

UNIVERSIDADE FEDERAL DE JUIZ DE FORA - CAMPUS AVANÇADO
GOVERNADOR VALADARES
BACHARELADO EM DIREITO

Lara Lacerda Marques

Do controle disciplinar à vigilância digital: o reconhecimento facial e a reprodução do racismo no sistema penal brasileiro

Governador Valadares/MG

2026

Lara Lacerda Marques

Do controle disciplinar à vigilância digital: o reconhecimento facial e a reprodução do racismo no sistema penal brasileiro

Trabalho de Conclusão de Curso apresentado ao Departamento de Direito como requisito parcial à obtenção do título de Bacharela em Direito da Universidade Federal de Juiz de Fora – Governador Valadares/MG.

Prof. Orientador: Me. João Pedro Teixeira de Faria Viana

Governador Valadares/MG

2026

Lara Lacerda Marques

Do controle disciplinar à vigilância digital: o reconhecimento facial e a reprodução do racismo no sistema penal brasileiro

Trabalho de Conclusão de Curso apresentado ao Departamento de Direito como requisito parcial à obtenção do título de Bacharela em Direito da Universidade Federal de Juiz de Fora – Governador Valadares/MG.

Aprovada(o) em: ____ de _____ de 2026.

BANCA EXAMINADORA

Prof. Me. João Pedro Teixeira de Faria Viana - Orientador
Universidade Federal de Juiz de Fora - Campus Governador Valadares

Profa. Dra. Tayara Talita Lemos
Universidade Federal de Juiz de Fora - Campus Governador Valadares

Prof. Dr. Renato Santos Gonçalves
Universidade Federal de Juiz de Fora - Campus Governador Valadares

RESUMO

Este trabalho tem como objetivo investigar a forma como a vigilância no sistema penal se atualiza no uso de câmeras de segurança que utilizam sistemas de inteligência artificial e como o racismo também se reproduz na forma algorítmica. O cenário atual revela uma transição dos modelos disciplinares tradicionais para uma cultura de vigilância onipresente sustentada pela dataficação de comportamentos sociais, a qual se integra a um sistema penal brasileiro historicamente estruturado pela seletividade racial e pelo mito da democracia racial. A metodologia utilizada consistiu em uma revisão bibliográfica fundamentada em produções teóricas que tratam da datavigilância e do racismo algorítmico, além da realização de estudos de casos concretos envolvendo prisões injustas decorrentes de falhas em tecnologias de reconhecimento facial. Os resultados demonstram que o reconhecimento facial atua como um instrumento de etiquetamento tecnológico que automatiza a seletividade penal contra a juventude negra, evidenciando a necessidade de estabelecer *standards* probatórios rígidos e transparência algorítmica para garantir a proteção dos direitos fundamentais na era digital.

Palavras-chave: Reconhecimento facial; Racismo algorítmico; Sistema penal brasileiro; Seletividade penal; Vigilância digital.

ABSTRACT

This study aims to investigate how surveillance in the penal system is updated through the use of security cameras employing artificial intelligence systems and how racism is also reproduced in an algorithmic form. The current scenario reveals a transition from traditional disciplinary models to an omnipresent surveillance culture sustained by the datafication of social behaviors, which is integrated into a Brazilian penal system historically structured by racial selectivity and the myth of racial democracy. The methodology employed consisted of a bibliographic review based on theoretical productions dealing with dataveillance and algorithmic racism, in addition to conducting studies of concrete cases involving wrongful arrests resulting from failures in facial recognition technologies. The results demonstrate that facial recognition acts as an instrument of technological labeling that automates penal selectivity against Black youth, highlighting the need to establish strict evidentiary standards and algorithmic transparency to ensure the protection of fundamental rights in the digital age.

Keywords: Facial recognition; Algorithmic racism; Brazilian penal system; Penal selectivity; Digital surveillance.

SUMÁRIO

1 INTRODUÇÃO.....	5
2 A CULTURA DE VIGILÂNCIA E A INTEGRAÇÃO DO RECONHECIMENTO FACIAL AO SISTEMA PENAL BRASILEIRO.....	6
3 A SELETIVIDADE PENAL E O ETIQUETAMENTO TECNOLÓGICO A PARTIR DAS BASES RACISTAS DO SISTEMA PENAL BRASILEIRO.....	12
4 A EVIDÊNCIA DO RACISMO ALGORÍTMICO: ESTUDO DOS CASOS DE JOÃO ANTÔNIO BASTOS E AILTON ALVES DE SOUSA.....	16
5 CONSIDERAÇÕES FINAIS.....	21
REFERÊNCIAS.....	23

1 INTRODUÇÃO

O presente trabalho analisa a transição das formas tradicionais de controle social para os novos mecanismos de vigilância digital no contexto do sistema penal brasileiro. Esta investigação parte da premissa de que o poder punitivo se atualiza em novas formas de controle ao longo da história para a manutenção do modelo disciplinar, firmado a partir da evolução do suplício físico contra o corpo para o controle da mente e do comportamento humano (Foucault, 1975). Para o referido autor, essa transformação histórica marcou o fim dos rituais violentos de execução pública e deu lugar a uma economia de direitos suspensos na qual o psiquismo do indivíduo é moldado por técnicas de poder.

A partir desse contexto surgiu a pergunta que orienta o trabalho: os sistemas de reconhecimento facial utilizados pela segurança pública correspondem a novas formas de controle e reprodução do racismo pelo sistema penal brasileiro?

O objetivo central deste estudo é investigar como a vigilância biométrica atua como um mecanismo de etiquetamento tecnológico que precede a própria investigação criminal, fundamentando-se nas lições de Howard Becker (2008) sobre a aplicação do rótulo de periculosidade. Para alcançar essa finalidade, o trabalho aborda as bases teóricas do controle disciplinar e da datavigilância, além da construção histórica da seletividade no sistema punitivo nacional descrita por Ana Luiza Flauzina (2006). No decorrer da pesquisa, analisa-se o ordenamento jurídico vigente e as recentes diretrizes do Superior Tribunal de Justiça e do Conselho Nacional de Justiça sobre a validade da prova de reconhecimento.

Para responder o questionamento, a pesquisa privilegia a revisão bibliográfica a fim de identificar os processos de atualização da vigilância e do racismo em seus formatos algorítmicos. Parte das contribuições de David Lyon (1994) ao tratar da forma como o avanço tecnológico atualizou a vigilância, que ultrapassou os muros das prisões e consolidou uma cultura de vigilância onipresente que se manifesta em dispositivos cotidianos como câmeras e celulares. Somado a isso, volta-se para as contribuições de José Van Dijck (2014) ao explicar que esse novo modelo de controle social é sustentado pelo processo técnico de dataficação, o qual consiste na conversão de comportamentos e práticas sociais em dados digitais processáveis por computadores.

