

ALGORITMOS DE
EXCLUSÃO: UMA ANÁLISE
CRÍTICA SOBRE O
TECNOCONSERVADORISMO
E A SUSPEIÇÃO
RACIALIZADA NO BRASIL
CONTEMPORÂNEO

"ALGORITHMS OF EXCLUSION: A CRITICAL ANALYSIS OF TECHNO-
CONSERVATISM AND RACIALIZED SUSPICION IN CONTEMPORARY
BRAZIL"

Ciências Humanas • 29/06/2026

REGISTRO DOI: [10.70773/revistatopicos/782706591](https://doi.org/10.70773/revistatopicos/782706591)

Juliana Santana Palomé¹

Leila Milli Fernandes²

RESUMO

Este artigo analisa a transição dos modelos de segurança pública no Brasil através de tecnologias de vigilância digital e controle algorítmico. Utilizando o referencial do The New Jim Code e do racismo algorítmico, desconstrói-se a suposta "neutralidade técnica" dessas ferramentas. Por meio de revisão bibliográfica e análise do tecnoconservadorismo, o trabalho examina como a dataficação e o reconhecimento facial institucionalizam a suspeição racializada. Os resultados indicam que a automação amplifica desigualdades históricas sob uma fachada de modernização. Originalmente, o texto propõe o amálgama entre "plataformentalização" e "neolombrosianismo digital", demonstrando como tais ferramentas herdam a seletividade penal colonial brasileira.

Palavras-chave: Vigilância Algorítmica; Tecnoconservadorismo; Racismo Estrutural; Segurança Pública; Brasil.

ABSTRACT

This article analyzes the transition of public security models in Brazil through digital surveillance technologies and algorithmic control. Using the framework of The New Jim Code and algorithmic racism, the supposed "technical neutrality" of these tools is deconstructed. Through a literature review and analysis of technoconservatism, the work examines how datafication and facial recognition institutionalize racialized suspicion. The results indicate that automation amplifies historical inequalities under a facade of modernization. Originally, the text proposes the amalgamation between "platformization" and "digital neo-Lombosianism," demonstrating how such tools inherit Brazilian colonial penal selectivity.

Keywords: Algorithmic Surveillance; Technoconservatism; Structural Racism; Public Security; Brazil.

1. INTRODUÇÃO

Nas últimas décadas, a gestão da segurança pública global tem experimentado um deslocamento paradigmático: a transição de modelos de policiamento mais tradicionais e reativos para estratégias baseadas em vigilância digital e controle algorítmico. A incorporação de sistemas de reconhecimento facial, análise preditiva de criminalidade (*predictive policing*) e algoritmos de classificação de risco (LYON, 2018) é frequentemente apresentada sob uma retórica de inevitabilidade tecnológica e modernização administrativa. Tais ferramentas são comercializadas e implementadas sob o signo da eficiência e da "neutralidade técnica", consolidando a ideia de que a mediação computacional seria capaz de expurgar a subjetividade e o erro inerentes à ação humana, produzindo decisões pretensamente objetivas e justas.

Lyon (2018) articula de forma contundente a transição da vigilância meramente contemplativa para uma vigilância classificatória. O autor demonstra que a estruturação de perfis (*profiling*), viabilizada pela mineração e pelo cruzamento massivo de metadados, atua como um potente instrumento de triagem social. Essa arquitetura algorítmica não apenas monitora, mas atua na produção ativa de hierarquias, operando sob a lógica da gestão antecipada de riscos e oportunidades.

Segundo Lyon (2018), tal classificação automatizada adquire um caráter performativo ao ditar a distribuição assimétrica de direitos: enquanto setores específicos da população são identificados como destinatários preferenciais de bens, serviços e mobilidade, outros estratos frequentemente selecionados por vieses históricos incorporados ao código são precocemente categorizados sob o

prisma da suspeição ou da criminalidade. Dessa forma, a vigilância contemporânea deixa de ser apenas um mecanismo de controle para se tornar um vetor de estratificação e marginalização institucionalizada.

