidadãos brasileiros no que tange ao tratamento de dados pessoais para tais fins.

Pois bem, entre os principais pontos do Anteprojeto, destacam-se os princípios fundamentais previstos no artigo 6°, incluindo a licitude, a finalidade, a adequação e a necessidade. Esses princípios visam garantir que o tratamento de dados ocorra de forma ética, controlada e em conformidade com os preceitos constitucionais, como a dignidade da pessoa humana.

Destaca-se ainda o artigo 7°, o qual dispõe sobre a diferenciação entre suspeitos, pessoas condenadas, vítimas, testemunhas, entre outros. Essa previsão é de extrema relevância no contexto dos sistemas de reconhecimento facial, visando regular as abordagens realizadas, bem como evitar a violação de direitos fundamentais.

Outro avanço com relação ao Anteprojeto é o previsto no artigo 8°, onde prevê que o responsável pelo tratamento de dados deve separar dados objetivos de dados subjetivos, visando evitar que pessoas inocentes tenham seus direitos violados em razões de um sistema preconceituoso, com dados enviesados e imprecisos, bem como evitar arbitrariedades.

Os artigos 42 a 44 do Anteprojeto dispõe sobre o uso das tecnologias de monitoramento, como os sistemas de reconhecimento facial, fixando critérios para sua implementação. Conforme previsão do artigo 42, toda e qualquer tecnologia de alto risco para direitos, liberdades e garantias para os titulares dos dados - o que se encaixa perfeitamente aos sistemas de reconhecimento facial, dado às inúmeras situações de suas falibilidades que culminaram na prisão de inocentes -, somente pode ser utilizada mediante previsão legal. Por sua vez, o artigo 43, dispõe que:

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

A vedação prevista no referido artigo é de extrema relevância, uma vez que restringe o uso de sistemas de controle populacional para identificar pessoas indeterminadas de maneira contínua e em tempo real. A vedação prevista é relevante tendo em vista que impede o comprometimento dos direitos de ir e vir, bem como impede o monitoramento constante e impedimento do uso desses sistemas serem direcionados de forma seletiva, especialmente com a população negra e periférica, como é o caso dos casos de falibilidade dos sistemas utilizados no Brasil.

Ainda com relação ao Anteprojeto, os artigos 29 e 33 preveem a obrigatoriedade de relatórios de impacto e registro de tratamento de dados.

O PL 1515/2022, por sua vez, apesar de se apresentar como um projeto similar ao Anteprojeto, é criticado por enfraquecer princípios fundamentais. Uma análise técnica realizada pelo Instituto de Referência em Internet e Sociedade (IRIS) e pelo Laboratório de Políticas Públicas e Internet (LAPIN) destaca os riscos à proteção de dados pessoais no contexto da segurança pública. (IRIS; LAPIN, 2022)

É possível observar mudanças significativas com relação ao Anteprojeto, uma vez que o PL suprime diversas garantias dos titulares e amplia excessivamente o poder discricionário do Estado (AZEVEDO, et. al, 2022). A nota também aponta que o projeto de lei enfraquece o sistema de proteção de dados ao suprimir princípios fundamentais, como a proporcionalidade e a responsabilização.

Outro ponto é a ampliação do campo de aplicação da lei, pois além de abarcar a área da segurança pública e persecução penal, prevê também a atuação da lei nas áreas de defesa nacional, segurança do Estado e inteligência.

Além disso, o PL adota o princípio da auditabilidade, em substituição ao princípio da responsabilização e prestação de contas, sendo que o primeiro é mais brando e vago, não garantindo a efetiva supervisão dos agentes públicos.

Por último, o projeto enfraquece severamente os direitos dos titulares, ao anular garantias como o direito de solicitar bloqueio ou eliminação de dados desnecessários, além de permitir o compartilhamento irrestrito de dados entre órgãos públicos e privados, inclusive sem autorização judicial ou previsão legal, criando um contexto de insegurança e risco à proteção dos direitos fundamentais.

Em análise às propostas legislativas, percebe-se que o PL 2338/2023 e o Anteprojeto da LGPD Penal se mostram os mais adequados no contexto dos sistemas de reconhecimento facial, em especial o APL, que estabelece princípios fundamentais, diferenciação no tratamento dos dados, se apresentando como uma estrutura mais aprofundada e garantista. A proposta do APL revela ser a mais apropriada no que diz respeito aos impactos do racismo algorítmico e a regulamentação no uso de tecnologias de reconhecimento facial no contexto da segurança pública e processo penal, visando que estas ferramentas não se tornem instrumentos de injustiça e violação de direitos.