O trabalho se divide em três capítulos, sendo que, no primeiro, investiga-se como a cultura da vigilância é reproduzida desde o surgimento das prisões e como ela foi apropriada pelo poder punitivo ao longo do tempo, atualizando-se nos modelos automatizados mais recentes. Com isso, investiga-se a chamada datavigilância (Van Dijck, 2014) enquanto

observação massiva e invisível do Estado por meio do processamento de metadados, explicando como funciona a monitoração por câmeras de segurança controladas por sistemas de inteligência artificial, bem como a forma como o reconhecimento de pessoas, que já possui suas problemáticas enquanto meio de prova, é reutilizado por esses sistemas. O segundo capítulo volta para o contexto histórico brasileiro, marcado pela colonização e pelo racismo estrutural. Nesse tópico, retoma-se a contribuição de Ana Flauzina (2006) a respeito da relação direta entre racismo e sistema penal, além de outros trabalhos que estudam a reprodução do racismo no meio digital e algorítmico.

Por fim, o estudo examina casos concretos de “erros” policiais derivados de falhas biométricas, como os episódios envolvendo João Antônio Bastos e Ailton Alves de Sousa, no contexto de espaços públicos, demonstrando a necessidade urgente de standards probatórios rígidos para a proteção dos direitos fundamentais na era digital. Através dessa análise, pretende-se evidenciar que a inovação tecnológica deve estar submetida ao controle judicial e à ética algorítmica para evitar que a modernização da segurança pública sirva apenas para perpetuar injustiças históricas contra a população negra.

2 A CULTURA DE VIGILÂNCIA E A INTEGRAÇÃO DO RECONHECIMENTO FACIAL AO SISTEMA PENAL BRASILEIRO

Historicamente, as formas tradicionais de punição e controle pelo poder punitivo fundamentaram-se na transição do suplício contra o corpo físico do condenado para a vigilância e o controle de sua “alma” (mente e comportamento), conforme analisa Foucault em sua obra “Vigiar e Punir”. O autor demonstra que, entre o final do século XVIII e o início do XIX, o corpo deixou de ser torturado como espetáculo público e passou a ser alvo de uma “economia de direitos suspensos”, enquanto modelo de punição que não busca ferir a carne, mas sim retirar direitos legais do indivíduo, como a sua liberdade. Nessa nova lógica, a alma se torna a “prisão do corpo”, a consciência e o psiquismo do indivíduo são moldados por técnicas de poder para que ele mesmo passe a controlar suas ações físicas e hábitos (Foucault, 1975).

Nesse novo modelo, o corpo passa a ser um meio para que o sistema obrigue o indivíduo a se transformar, utilizando um controle rígido do tempo, dos gestos e das atividades diárias. Foucault (1975) descreve essa transição como o fim da “melancólica festa da punição”, referindo-se aos rituais violentos de execução pública que serviam de espetáculo

e o surgimento do "enterramento burocrático da pena", com o isolamento discreto e administrativo do condenado dentro das prisões, longe dos olhos da sociedade.

Essa vigilância exercida pelo Estado modernizou-se, ultrapassando os muros das prisões para consolidar o que David Lyon (1994) define como "cultura de vigilância". Esse conceito descreve um estilo de vida contemporâneo em que o monitoramento se torna onipresente, manifestando-se em dispositivos do cotidiano como câmeras, celulares e scanners. Esse novo modelo de controle é sustentado pela “dataficação”, processo técnico, descrito por José Van Dijck (2014), como a conversão de comportamentos, gestos e práticas sociais em dados quantificáveis que podem ser processados por computadores.

A partir dessa transformação das ações humanas em informação digital, estabelece-se a "datavigilância" (Van Dijck, 2014), que consiste na observação contínua, invisível e massiva desses dados por parte de governos e grandes empresas. Assim, enquanto o Panóptico de Bentham baseava-se na visibilidade constante do detento dentro de uma arquitetura física de torres e celas, a contemporaneidade permite que o Estado substitua ou complete esse confinamento por mecanismos digitais. Exemplos claros dessa transição são o uso de tornozeleiras eletrônicas e o monitoramento biométrico, que permitem vigiar o indivíduo em tempo real, mesmo quando ele não está fisicamente trancado em uma instituição.

Nesse mesmo viés, Bezerra e Costa (2022) explicam que a evolução tecnológica permite a conversão de comportamentos e práticas sociais em dados quantificáveis, consolidando o poder nas mãos de grandes corporações e do Estado por meio da extração massiva de metadados. Dessa forma, os mecanismos de aplicação do poder punitivo estatal foram reconfigurados pelo que se denomina "capitalismo de dados"¹, um modelo econômico baseado na transformação de informações pessoais em mercadoria e instrumentos de controle. A punição e a vigilância, que antes dependiam da presença física de um inspetor, como o Panóptico, agora utilizam o Big Data, o processamento e a análise de volumes massivos de dados digitais para identificar padrões e a Inteligência Artificial para traçar perfis e realizar previsões comportamentais, detectando o que as autoridades classificam como "potencial criminoso", a partir de uma suposição estatística de que alguém pode vir a cometer um delito com base em seus rastros digitais (Bezerra, Costa, 2022).

Dentro dessa nova arquitetura de fiscalização, o reconhecimento facial desponta como o instrumento central de controle ao converter a biometria humana em dados processáveis

¹O termo "capitalismo de dados" utilizado pelos autores refere-se ao conceito de *data capitalism* (ou *data-centric capitalism*) desenvolvido por Evgeny Morozov em 2015, que caracteriza o atual modo de produção informacional dominante baseado na exploração comercial de metadados e na vigilância algorítmica (Bezerra, Costa, 2022).

para identificação instantânea (Silva; Silva, 2019). Historicamente, o uso da fotografia para identificar suspeitos remonta ao ano de 1852, na Suíça, com Karl Durkheim, consolidando-se na Inglaterra em 1870 por meio do registro dos chamados “criminosos habituais” (Oliveira, 2023). Essa utilização de registros visuais foi integrada ao ordenamento processual e formalizada no instituto jurídico do reconhecimento de pessoas, estabelecendo-se como um meio de prova destinado à identificação da autoria delitiva por meio de processos comparativos. Em termos técnicos atuais, o funcionamento dessa ferramenta baseia-se em um procedimento sequencial que detecta um rosto em uma cena e extrai pontos característicos, transformando essas métricas em um vetor matemático (Mello, 2025). Na sequência, este vetor é confrontado com registros armazenados em bancos de dados para gerar um índice de semelhança estatística denominado *match* (Mello, 2025).

É relevante destacar que as bases de dados que alimentam esses sistemas podem ser compostas tanto por fotografias reais de registros estatais quanto por imagens geradas por Inteligência Artificial (IA). Recentemente, a Portaria nº 1.122/2026 do Ministério da Justiça regulamentou o uso da IA para a criação de *fillers*, que são pessoas sintéticas com características compatíveis com a descrição da testemunha, visando evitar o uso de fotos de inocentes em alinhamentos (Maranhão, 2026). Contudo, a tecnologia opera de forma probabilística e não determinística, o que significa que o sistema não afirma com certeza absoluta a identidade, mas apenas aponta uma probabilidade dentro de um limiar definido, exigindo que o resultado seja tratado juridicamente como um indício (Mello, 2025).