Longe de serem neutros, os algoritmos atuam como "caixas-pretas" que reproduzem e, em larga escala, amplificam desigualdades históricas e estruturas de poder preexistentes. Como argumenta Noble (2021), os sistemas de busca e classificação podem reforçar o racismo através de sua arquitetura de dados; no mesmo sentido, Benjamin (2019) cunha o conceito de *The New Jim Code* para descrever como tecnologias aparentemente inovadoras institucionalizam formas de discriminação automatizada sob uma fachada de progresso técnico.

Ao analisar a opressão algorítmica, Noble (2021) pondera que as decisões automatizadas são estruturadas por formulações matemáticas construídas por seres humanos. Os conceitos de *big data* e algoritmos não operam de forma benigna, neutra ou inteiramente objetiva; ao contrário, as pessoas que definem essas arquiteturas e escolhem quais dados priorizar carregam valores, vieses e noções que podem promover ativamente discriminações de gênero e raça.

No cenário brasileiro, essa problemática assume contornos de urgência democrática. O Brasil é marcado por uma histórica seletividade penal, pela profunda desigualdade socioeconômica e por uma racialização estrutural do sistema de justiça, onde o corpo negro é historicamente constituído como o alvo prioritário do controle estatal.

Um caso emblemático, reportado pelo portal de notícias g1, detalha a trajetória de um cidadão detido indevidamente em quatro ocasiões distintas. As abordagens policiais foram motivadas por uma identificação errônea que o vinculava a um indivíduo foragido do estado de Mato Grosso, a despeito de discrepâncias elementares nos dados antropométricos e biográficos, tais como idade e sobrenome (SOUZA; SILVA, 2026). A reincidência do erro em face de um indivíduo fenotipicamente negro sugere que a automação da vigilância não é neutra, mas pode atuar como um mecanismo de replicação e intensificação do racismo estrutural.

Diante desse cenário, a tecnologia deixa de ser uma ferramenta puramente técnica para se tornar um vetor de seletividade penal, no qual a arquitetura do código e a base de dados podem institucionalizar preconceitos históricos, comprometendo a eficácia da segurança pública e vulnerabilizando grupos historicamente marginalizados.

A criminologia neoconservadora encontrou nas plataformas digitais brasileiras o ambiente ideal para a automação de vieses, consolidando o que se denomina tecnoconservadorismo (ROSA et al., 2025). Esse fenômeno, impulsionado por figuras como Olavo de Carvalho através do uso estratégico de dispositivos eletrônicos para fins tecnopolíticos (SABARIEGO, 2018), instrumentaliza o racismo algorítmico ao transformar preconceitos históricos em métricas de vigilância. Assim, a tecnologia deixa de ser apenas um meio de difusão ideológica para se tornar um mecanismo ativo de reprodução da seletividade penal no ciberespaço.

Nesse cenário, o racismo algorítmico atua como o braço operacional do tecnoconservadorismo. Ao codificar a lógica do "inimigo" em

sistemas de inteligência e moderação de conteúdo, essas plataformas automatizam a exclusão e a criminalização de grupos historicamente marginalizados, conferindo uma aparência de "verdade matemática" à seletividade racial inerente ao sistema de justiça brasileiro.

Diante do exposto, este artigo busca responder ao seguinte problema de pesquisa: Como a vigilância algorítmica, articulada ao tecnoconservadorismo, contribui para a produção do inimigo interno no Brasil, reproduzindo desigualdades raciais e estruturais na segurança pública?

Para além de uma síntese da literatura sociotécnica internacional, a contribuição original deste trabalho reside no esforço analítico de tensionar a universalidade de conceitos globais à luz da particularidade histórica e colonial brasileira. Longe de operar uma aplicação puramente dedutiva que utilizaria a realidade nacional como mera ilustração de teorias estrangeiras, este artigo avança ao propor o amálgama conceitual entre a "plataformentalização" (como racionalidade privada de gestão de condutas) e o "neolombrosianismo digital" (enquanto reatualização da seletividade penal). Demonstra-se, assim, como a infraestrutura de dados contemporânea não apenas herda passivos, mas atua como um vetor dinâmico de reconfiguração da soberania punitiva do Estado brasileiro.