Por fim, uma proposta técnica é remover os atributos como raça, gênero e localização geográfica presente nos dados utilizados para desenvolver os algoritmos de aprendizado de máquina. Essa remoção visa alcançar a neutralidade algorítmica e um modelo livre de vieses preconceituosos (CHAVES JUNIOR; GUASQUE; PADUA, 2023). Considerando a crescente adoção das tecnologias de reconhecimento facial, é essencial que o Estado incorpore diretrizes como essa em

suas políticas públicas, especialmente quando os algoritmos são utilizados em contextos sensíveis como a segurança pública e o sistema penal.

Considerações finais

O presente trabalho foi desenvolvido em razão da necessidade de se discutir as falhas das tecnologias de reconhecimento facial e os impactos no sistema penal brasileiro. Os avanços da inteligência artificial, especialmente no que se refere a essas ferramentas, trazem a necessidade de um debate acerca dos limites éticos, jurídicos e sociais dessas tecnologias.

Verificou-se que, embora o reconhecimento facial seja apresentado como uma ferramenta que possui alguma eficácia na segurança pública, no que diz respeito à identificação de suspeitos e no controle da criminalidade, os inúmeros casos de prisões injustas comprovam que a ausência de uma regulamentação da tecnologia pode se tornar um mecanismo de violação de direitos fundamentais.

A análise desenvolvida reflete as desigualdades estruturais do sistema penal brasileiro, e demonstra como as ferramentas tecnológicas estão distantes de serem uma solução neutra e objetiva, considerando que a maioria dos erros dos dispositivos alcança pessoas negras e pobres, grupos historicamente afetados pela seletividade penal. Conforme demonstrado, estes erros não ocorrem por mera causalidade, mas em razão da presença do racismo algorítmico nas tecnologias de reconhecimento facial: os sistemas são treinados por seres humanos que podem, propositalmente ou não, reproduzir vieses raciais e padrões discriminatórios já existentes na sociedade.

Nesse viés, salienta-se a necessidade da atuação do Estado para garantir a proteção dos direitos fundamentais e impedir que os dispositivos reproduzam falhas e preconceitos presentes na sociedade e no sistema penal. O estudo apresentou como proposta a criação de uma regulamentação específica do uso do reconhecimento facial no Brasil, que deve ser acompanhada de políticas visando a transparência, neutralidade algorítmica e diversidade nas equipes.

Nesse sentido, foram analisadas algumas propostas legislativas, entre as quais destaca-se o Anteprojeto de Lei de Proteção de Dados Pessoais para

Segurança Pública e Persecução Penal (APL), que se apresenta como a mais adequada em razão de estabelecer princípios fundamentais, diferenciar o tratamento de dados e enfrentar os impactos do racismo algorítmico.

Conclui-se, portanto, que o Brasil ainda precisa avançar na discussão de uma regulamentação eficaz referente ao uso das ferramentas de reconhecimento facial no âmbito da segurança pública e do sistema penal, e o Anteprojeto de Lei surge como uma perspectiva promissora para o futuro dessas tecnologias.

Referências

ALENCAR, Itana. **Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por 'racismo algorítmico'**; inocente ficou preso por 26 dias. G1, Bahia, 01 set. 2023. Disponível em: https://g1.globo.com/google/amp/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoes-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-preso-por-26-dias.ghtml. Acesso em: 28 jul. 2025.

ALMEIDA, Silvio Luiz de. **Racismo Estrutural**. São Paulo: Pólen, 2019. Disponível em: https://sites.ufpe.br/enegrecer/wp-content/uploads/sites/146/2023/01/ALMEIDA-Silvio-Racismo-estrutural-Livro-2019.pdf. Acesso em: 05 ago. 2025.

AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. Disponível em: . Acesso em: 03/08/2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 05 ago. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 ago. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Políticas Penais. **Levantamento Nacional de Informações Penitenciárias** – *INFOPEN: 1º semestre de 2024*. Brasília, 2024. Disponível em: https://www.gov.br/senappen/pt-br/assuntos/noticias/senappen-divulga-levantamento-de-informacoes-penitenciarias-referente-ao-primeiro-semestre-de-2024/relipen-1-semestre-de-2024.pdf/view

BRASIL. **Projeto de Lei n. 1515/2022**. Disponível em: https://www.camara.leg.br/propostas-legislativas/2326300. Acesso em: 05 ago. 2025.

BRASIL. **Projeto de Lei n. 2338/2023**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262. Acesso em: 05 ago. 2025.
CERQUEIRA, Daniel; BUENO, Samira (coord.). **Atlas da violência 2024.** Brasília: Ipea; FBSP, 2024. Disponível em: https://publicacoes.forumseguranca.org.br/items/81f69453-baf0-4e6a-9f61-f4f6950b1317. Acesso em: 05 ago. 2025.