O reconhecimento facial, por sua vez, caracteriza-se como uma tecnologia de identificação biométrica que utiliza algoritmos automatizados para extrair e organizar padrões a partir de imagens ou vídeos. Segundo Silva e Silva (2019), essa ferramenta busca proporcionar uma percepção de maior eficiência e segurança no contexto das cidades inteligentes ao converter traços biológicos humanos em dados processáveis. Em termos técnicos, o procedimento inicia-se com a detecção de um rosto em uma cena, seguida da extração de pontos característicos específicos, a exemplo da distância entre os olhos e o contorno facial, transformando essas métricas em um vetor matemático. Conforme Mello (2025), esse vetor é confrontado com registros previamente armazenados em bancos de dados para gerar um índice de semelhança que, ao atingir um patamar de probabilidade estabelecido pelos desenvolvedores, indica a ocorrência de um “*match*”, termo técnico que designa a correspondência estatística entre as imagens.

No cenário brasileiro, a implementação desta tecnologia tem sido promovida como um símbolo de modernização da segurança pública, sendo adotada sob a justificativa de conferir

agilidade ao combate à criminalidade urbana. Atualmente, o país conta com centenas de projetos ativos em diversas unidades da federação, abrangendo milhões de cidadãos sob potencial monitoramento estatal. Conforme detalha Lima (2022), o principal objetivo prático dessas iniciativas reside na localização em tempo real de pessoas com mandados de prisão em aberto ou na identificação de indivíduos desaparecidos, permitindo que o Estado exerça um controle territorial mais incisivo, especialmente em grandes aglomerações e infraestruturas críticas.

A aplicação material dessa tecnologia pode ser observada de forma emblemática em eventos de massa e sistemas de transporte de diversos estados. Os governos do Rio de Janeiro e da Bahia foram pioneiros ao utilizarem projetos-piloto durante o Carnaval de 2019 para monitorar foliões e identificar suspeitos em meio às multidões. No Rio de Janeiro, o sistema também foi aplicado em ambientes esportivos, a exemplo do Estádio do Maracanã, onde levantamentos realizados por meio da Lei de Acesso à Informação revelaram que, de 11 detenções efetuadas com base na biometria facial, 63% resultaram em falsos positivos, o que evidencia a fragilidade técnica da ferramenta. Além disso, o estado da Bahia consolidou a implementação massiva da tecnologia para monitorar a capital, Salvador, e outros 77 municípios do interior (Lima, 2022; Bezerra, Costa, 2022). A cidade de Recife também expandiu sua capacidade de vigilância com equipamentos dotados de zoom óptico de longo alcance e rotação de 360 graus, consolidando o reconhecimento facial como eixo central das novas estratégias de policiamento ostensivo no Brasil (Lima, 2022; Oliveira, 2023).

No âmbito da capital paulista o Decreto Municipal nº 63.552/2024 institucionalizou o Programa Smart Sampa, instituído sob a gestão da Secretaria Municipal de Segurança Urbana (SMSU), consolidando uma infraestrutura de vigilância urbana permanente que integra cerca de 20.000 câmeras dotadas de inteligência artificial (São Paulo, 2024). O sistema utiliza o software de origem russa FindFace Multi, da empresa NtechLab, o qual é capaz de extrair características biométricas em tempo real e gerar alertas automáticos sempre que o índice de similaridade com bancos de dados oficiais supera o patamar de 90%. Todavia a execução do programa é regida pelo Procedimento Operacional Padrão (POP) nº 16/2025, o qual estabelece uma lógica de resposta imediata com validação humana residual por parte do Operador de Telecomunicações.

Tal arquitetura operacional tensiona garantias fundamentais visto que a coleta massiva de dados biométricos em espaços públicos ocorre sob uma opacidade algorítmica que dificulta o exercício do contraditório, transformando a presunção de inocência em um risco estatístico (Molero, 2025). Por conseguinte a integração dessas tecnologias ao policiamento ostensivo

consolida o reconhecimento facial como o eixo central de uma nova governança algorítmica que reproduz desigualdades históricas sob um verniz de modernização tecnológica (Molero, 2025; Lima, 2022; Oliveira, 2023).

Essa nova tecnologia, embora apresentada como inovação disruptiva, aproveita e potencializa as fragilidades históricas do reconhecimento de pessoas, utilizado como meio de prova para identificar o autor de um crime por meio de um processo psicológico de comparação entre a percepção sensorial do fato e as lembranças armazenadas no passado (Oliveira, 2023; Lopes, 2011). No ordenamento jurídico brasileiro, o procedimento é regido pelo Código de Processo Penal (CPP), que estabelece o seguinte rito formal (Brasil, 1941):

Art. 226. Quando houver necessidade de fazer-se o reconhecimento de pessoa, proceder-se-á pela seguinte forma:

I - a pessoa que tiver de fazer o reconhecimento será convidada a descrever a pessoa que deva ser reconhecida;

II - a pessoa, cujo reconhecimento se pretender, será colocada, se possível, ao lado de outras que com ela tiverem qualquer semelhança, convidando-se quem tiver de fazer o reconhecimento a apontá-la;

III - se houver razão para recear que a pessoa chamada para o reconhecimento, por efeito de intimidação ou outra influência, não diga a verdade em face da pessoa que deve ser reconhecida, a autoridade providenciará para que esta não veja aquela;

IV - do ato de reconhecimento lavrar-se-á auto pormenorizado, subscrito pela autoridade, pela pessoa chamada para proceder ao reconhecimento e por duas testemunhas presenciais.

Parágrafo único. O disposto no III deste artigo não terá aplicação na fase da instrução criminal ou em plenário de julgamento.

Complementando esse rito, o artigo 228 do CPP funciona como uma salvaguarda contra a contaminação cognitiva mútua, evitando o risco de que o relato ou a opinião de uma pessoa influencie indevidamente a lembrança de outra. Conforme explicam Oliveira (2023) e Mello (2025), essa norma determina que, havendo mais de um reconhecedor, cada um deve realizar o ato separadamente para evitar o fenômeno das "falsas memórias", baseadas em lembranças distorcidas ou de eventos que nunca ocorreram, frequentemente causadas por sugestões externas ou falhas naturais do cérebro (Stein; Pergher, 2001).

É imperativo salientar que, no âmbito da Teoria das Provas, o reconhecimento de pessoas possui uma natureza probabilística e não determinística. Isso significa que o sistema não afirma com certeza absoluta a identidade do indivíduo, mas aponta apenas uma probabilidade estatística de correspondência dentro de um limite pré-definido. Por essa razão, autores como Mello (2025) e Oliveira (2023) criticam a tentativa de equiparar esse índice matemático a uma prova robusta de autoria, classificando-o como um elemento informativo frágil que, sob o prisma da presunção de inocência, exige obrigatoriamente a corroboração por outros meios independentes para superar a dúvida razoável.

Todavia, a aplicação prática desses dispositivos enfrenta graves discussões jurídicas, visto que por décadas a jurisprudência tratou tais formalidades como “mera recomendação”, permitindo a validação de identificações informais viciadas (Mello, 2025). Uma prática comum é o *show-up*, que consiste na exibição isolada de uma fotografia para confirmação da vítima, o que induz ao erro e reforça a produção do suspeito natural (Oliveira, 2023). Nesse contexto, a Inteligência Artificial agrava a seletividade ao reatualizar o positivismo criminológico, associando a delinquência a fenótipos específicos (Oliveira, 2023). O “criminoso nato” lombrosiano habita hoje o imaginário algorítmico, convertendo traços físicos de grupos minorizados em indícios de potencial criminal (Oliveira, 2023).