O objetivo central deste trabalho é analisar a interseção entre vigilância algorítmica, racismo estrutural e as racionalidades políticas punitivas no Brasil contemporâneo. Para tanto, a investigação estrutura-se da seguinte forma: primeiro, apresenta-se o percurso metodológico adotado; em seguida, discute-se a desconstrução

analítica da neutralidade tecnológica face ao racismo estrutural brasileiro; após, analisa-se o fenômeno do tecnoconservadorismo como motor das políticas de segurança digital; na sequência, examina-se como a dataficação do policiamento institucionaliza a suspeição; e, por fim, tecem-se as considerações finais apontando caminhos propositivos de resistência.

2. PROCEDIMENTOS METODOLÓGICOS

Para garantir a cientificidade e a replicabilidade das conclusões apresentadas, este estudo ampara-se em uma abordagem qualitativa de caráter exploratório-reflexivo, utilizando como procedimentos fundamentais a pesquisa bibliográfica sistemática e a análise de conceitos teóricos aplicados à criminologia.

O levantamento bibliográfico foi estruturado a partir de consultas realizadas no primeiro semestre de 2026 nas bases de dados da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), no *SciELO* (Scientific Electronic Library Online) e no *Google Scholar*. O recorte temporal delimitado compreendeu a literatura crítica produzida entre os anos de 2015 e 2026, período que coincide com a expansão das plataformas de redes sociais e com o início da implementação de projetos de cidades inteligentes e sistemas de monitoramento biométrico no Brasil.

Os descritores de busca operados de forma combinada (operadores booleanos AND e OR) foram: "racismo algorítmico", "tecnoconservadorismo", "vigilância", "segurança pública" e "seletividade penal". Os critérios de inclusão adotados determinaram a seleção de obras de referência internacional no campo dos estudos sociotécnicos de dados e de artigos nacionais publicados

em periódicos avaliados por pares que debatessem empiricamente a segurança pública brasileira. Foram excluídos trabalhos estritamente técnicos de engenharia de software que não fizessem a correlação social do impacto dos sistemas.

A análise de dados deu-se por meio da triangulação teórica entre a literatura sobre vieses automatizados, a criminologia crítica brasileira e dados institucionais empíricos sobre prisões por reconhecimento facial. Esse procedimento permitiu rastrear os nexos causais que vinculam o desenho do código de programação (*inputs*) aos impactos excludentes observados na atividade policial de ponta (*outputs*).

3. A FALÁCIA DA NEUTRALIDADE TÉCNICA E O RACISMO ALGORÍTMICO

A implementação de algoritmos na segurança pública brasileira é frequentemente escoltada por um discurso tecnocrático que posiciona o código computacional como uma entidade purificada de paixões humanas e preconceitos ideológicos. Essa "mística da objetividade" (NOBLE, 2021) sugere que, ao converter comportamentos sociais em variáveis matemáticas, o Estado alcançaria uma justiça procedimental inquestionável. No entanto, tal perspectiva ignora que a tecnologia é uma produção sociocultural, carregando consigo os valores, as omissões e as hierarquias de seus criadores e dos contextos em que é gerada.

Nesse cenário, debates públicos ilustram como essa suposta neutralidade é confrontada pela realidade prática ao analisar projetos governamentais como o "Smart Sampa"¹. A iniciativa de monitoramento por reconhecimento facial massivo reaquece o

debate sobre o perfilamento racial, servindo como exemplo de como algoritmos aplicados ao espaço urbano podem ampliar e cancelar estruturas históricas de exclusão. Para compreender essa engrenagem, é preciso definir o "digital" não como um determinante isolado, mas como um conjunto de interações sociais radicalmente condicionadas pela tecnologia (FACIOLI; PADILHA, 2020). Sob essa ótica, o modo de vivenciar a cidade e a segurança pública é alterado por dispositivos que organizam o real através de programações que, embora pareçam puramente matemáticas, são profundamente políticas.