CHAVES JUNIOR, Airto; GUASQUE, Bárbara; PADUA, Thiago Santos Aguiar de. **Segregação racial e vieses algorítmicos:** máquinas racistas no âmbito do controle penal. Revista Brasileira de Direito, v. 19, n. 2, p. 4768, 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.

DA SILVA, Mozart Linhares; ARAÚJO, Willian Fernandes. **Biopolítica, racismo estrutural-algorítmico e subjetividade**. Educação Unisinos, v. 24, n. 1, p. 1-20, 2020.

DE AGUIAR ARAÚJO, Rômulo de; DEPERON CARDOSO, Naiara Deperon; MARCÉLIA DE PAULA, Amanda. **Regulação e uso do reconhecimento facial na segurança pública do Brasil**. *Revista de Doutrina Jurídica*, Brasília, DF, v. 112, n. 00, p. e021009, 2021. DOI: 10.22477/rdj.v112i00.734. Disponível em: https://revistajuridica.tjdft.jus.br/index.php/rdj/article/view/734. Acesso em: 22 ago. 2025.

DE ALMEIDA, José Antonio Caldeira et al. **TECNOLOGIAS DE RECONHECIMENTO FACIAL:** O RACISMO ALGORÍTMICO COMO INSTRUMENTO DE POLÍTICA DE SEGURANÇA PÚBLICA. Revista Eletrônica Direito e Política, v. 20, n. 1, p. 202-219, 2025.

EloInsights. **O que é racismo algorítmico e como superá-lo**. **EloGroup Insights**, 16 nov. 2022. Disponível em: https://elogroup.com/insights/o-que-e-racismo-algoritmico-e-como-supera-lo/. Acesso em: 31 jul. 2025.

FANTÁSTICO. **Medo, frustrado e constrangido', diz homem detido por engano em estádio após erro do sistema de reconhecimento facial**. 21 abr. 2024. Disponível em: https://g1.globo.com/google/amp/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml. Acesso em: 31 jul. 2025.

Instituto Igarapé. **Reconhecimento facial no Brasil**. Rio de Janeiro, 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 05 ago. 2025.

IT Forum. **Diagnostico comportamental dos profissionais de TI**: Quais são os desafios, motivadores e o que buscam os executivos que atuam na área de Tecnologia. São Paulo, 2024. Disponível em: https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F504542%2F1726512743E-book_Carreira_Tech.pdf. Acesso em: 02 ago 2025.

MBEMBE, Achille. **Necropolítica. Arte & ensaios**, n. 32, p. 122-151, 2016. Disponível em:https://www.procomum.org/wpcontent/uploads/2019/04/necropolitica.pdf. Acesso em: 29 jul 2025.

MESQUITA, Clívia. RJ: **Jovem negro acusado por reconhecimento facial é inocentado pela terceira vez**. Brasil de fato, Rio de Janeiro, 06 out. 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: 28 jul. 2025.
MIRANDA, Pedro Fauth Manhães.; SCHNEIDER, Camila Berlim. Vigilância e segurança pública: preconceitos e segregação social ampliados pela suposta neutralidade digital. **Emancipação**, v. 20, p. 1–22, 2020. Disponível em: https://revistas.uepg.br/index.php/emancipacao/article/view/14258 Acesso em: 29 jul. 2025.

Nunes, P. **Novas ferramentas, velhas práticas:** reconhecimento facial e policiamento no Brasil. In: Centro de Estudos de Segurança e Cidadania. Retratos da violência cinco meses de monitoramento, análises e descobertas. Rio de Janeiro: CESEC, 2019. p. 67-71, Disponível em: http://observatorioseguranca.com.br/wordpress/wp-content/uploads/2019/11/1relatoriorede.pdf. Acesso em: 19 jul. 2025.

SILVA, Tarcízio. **Google acha que ferramenta em mão negra é uma arma**. 02 abr. 2020. Disponível em: https://tarciziosilva.com.br/blog/google-acha-que-ferramenta-em-mao-negra-e-uma-arma/. Acesso em: 29 jul. 2025.

SILVA, Tarcízio. **Racismo algorítmico: inteligência artificial e discriminação nas redes digitais**. Edições Sesc SP, 2022. Disponível em: https://assets.pubpub.org/7bm06qr3/61661883837114.pdf. Acesso em: 05 ago. 2025.

TAVARES, Josafá. **Representatividade negra na TI**. Rio de Janeiro, 2024. Disponível em: https://www.mindtek.com.br/2024/11/representatividade-negra-na-tecnologia/. Acesso em: 02 ago. 2025.