Diante desses riscos, a Lei Geral de Proteção de Dados (LGPD) impõe limites ao classificar a biometria como dado pessoal sensível (Brasil, 2018). Embora existam exceções para a segurança pública, o tratamento de tais dados não confere um “cheque em branco” ao Estado, devendo respeitar a transparência e a dignidade humana (Bezerra; Costa, 2022). Para interromper o ciclo de injustiças, o Tema 1.258 do Superior Tribunal de Justiça (STJ) fixou a tese de que a inobservância do rito legal torna a prova inválida, enquanto a Resolução nº 484 do CNJ instituiu diretrizes rígidas, como a obrigatoriedade da gravação audiovisual integral do ato (STJ, 2025; CNJ, 2022).

Nesse sentido, as imagens produzidas pelo reconhecimento de pessoas, enquanto meio de prova, são frequentemente integradas aos bancos de dados de sistemas de Inteligência Artificial, replicando as fragilidades da prova no ambiente digital (Mello, 2025). Essa transposição, operada sem a devida observância da cadeia de custódia, automatiza e propaga falhas de identificação em escala massiva. Tal dinâmica converte o erro informativo em um catalisador da seletividade penal ao classificar corpos a partir de métricas probabilísticas que comprometem a presunção de inocência (Fernandes; Pietrani, 2025).

Essa atualização tecnológica, portanto, não é neutra. Conforme identificado por Lima (2022), o aparato tecnológico é alimentado por bases de dados que refletem o racismo estrutural, compreendido como o conjunto de práticas históricas, hábitos e situações que privilegiam um grupo racial em detrimento de outro. Com isso, o reconhecimento facial transforma-se em um fenômeno sociotécnico, um processo onde fatores sociais e ferramentas técnicas atuam de forma conjunta e que atinge seletivamente a população negra. O racismo algorítmico aparece, então, como a reprodução e automação de desigualdades raciais por meio de cálculos matemáticos e programas de computador e atua, portanto, como uma “camada adicional” ao racismo histórico, realizando uma ordenação racializada da violência e

dos recursos de segurança, resultando na distribuição desigual de policiamento e punição com base na cor da pele em prejuízo de grupos minorizados (Silva, 2022).

Nesse sentido, Mello (2025) argumenta que o reconhecimento facial é frequentemente transformado de um "indício probabilístico", caracterizado por uma informação baseada apenas em chances estatísticas, em uma "certeza jurídica", ou um fato aceito pelo tribunal como verdade absoluta. Conforme explica o autor, essa interpretação transfere todo o risco de falhas tecnológicas para o acusado, uma vez que a falta de transparência no funcionamento dos algoritmos e o uso do segredo comercial impedem que a defesa analise e identifique erros no sistema. Isso obriga o réu a tentar comprovar sua inocência contra um resultado automatizado que a própria instituição muitas vezes não consegue explicar detalhadamente, atingindo de maneira seletiva a juventude negra das periferias.

Sob essa ótica, volta-se à investigação do uso dessas ferramentas digitais como forma de perpetuação do projeto colonial de controle social (Flauzina, 2006), com a manutenção de antigas estruturas de dominação e exclusão sob uma máscara de neutralidade técnica, que utiliza métodos matemáticos para legitimar a seletividade e a violência do sistema penal brasileiro (Bezerra; Costa, 2022). No sistema penal brasileiro, portanto, vigiar é uma forma de exercer poder. O reconhecimento facial, que hoje se apresenta como uma inovação tecnológica voltada à segurança pública, não representa uma ruptura com as formas tradicionais de controle, mas sim a continuidade de práticas históricas que incidem, de forma seletiva, sobre determinados grupos sociais (Silva; Silva, 2019; Mello, 2025).

3 A SELETIVIDADE PENAL E O ETIQUETAMENTO TECNOLÓGICO A PARTIR DAS BASES RACISTAS DO SISTEMA PENAL BRASILEIRO

A análise do sistema carcerário brasileiro demonstra que as prisões indevidas são o resultado de um processo estrutural de seletividade que utiliza, por exemplo, o reconhecimento de pessoas como um instrumento de exclusão. Relatórios do Conselho Nacional de Justiça (CNJ) indicam a gravidade desse cenário ao revelar que 83% das pessoas presas injustamente por erros de reconhecimento no Brasil são negras (Costa; Jesus, 2025; Lima, 2022).

Para compreender como a inovação tecnológica se converte em um instrumento de seletividade penal, com a tendência do sistema de justiça em escolher e perseguir grupos específicos, é fundamental recorrer às lições da Teoria do Etiquetamento (*Labelling*

Approach), sistematizada por Howard Becker (2008). Segundo essa perspectiva teórica, a criminalidade não é uma qualidade natural ou intrínseca de um ato, mas sim o resultado de um processo de reação social e institucional; em outras palavras, o "desviante" ou criminoso é aquele a quem o Estado e a sociedade aplicaram o rótulo de perigoso.

Nesse contexto, o processo de etiquetamento ocorre de forma automatizada e sistêmica no ambiente digital. Conforme explicam Mello (2025) e Oliveira (2023), o Estado realiza uma pré-seleção dos alvos da sua força punitiva ao alimentar bancos de dados e álbuns de suspeitos que contém fotografias de pessoas negras, muitas vezes extraídas de redes sociais sem qualquer critério técnico ou cadeia de custódia. Desse modo, a tecnologia deixa de ser apenas uma ferramenta de identificação para se tornar um mecanismo que define, antecipadamente, quem são as pessoas que devem ser vigiadas pelas autoridades.

Essa dinâmica resulta na criação do "suspeito natural", aquele que é construído socialmente como culpado apenas por sua aparência ou cor da pele, antes mesmo de qualquer investigação. Como observa Oliveira (2023), o uso desses álbuns em delegacias, sem uma devida regulação normativa, leis específicas que controlem sua aplicação, acaba por induzir as vítimas ao erro ao apresentar-lhes indivíduos que já foram previamente estigmatizados, ou seja, marcados negativamente pelo sistema penal. Nesse sentido, como alertam Bezerra e Costa (2022), esse rótulo digital, uma vez inserido no sistema de vigilância, torna-se uma marca indelével, pois o cidadão passa a despertar desconfiança constante apenas por constar em uma base de dados que reproduz e automatiza o racismo estrutural, transformando a tecnologia em um novo instrumento de exclusão sob uma falsa aparência de precisão matemática.

Para compreender a razão pela qual esse rótulo digital atinge de forma tão desproporcional a população negra, é essencial reconhecer que a seletividade penal não é um erro recente das tecnologias, mas a base que estrutura o sistema de justiça brasileiro de forma histórica. Conforme fundamenta Flauzina (2006), o Brasil construiu o chamado “mito da democracia racial”, uma falsa crença de que as raças convivem em harmonia, a qual serviu para mascarar a violência contínua do nosso aparato punitivo. Nesse sentido, para manter a imagem de um Estado justo, o racismo no sistema penal passou a ser tratado pelas instituições pelo que a autora define como uma atuação "pelo acostamento", isto é, o preconceito racial sempre foi rebaixado a um mero desvio acidental ou a uma característica secundária (um adjetivo) das falhas estatais, quando, na realidade prática, ele é o motor principal (o substantivo) que de fato justifica o controle severo sobre a população negra.