Para compreender essa engrenagem, é preciso definir o "digital" não como um determinante isolado, mas como um conjunto de interações sociais radicalmente condicionadas pela tecnologia (FACIOLI; PADILHA, 2020). Sob essa ótica, o modo de vivenciar a cidade e a segurança pública é alterado por dispositivos que organizam o real através de programações que, embora pareçam puramente matemáticas, são profundamente políticas.

A fundação dessa problemática reside na natureza dos algoritmos, que funcionam como um conjunto de operações matemáticas responsáveis por proporcionar o aprendizado das máquinas e determinar quais conteúdos e decisões são entregues a cada público (SILVA, 2022). Em termos técnicos estruturais, convém diferenciar a Inteligência Artificial geral do aprendizado de máquina (*machine learning*), enfatizando que este último aprende especificamente a partir de bases de dados compostas por "exemplos" e "instruções" prévias. Ocorre que essa instrução informacional não é asséptica; os algoritmos atuam como mediadores da informação digital (GONÇALVES, 2024), funcionando como uma "receita" que molda o comportamento da máquina para

atingir objetivos que, frequentemente, priorizam a eficiência seletiva e o controle social em detrimento da ética e da justiça distributiva.

A suposta neutralidade dessas ferramentas é reforçada pela "opacidade algorítmica" (PASQUALE, 2015), que oculta os critérios decisórios dos sistemas as chamadas "caixas-pretas" corporativas e estatais e impede a devida contestação ou a transparência jurídica por parte dos indivíduos diretamente afetados pelas classificações. Safiya Noble (2021) desmistifica essa pretensa objetividade ao demonstrar como mecanismos de busca estruturam suas lógicas a partir de matrizes econômicas e humanas, reproduzindo vieses discriminatórios. As lógicas computacionais são condicionadas por uma matriz de poder interseccional (COLLINS; BILGE, 2021) que reflete a crônica falta de diversidade da indústria tecnológica global, majoritariamente concentrada em um perfil demográfico de homens brancos e ricos do Vale do Silício.

Portanto, o que se observa no tecido social é uma vulnerabilização sistêmica. A discriminação algorítmica deixa de ser um erro técnico para se tornar uma reprodução automatizada das opressões vigentes o chamado "racismo algorítmico" (SILVA, 2022). Como os sistemas dependem de dados que espelham preconceitos sociais e práticas policiais preexistentes, a automação acaba por institucionalizar novas formas de marginalização e "algoritmos de exclusão" (O'NEIL, 2020). Essa aceleração tecnológica ocorre frequentemente à revelia das minorias políticas, cujos direitos à privacidade, à presunção de inocência, à dignidade e à igualdade são preteridos em prol de um capitalismo informacional e de uma governança punitiva que naturalizam desigualdades sob o manto de processos matemáticos supostamente isentos.

4. O *NEW JIM CODE* E A INVISIBILIDADE DO VIÉS *NEW JIM CODE* E A INVISIBILIDADE DO VIÉS NA GOVERNANÇA ALGORÍTMICA

A análise sociotécnica contemporânea no campo da segurança pública exige a superação definitiva do paradigma da neutralidade axiológica dos algoritmos. Benjamin (2019) fundamenta essa crítica por meio do conceito de *The New Jim Code* (O Novo Código de Jim), definido como o emprego de novas tecnologias que refletem e reproduzem desigualdades existentes, mas que são promovidas e percebidas como mais objetivas e progressivas que os sistemas discriminatórios de uma era anterior. Esta estrutura não apenas herda passivos históricos, mas sedimenta preconceitos estruturais no âmago dos sistemas de inteligência artificial aplicados ao controle social.

Para compreender a capilaridade do *New Jim Code*, é imperativo distingui-lo de seu predecessor histórico, o regime de *Jim Crow*. Enquanto as leis segregacionistas estadunidenses operavam mediante um aparato jurídico-político explícito e visível para marginalizar populações negras, a codificação algorítmica atua de forma insidiosa, sutil e opaca. No regime anterior, a opressão era sustentada publicamente pela pseudociência e pela institucionalidade estatal; na contemporaneidade, a segregação é automatizada e blindada por uma suposta "objetividade técnica" que, sob o pretexto da modernização administrativa, recrudesce o racismo e as assimetrias de poder.