Sob essa mesma perspectiva, Flauzina (2006) alerta para o perigo dos chamados atalhos da criminologia. A autora explica que muitos autores tentam justificar a seletividade do sistema penal focando apenas na pobreza e na classe social, ignorando que a raça é o pilar central dessa exclusão no contexto nacional, uma vez que o sistema punitivo brasileiro foi desenhado desde o período colonial para gerenciar e controlar especificamente pessoas negras. Desse modo, na estrutura social brasileira, a cor da pele chega antes de qualquer outra característica do indivíduo, como a sua profissão ou o seu nível de escolaridade. A suspeição generalizada e as prisões em massa, portanto, não são falhas operacionais do sistema, mas sim o seu modo de funcionamento padrão, criado justamente para neutralizar um grupo que historicamente foi estigmatizado. Atualmente, com esse desenvolvimento tecnológico, a seletividade passou a operar também por meio de álbuns de suspeitos no meio digital, os quais automatizam o estigma do suspeito natural em decorrência do déficit de transparência e da ausência de rastreabilidade algorítmica (Oliveira, 2023; Mello, 2025).

Essa automação do preconceito materializou-se de forma trágica no Brasil, no ano de 2020, quando o caso do músico Luiz Carlos Justino ganhou notoriedade pública em razão das graves falhas associadas aos métodos de reconhecimento. Na referida ocasião, o jovem violoncelista negro foi preso na cidade de Niterói, no Rio de Janeiro, por um crime de roubo ocorrido três anos antes, apenas porque sua imagem estava em um catálogo de suspeitos da polícia. Nesse caso específico, conforme relata Oliveira (2023), o magistrado André Luiz Nicolitt questionou precisamente por que um jovem músico negro, sendo este alguém que nunca havia sido condenado por um crime antes, constava em um álbum de fotografias policial. Ao revogar a prisão do jovem, o juiz concluiu que tal prática reflete uma construção da suspeição baseada unicamente no fenótipo, isto é, nas características físicas observáveis como a cor da pele, e no território, não se sustentando em indícios concretos de crime.

Além disso, conforme observado na análise do processo feita por Mello (2025), o músico foi identificado por uma foto retirada de redes sociais sem qualquer investigação prévia, desrespeitando assim a cadeia de custódia, que consiste justamente na documentação obrigatória do caminho legal e dos critérios de segurança na coleta de uma prova. Esse tipo de procedimento irregular é exatamente o que transforma o cidadão comum em um suspeito natural, configurando um indivíduo que já é construído e visto como culpado pelo sistema de justiça criminal antes mesmo de o fato ocorrer, sendo pré-julgado apenas por sua origem e aparência. Consequentemente, o episódio de Luiz Justino ilustra de forma material e trágica como a falta de rigor técnico nos reconhecimentos visuais atua em conjunto com o racismo

institucional para encarcerar a juventude negra, servindo como o exemplo prático perfeito para as teorias criminológicas abordadas anteriormente.

Ademais, essa "identidade criminoso" fabricada pelo sistema ganha uma nova camada de perversidade por meio da Inteligência Artificial. Mello (2025) alerta que o risco institucional emerge quando resultados puramente estatísticos, os chamados *matches* algorítmicos, isto é, correspondências automáticas de rostos sugeridas pela máquina, são tratados pelas autoridades como uma "identidade positiva", ou seja, como uma prova absoluta de identificação, convertendo uma inferência técnica em certeza jurídica. O algoritmo, portanto, não apenas calcula semelhanças; ele legitima o processo de etiquetamento social sob uma máscara de neutralidade tecnológica, criando a falsa impressão de que o sistema é imparcial e justo, enquanto esconde os preconceitos de seus programadores e a falta de qualidade das bases de dados.

Por conseguinte, fica evidente que a tecnologia de vigilância não atua em um espaço neutro, mas se instala sobre um contexto historicamente moldado para criminalizar a negritude. Ao associar essa herança histórica com o uso de algoritmos, constata-se que o racismo algorítmico e a criação de álbuns de suspeitos em delegacias são apenas a atualização de um antigo projeto colonial de controle social. Logo, o sistema penal absorve essas novas ferramentas de identificação digital não para corrigir suas próprias injustiças, mas para automatizar a perseguição de pessoas negras, dando a isso uma falsa aparência de precisão matemática e neutralidade científica.

O racismo algorítmico nas câmeras de vigilância opera como um mecanismo de controle que reproduz desigualdades históricas sob um verniz de objetividade técnica. Esse fenômeno ocorre por meio da aquisição de imagem em espaços públicos seguida pelo pré-processamento para a normalização das capturas. O fluxo continua com a extração de características faciais por algoritmos de redes neurais profundas para a comparação com bancos de dados de pessoas procuradas. A ferramenta estabelece então uma pontuação de similaridade para quantificar as semelhanças e finaliza com a decisão técnica de correspondência caso um limiar definido seja ultrapassado. Essa sucessão de etapas não é neutra uma vez que a curadoria dos dados e os critérios de suspeição são atravessados pela criminalização de jovens negros e periféricos o que resulta em taxas de erro elevadas para peles escuras e na automatização da violência racial (Marini; Hora; Avila, 2025).

Consequentemente, o reconhecimento facial atua como um acelerador da seletividade penal, na medida em que o erro tecnológico não se distribui de forma aleatória, atingindo desproporcionalmente os corpos e territórios historicamente submetidos a uma vigilância mais

intensa (Mello, 2025). Ao transformar a raça em uma espécie de "prova moral", em que a estética de uma pessoa é usada como indício de periculosidade, o Estado reatualiza o projeto colonial de controle social, deslocando o ônus da prova para o acusado (Flauzina, 2006). Isso obriga o réu a tentar provar sua inocência diante de uma certeza gerada por um sistema de funcionamento opaco e sem transparência. Portanto, a resistência a essa vigilância exige a desconstrução desses rótulos digitais e a imposição de *standards* probatórios, ou seja, critérios rígidos para aceitar uma prova no processo, que impeçam a conversão de estigmas em condenações injustas (Oliveira, 2023; Mello, 2025).

Consequentemente, o uso do reconhecimento facial, quando desvinculado dessas cautelas científicas, tende a legitimar o erro judiciário sob um manto de suposta objetividade matemática. Lima (2022) alerta que a crença na neutralidade da máquina mascara o fato de que os sistemas de Inteligência Artificial cometem erros graves, atingindo desproporcionalmente pessoas negras devido ao enviesamento das bases de dados e ao racismo estrutural. Assim, para evitar que o sistema penal se converta em uma linha de montagem de condenações injustas, a prova de reconhecimento deve ser tratada não como uma certeza jurídica, mas como uma inferência probabilística, ou seja, uma conclusão baseada em chances estatísticas que exige, obrigatoriamente, a confirmação por elementos de prova independentes e externos ao ato de reconhecer.

Diante da insuficiência do mero cumprimento de formalidades jurídicas para conter a seletividade penal automatizada, isto é, a tendência de algoritmos em selecionar e penalizar grupos específicos, volta-se para o estudo de casos em que apreensões por reconhecimento facial movidos por sistemas de Inteligência Artificial ocorreram de forma indevida, escancarando a reprodução do racismo.

4 A EVIDÊNCIA DO RACISMO ALGORÍTMICO: ESTUDO DOS CASOS DE JOÃO ANTÔNIO BASTOS E AILTON ALVES DE SOUSA

Conforme discutido anteriormente, a transposição da seletividade penal para o ambiente digital não constitui uma ruptura, mas a sofisticação de um projeto de controle. O caso do músico Luiz Carlos Justino, jovem violoncelista negro, foi detido na cidade de Niterói por um crime de roubo ocorrido três anos antes apenas porque sua imagem constava em um álbum de suspeitos da polícia. Conforme analisado por Oliveira (2023) o músico foi identificado por uma foto retirada de redes sociais sem qualquer investigação prévia o que

desrespeitou a cadeia de custódia e transformou o cidadão comum em um suspeito natural. Esse episódio ilustra de forma material como a falta de rigor técnico nos reconhecimentos visuais atua em conjunto com o racismo institucional para encarcerar a juventude negra em um processo de etiquetamento que precede o próprio fato delituoso (Oliveira, 2023).

Essa dinâmica de controle, como observada no caso de Justino, reflete a transição histórica das técnicas de punição descritas anteriormente quando o foco estatal se desloca do suplício físico para a gestão das almas e comportamentos (Foucault, 1975). A inclusão indevida em álbuns de suspeitos atua como uma ferramenta de vigilância invisível que molda a consciência do indivíduo e restringe sua liberdade de circulação antes mesmo de qualquer sentença judicial. Dessa forma o álbum de fotografias nas delegacias representa o estágio analógico da datavigilância o qual prepara o terreno para a conversão de trajetórias de vida em dados processáveis por sistemas automatizados. O músico Luiz Justino foi vítima dessa engrenagem que utiliza a imagem como um registro permanente de periculosidade e ignora a presunção de inocência em favor de uma gestão administrativa de corpos considerados desviantes (Oliveira, 2023).

Nesse sentido, a utilização da Inteligência Artificial no sistema de justiça criminal ganha uma nova camada de perversidade quando resultados puramente estatísticos são tratados pelas autoridades como uma prova absoluta de identificação. O algoritmo acaba por legitimar o processo de etiquetamento social sob uma máscara de neutralidade tecnológica que esconde os preconceitos de seus programadores e a falta de qualidade das bases de dados (Mello, 2025). Por conseguinte, o caso de Luiz Carlos Justino serve como o exemplo prático das teorias criminológicas que discutem a seletividade penal uma vez que a suspeição foi construída unicamente com base no fenótipo e no território (Oliveira, 2023).

A seletividade penal evidenciada nesse episódio demonstra como o sistema de justiça opera por meio de um processo de criminalização secundária que escolhe seus alvos com base em estereótipos sociais (Costa e Jesus, 2025). O uso da Inteligência Artificial nesse contexto não altera a lógica de exclusão mas apenas a acelera ao conferir uma roupagem de precisão matemática a preconceitos históricos (Mello, 2025). Assim o rótulo de criminoso é aplicado ao jovem negro de periferia como uma qualidade intrínseca à sua existência o que valida a atuação repressiva das agências policiais sem a necessidade de indícios concretos de autoria. O músico torna-se então o "suspeito natural" cuja biometria já nasce sob suspeita dentro de um banco de dados desenhado para gerenciar riscos sociais em detrimento de direitos individuais (Oliveira, 2023).

Em uma perspectiva de vigilância em tempo real e uso direto de ferramentas biométricas, observa-se o episódio ocorrido com o *personal trainer* João Antônio Trindade Bastos durante a decisão do Campeonato Sergipano de Futebol (G1, 2024). O jovem foi abordado e levado algemado pela Polícia Militar diante de milhares de espectadores porque o sistema de reconhecimento facial implementado no estádio indicou erroneamente que ele seria um criminoso procurado pela justiça (Revista Fórum, 2024). Todavia, o sistema incorreu em um falso positivo visto que João Antônio não possuía qualquer pendência criminal e foi liberado apenas após o esclarecimento do equívoco na delegacia (G1, 2024).

O episódio ocorrido no Estádio Lourival Batista (SE) ilustra perfeitamente a implementação do Panóptico digital em espaços de lazer onde a observação contínua e massiva é normalizada sob o discurso da segurança pública. Nesses ambientes a tecnologia de reconhecimento facial opera por meio da dataficação a qual converte as expressões e comportamentos dos torcedores em vetores matemáticos quantificáveis. João Antônio teve sua identidade biométrica sequestrada por um algoritmo que busca correspondências probabilísticas em bases de dados muitas vezes alimentadas por imagens viciadas ou desatualizadas (Mello, 2025). A abordagem algemada diante de milhares de pessoas materializa o custo humano desta datavigilância que transforma o cidadão comum em um dado estatístico passível de erro sistêmico.

Sob a ótica do racismo algorítmico, o constrangimento sofrido pelo jovem não pode ser interpretado como um erro meramente técnico ou isolado. Conforme defendido pela assistência jurídica de João Antônio, ele foi vítima de um racismo estrutural que se manifesta na automação de preconceitos por meio de algoritmos treinados majoritariamente por pessoas brancas. Como os sistemas de Inteligência Artificial apresentam maior dificuldade em identificar rostos negros devido à falta de representatividade nas bases de treinamento, a probabilidade de abordagens indevidas recai desproporcionalmente sobre essa população (G1, 2024).

No caso de João Antônio, o uso da Inteligência Artificial operou como um instrumento de controle territorial que converte a biometria humana em vetores matemáticos para fins de comparação instantânea (Mello, 2025). A falibilidade da ferramenta em ambientes de massa evidencia que a tecnologia não possui certeza absoluta e deve ser tratada juridicamente apenas como um indício probabilístico que demanda corroboração por outras provas (Mello, 2025).

É imperativo destacar que a falibilidade tecnológica no caso de João Antônio encontra explicação científica no chamado "efeito de raça cruzada" o qual demonstra a dificuldade humana e algorítmica em codificar rostos de grupos étnicos distintos (Costa e Jesus, 2025).

Além disso, como os desenvolvedores dos sistemas são majoritariamente brancos, a Inteligência Artificial é treinada com bases de dados que carecem de representatividade racial o que gera taxas de erro superiores para pessoas negras (Bezerra e Costa, 2022). O racismo algorítmico portanto não é um defeito acidental, mas uma característica estruturante de ferramentas que automatizam a violência racial ao tratar traços fenotípicos como marcadores de periculosidade (Silva, 2022). A suspensão do programa em Sergipe revela o reconhecimento estatal da precariedade desses métodos que sacrificam a dignidade de corpos negros no altar da modernização tecnológica (Revista Fórum, 2024).