A violência algorítmica fundamenta-se na falácia de que os sistemas computacionais seriam imunes à reprodução de vieses por carecerem de subjetividade ou intenção humana. Benjamin (2019)

refuta essa premissa ao asseverar que, se as máquinas são programadas para a execução de tarefas específicas, tanto o artefato quanto o desenvolvedor são orientados por teleologias políticas. Diante de efeitos discriminatórios sistêmicos, a inércia dos detentores do poder tecnológico em modificar tais arquiteturas configura a perpetuação deliberada de um sistema de supremacia racial.

Nesse sentido, a hermenêutica dos "erros" tecnológicos deve ser deslocada do campo do acidente fortuito para o campo do projeto político. Incidentes críticos, como a rotulação aviltante de indivíduos negros por sistemas de visão computacional ou os alarmes falsos de reconhecimento facial na segurança urbana, não constituem meras anomalias técnicas passageiras. De acordo com a perspectiva de Benjamin (2019), a análise da arquitetura desses sistemas revela que tais resultados representam a funcionalidade plena de dados modelados sob uma cultura de antinegritude; o erro, portanto, opera como um "acerto" dentro de uma lógica de exclusão pré-configurada.

Essa arquitetura discriminatória estabelece um paralelo digital com as antigas práticas de *redlining* urbano, que historicamente mapeavam zonas periféricas para o bloqueio de investimentos em áreas habitadas por minorias. Atualmente, os algoritmos de predição criminal utilizam esses mesmos dados segregacionistas como insumos (*inputs*), permitindo que sistemas automatizados gerem perfis de suspeição que preservam privilégios de classe e raça, enquanto aprofundam a criminalização de grupos historicamente marginalizados pela segurança pública.

A sofisticação do racismo algorítmico atinge seu ápice no que Benjamin (2019) denomina "benevolência tecnológica" (*technological benevolence*). O conceito descreve dispositivos projetados sob a retórica humanitária da solução de problemas sociais, mas que, na prática, contribuem substancialmente para o fortalecimento da discriminação racial e o aprofundamento das desigualdades. O uso de monitoramento eletrônico e de tornozeleiras exemplifica essa contradição: embora apresentado como alternativa progressista ao cárcere físico, estabelece uma "liberdade vigiada" que expande a malha punitiva do Estado e pereniza o controle sobre o corpo negro fora dos muros da prisão.

Em última análise, essa dinâmica consolida a criação de realidades verticais, caracterizadas pela oferta de segurança para alguns estratos sociais e hipervigilância invasiva para outros (BENJAMIN, 2019). Enquanto a coleta de dados serve à personalização do consumo de luxo para as elites, para os grupos subalternizados ela funciona como um aparato de exposição indesejada e controle criminal. Desafiar essa ordem no campo da segurança pública exige, portanto, a adoção de práxis abolicionistas e um rigor crítico que desmonte o *status quo* da tecnocracia punitiva.

5. O TECNOCONSERVADORISMO E A RACIONALIDADE PUNITIVA DIGITAL

O tecnoconservadorismo não deve ser compreendido meramente como o uso circunstancial de tecnologias digitais por governos ou partidos de direita, mas sim como uma racionalidade política específica que instrumentaliza a inovação tecnológica para reatualizar e intensificar projetos históricos de controle social, seletividade e exclusão (ROSA et al., 2025). Esta nova face do

conservadorismo ganha destaque no cenário político brasileiro pela sua capacidade de amalgamar valores morais tradicionais e o aparato econômico neoliberal às dinâmicas operacionais das plataformas digitais. O fenômeno fundamenta-se na simbiose entre o discurso conservador e a arquitetura das redes, legitimando a lógica concorrencial corporativa no interior da própria gestão estatal (ROSA et al., 2025).