Dando seguimento à análise da expansão tecnológica nos grandes centros urbanos, o caso de Ailton Alves de Sousa exemplifica como o monitoramento ininterrupto pode gerar ciclos de perseguição indevida sob o amparo do projeto Smart Sampa na cidade de São Paulo (Gonçalves, 2026). O coordenador de departamento pessoal foi detido pela Polícia Militar e pela Guarda Civil Metropolitana quatro vezes em um intervalo de apenas sete meses porque as câmeras inteligentes da prefeitura o identificaram erroneamente como um foragido da justiça do estado de Mato Grosso (Souza, 2026).

O constrangimento ocorreu em situações cotidianas visto que o cidadão foi abordado ao sair de casa, no ambiente de trabalho e até mesmo enquanto acompanhava sua mãe em uma consulta médica (Souza, 2026). É relevante destacar que o reconhecimento foi processado de forma automática por meio de algoritmos que cruzam as imagens capturadas em vias públicas com o Banco Nacional de Mandados de Prisão (Gonçalves, 2026).

A falha sistêmica nesse episódio reside no fato de que o mandado de prisão original não possuía fotografia, o que permitiu que o software associasse arbitrariamente o rosto de Ailton a um crime de homicídio ocorrido no Centro-Oeste (Souza, 2026). Embora existissem divergências claras como a grafia do sobrenome, que no documento do foragido consta com a letra “z”, e uma diferença de doze anos de idade entre o inocente e o verdadeiro suspeito, a tecnologia tratou a probabilidade estatística como uma certeza administrativa (Gonçalves, 2026).

Sob a perspectiva do racismo algorítmico, o fato de Ailton ser morador de Heliópolis, a maior favela de São Paulo, demonstra que a vigilância se concentra e se torna mais agressiva em territórios ocupados majoritariamente pela população negra e pobre (Souza, 2026). Conforme os dados do Relatório de Transparência do programa, cerca de 71% das vítimas de erros por inconsistência facial no Smart Sampa são pessoas negras, o que comprova que a ferramenta atua como um vetor de reprodução da seletividade penal (Molero, 2025).

A persistência do erro no caso de Ailton, mesmo após diversas solicitações de sua defesa para a exclusão dos dados, revela a precariedade dos protocolos de correção e a confiança cega das autoridades na resposta da máquina (Souza, 2026). Esse cenário materializa o que a literatura define como etiquetamento tecnológico, uma vez que o cidadão passou a viver em estado de medo constante e sob suspeição generalizada apenas por constar em um banco de dados viciado (Mello, 2025). Diante desse descontrole, observa-se que a automação do reconhecimento facial não apenas falha em identificar os reais culpados, mas também institui uma vigilância desproporcional que sacrifica a dignidade de indivíduos vulnerabilizados sob o pretexto da eficiência administrativa (Molero, 2025).

Nesse cenário, o marco inicial para a correção desses rumos foi o julgamento do Habeas Corpus nº 598.886/SC pelo Superior Tribunal de Justiça (Brasil, 2020). Esta decisão histórica despertou os operadores do sistema de justiça para o fato de que a conformidade com o Art. 226 do Código de Processo Penal não é facultativa, mas sim uma condição de validade da prova (CNJ, 2024). Tal entendimento reforça que o reconhecimento pessoal ou facial não possui força probante absoluta de modo que não pode induzir sozinho à certeza da autoria delitiva em razão de sua inerente fragilidade epistêmica.

Nesse sentido, a Resolução nº 484/2022 do Conselho Nacional de Justiça estabelece que o reconhecimento deve ser tratado como uma prova irrepetível e subsidiária (CNJ, 2022). A falta de transparência e a ausência de legislação específica no Brasil permitem que as instituições continuem investindo em tecnologias que muitas vezes reatualizam o positivismo criminológico do século XIX (Oliveira, 2023). O criminoso nato habita atualmente o imaginário algorítmico e as câmeras de vigilância operam como uma extensão do panóptico digital mantendo a população negra sob observação punitiva constante (Mello, 2025).

A opacidade dos algoritmos funciona como uma barreira ao contraditório efetivo uma vez que as empresas desenvolvedoras protegem seus códigos sob o manto do segredo comercial (Mello, 2025). Essa falta de transparência impede que a defesa examine os vieses de treinamento e os critérios de pontuação de similaridade que levaram à identificação de um suspeito (Bezerra e Costa, 2022). Tal cenário reatualiza o positivismo criminológico do século XIX ao buscar na biologia e na tecnologia a justificativa moral para o encarceramento em massa (Oliveira, 2023). O "criminoso nato" agora é definido por uma porcentagem de *match* emitida por uma máquina cuja lógica de funcionamento é inacessível ao escrutínio público e judicial (Mello, 2025). Portanto o racismo algorítmico atua como um motor invisível que sustenta a seletividade penal brasileira e perpetua o projeto colonial de controle social (Silva, 2022).

Por conseguinte, os episódios narrados demonstram que a implementação da Inteligência Artificial na persecução penal sem as devidas cautelas científicas compromete garantias fundamentais como a presunção de inocência (CNJ, 2024). A substituição da análise humana criteriosa por resultados puramente estatísticos favorece a ocorrência de erros judiciais de efeitos irreversíveis para a liberdade individual (Mello, 2025). Assim, a desconstrução do racismo algorítmico exige uma mudança profunda na cultura jurídica brasileira para que a cor da pele deixe de ser utilizada como um marcador tecnológico de culpabilidade (Fernandes e Pietrani, 2025).

Em última análise, os estudos de caso apresentados confirmam que a seletividade penal não é um erro acidental da máquina mas sim o seu modo de funcionamento padrão em uma sociedade estruturada pelo racismo (Flauzina, 2006). A resistência a essa vigilância indiscriminada exige a imposição de *standards* probatórios rígidos que impeçam a conversão de estigmas em condenações injustas (Mello, 2025). Somente por meio da transparência algorítmica e do controle judicial rigoroso será possível garantir que a inovação tecnológica não sirva apenas para perpetuar o projeto colonial de controle social sobre corpos negros (Oliveira, 2023).

5 CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo desta pesquisa permite concluir que o uso do reconhecimento facial no sistema penal brasileiro não representa uma mera evolução técnica, mas sim a consolidação de uma vigilância digital que sofisticou o projeto colonial de controle social. A partir dos conceitos de datavigilância propostos por Van Dijck (2014) e da cultura de vigilância descrita por David Lyon (1994), observou-se que a conversão de identidades em dados processáveis permitiu ao Estado exercer um monitoramento onipresente que ultrapassa os limites físicos das prisões e reconfigura o poder punitivo.

Ao confrontar a teoria com a prática, o caso do músico Luiz Carlos Justino exemplifica como a seletividade penal opera na realidade policial, uma vez que a inclusão de sua imagem em álbuns de suspeitos, bem como sua utilização nos sistemas de IA que movem as câmeras de segurança, funcionou como um mecanismo de criminalização prévia baseado unicamente no fenótipo e em territórios periféricos que são historicamente submetidos a uma vigilância mais intensa. De maneira semelhante, o constrangimento sofrido por João Antônio Bastos confirma as teses de Silva (2022) sobre o racismo algorítmico, visto que a falha do

sistema em ambiente de massa evidenciou que a utilização de bases de treinamento compostas majoritariamente por faces de pessoas brancas automatiza a violência racial contra corpos negros ao dificultar a codificação de traços fenotípicos diversos.

Ademais, os repetidos erros do programa Smart Sampa contra Ailton Alves de Sousa materializam o risco apontado por Mello (2025) de converter indícios probabilísticos em certezas jurídicas, o que retira do indivíduo a presunção de inocência e transfere para o acusado o ônus de provar sua inocência diante de um erro tecnológico que se apresenta sob um verniz de objetividade técnica. Portanto, a pesquisa demonstra que a tecnologia atua como um acelerador da seletividade penal descrita por Flauzina (2006), conferindo uma aparência de objetividade matemática a preconceitos históricos que estruturam o aparato punitivo nacional.

Por conseguinte, a resistência a essa vigilância indiscriminada depende da observância rigorosa dos standards probatórios fixados pelo Superior Tribunal de Justiça e pelo Conselho Nacional de Justiça, garantindo que a inovação tecnológica não sirva para perpetuar injustiças históricas sob uma máscara de neutralidade matemática. Conclui-se, desse modo, que o enfrentamento ao racismo algorítmico exige transparência e controle judicial rígido para que os códigos de computador respeitem integralmente os direitos fundamentais e a dignidade humana.

REFERÊNCIAS

BECKER, Howard S. **Outsiders: estudos de sociologia do desvio**. Rio de Janeiro: Zahar, 2008.

BEZERRA, Arthur Coelho; COSTA, Camila Mattos da. Pele negra, algoritmos brancos: informação e racismo nas redes sociotécnicas. **Liinc em Revista**, Rio de Janeiro, v. 18, n. 2, e6043, nov. 2022.

BRASIL. Conselho Nacional de Justiça. **Manual de procedimentos de reconhecimento de pessoas: conforme a Resolução CNJ N. 484/2022**. Brasília, DF: CNJ, 2024.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 484, de 19 de dezembro de 2022**. Estabelece diretrizes para a realização do reconhecimento de pessoas em procedimentos e processos criminais e sua avaliação pelo Poder Judiciário. Brasília: CNJ, 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus nº 598.886/SC**. Relator: Ministro Rogério Schietti Cruz, Sexta Turma, julgado em 27 out. 2020. Disponível em: <https://www.stj.jus.br>. Acesso em: 27 jun. 2026.

BRASIL. Superior Tribunal de Justiça. **Tema Repetitivo 1.258**. Reconhecimento de pessoas em procedimentos criminais e a nulidade da prova em caso de inobservância do art. 226 do CPP. Brasília: STJ, 2025.

COSTA, Luis Alberto O.; JESUS, Thiago Allisson C. Reconhecimento pessoal e seletividade penal: uma análise acerca da necessidade da estrita aplicabilidade do rito previsto no Código de Processo Penal. **Revista Brasileira de Direito Processual Penal**, v. 11, n. 1, e1125, jan./abr. 2025.

FERNANDES, Maíra; LIMA, Thallita; PIETRANI, Jéssica. Reconhecimento facial e os riscos da vigilância indiscriminada. **Consultor Jurídico**, 5 nov. 2025.

FLAUZINA, Ana Luiza Pinheiro. **Corpo negro caído no chão: o sistema penal e o projeto genocida do estado brasileiro**. 2006. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2006.

FOUCAULT, Michel. **Vigiar e Punir: nascimento da prisão**. 25. ed. Petrópolis: Vozes, 2002.

G1 SE. ‘Medo, frustrado e constrangido’, diz homem detido por engano em estádio após erro do sistema de reconhecimento facial. 2024. **G1 SE**. Disponível em:

<https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-home-m-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghml>. Acesso em: 27 jun. 2026.

GONÇALVES, André Luiz Dias. Erro no Smart Sampa faz homem ser preso quatro vezes por engano. **TecMundo**, 26 mar. 2026. Disponível em: <https://www.tecmundo.com.br/seguranca/411949-erro-no-smart-sampa-faz-homem-ser-preso-quatro-vezes-por-engano.htm>. Acesso em: 2 jul. 2026

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

LOPES, Mariângela T. **O reconhecimento como meio de prova: necessidade de reformulação do direito brasileiro**. 2011. Tese (Doutorado em Direito) – Universidade de São Paulo, São Paulo, 2011.

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

MARANHÃO, Felipe. IA no reconhecimento de pessoas: Portaria 1.122/26 do Ministério da Justiça. **Consultor Jurídico**, 6 fev. 2026.

MARINI, Marisol; HORA, Nina da; AVILA, Sandra. Reconhecimento sob suspeita: colaboração entre antropologia e ciência da computação na crítica ética ao reconhecimento facial. **gis - gesto, imagem e som**, São Paulo, v. 10, e-230902, 2025.

MELLO, Rodrigo Moreira de. **Reconhecimento facial, prova penal e racismo estrutural no Brasil: Erro judiciário, seletividade e criminalização cultural durante a pandemia de COVID-19**. 2025. Trabalho de avaliação modular (Pós-Graduação) – FEMPERJ, Rio de Janeiro, 2025.

MOLERO JUNIOR, Luciano Finozzi. **Reconhecimento facial na segurança pública e o racismo estrutural: análise constitucional do Programa Smart Sampa (Decreto Municipal nº 63.552)**. 2025. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2025.

OLIVEIRA, Laryssa Amado de. **As problemáticas do reconhecimento facial como prova no processo penal: estudo do caso Luiz Justino e das modificações jurisprudenciais e legislativas posteriores**. 2023. Trabalho de Conclusão de Curso (Graduação em Segurança Pública) – Universidade Federal Fluminense, Niterói, 2023.

Jovem detido em jogo de futebol relata constrangimento após falha no reconhecimento facial da PM. **Revista Fórum**. 2024. Disponível em: <https://revistaforum.com.br>. Acesso em: 27 jun. 2026.

SÃO PAULO (Município). **Decreto nº 63.552, de 4 de julho de 2024**. Institui o Programa Smart Sampa. Diário Oficial da Cidade de São Paulo, São Paulo, 5 jul. 2024. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/decreto-63552-de-4-de-julho-de-2024>. Acesso em: 02 jul. 2026.

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

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: **Anais do 5º Congresso Internacional de Direito e Contemporaneidade**, Santa Maria, 2019.

SOUZA, Felipe; SILVA, Henrique. Após ser identificado por câmeras do Smart Sampa, morador da Zona Sul de SP é detido 4 vezes por engano em 7 meses. **G1**, 26 mar. 2026. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2026/03/26/apos-ser-identificado-por-cameras-do-s-mart-sampa-morador-da-zona-sul-de-sp-e-detido-4-vezes-por-engano-em-7-meses.ghtml>. Acesso em: 3 jul. 2026.

STEIN, L. M.; PERGHER, G. K. Criando falsas memórias em adultos por meio de palavras associadas. **Psicologia: Reflexão e Crítica**, v. 14, p. 353-366, 2001.

VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Vigilância & Sociedade**, v. 12, n. 2, p. 197-208, 2014.