No Brasil, este movimento contrarrevolucionário encontrou sustentação teórica e prática difusa na circulação de ideias neoconservadoras e olavistas, que passaram a permear o cotidiano de diversos profissionais do sistema de justiça criminal, incluindo magistrados, promotores e delegados de polícia. Esses atores utilizam o espaço digital para formar comunidades virtuais fechadas que se fortalecem mutuamente através da replicação de discursos punitivos. Não se trata de uma simples adaptação instrumental das redes, mas de uma transformação profunda na maneira como discursos de ordem são produzidos, disseminados e consumidos, forjando novas subjetividades institucionais e impactando diretamente a formulação de políticas de segurança pública.

A espinha dorsal dessa racionalidade é a "plataformentalização", conceito analítico original que designa a articulação íntima entre a governamentalidade algorítmica e a plataformização social. Por meio de algoritmos de recomendação e moderação, as plataformas operam como ferramentas de gestão das condutas humanas, onde a condução dos comportamentos e a regulação das populações passam a ser mediadas e reconfiguradas por interesses privados e lógicas algorítmicas (ROSA; JOBIM; NEMER, 2023). Esta dinâmica direciona a atenção coletiva para conteúdo de alto apelo emocional como o medo do crime, criando bolhas informacionais que

promovem o justicamento, discursos punitivos e o negacionismo científico face às evidências sociológicas sobre a criminalidade.

No campo da criminologia, o tecnoconservadorismo reinterpreta a disciplina sob um viés estritamente moralista, punitivista e simplista. A criminologia conservadora brasileira privilegia o encarceramento em massa e a responsabilidade estritamente individual, desconsiderando por completo as variáveis socioeconômicas e estruturais do crime. É recorrente a reatualização de abordagens de matiz neolombrosiana na literatura que alimenta essas redes, as quais reduzem o indivíduo criminalizado a uma anomalia biológica ou a uma escolha puramente racional voltada para o mal, desprovida de qualquer senso de alteridade (PESSI; SOUZA, 2017; SAMENOW, 2020 *apud* ROSA et al., 2025). Tal perspectiva atua na legitimação da violência estatal e no extermínio de garantias processuais.

A racionalidade punitiva digital funde a promessa da infalibilidade tecnológica ao discurso político da "lei e da ordem". A vigilância algorítmica deixa de ser apenas uma ferramenta administrativa interna para se tornar uma vitrine político-eleitoral de dureza contra o crime. Essa lógica opera através de uma "fetichização do dado", onde a complexidade dos fenômenos urbanos é reduzida a insumos binários. Ao apresentar soluções de monitoramento biométrico e predição como "inevitáveis", o Estado exime-se do debate sobre políticas públicas estruturais e redistributivas, substituindo o investimento social na saúde e na educação pela expansão contínua da infraestrutura tecnológica de captura penal.

6. DATAFICAÇÃO DO POLICIAMENTO E A INSTITUCIONALIZAÇÃO DA SUSPEIÇÃO RACIALIZADA NO BRASIL

A transição para o policiamento orientado por dados (*data-driven policing*) no Brasil não ocorre de forma daltônica ou neutra; pelo contrário, ela acopla-se de maneira perfeita a uma arquitetura de segurança pública que, historicamente, opera sob a lógica da filtragem racial e da herança colonial. A dataficação, nesse contexto, atua como uma camada de verniz tecnológico que automatiza a suspeição, transformando o tirocínio policial e o viés discriminatório histórico em evidência estatística pretensamente inquestionável. Conforme adverte a literatura crítica, o racismo algorítmico não deve ser compreendido como uma falha técnica pontual ou um erro de calibração do sistema, mas sim como uma característica inerente a ferramentas desenhadas e alimentadas no interior de sociedades estruturalmente racistas (SILVA, 2022).

O uso massivo de tecnologias de reconhecimento facial em espaços públicos e grandes eventos urbanos exemplifica a materialização dessa infraestrutura de exclusão. A eficácia dessas ferramentas é cronicamente comprometida por bases de dados policiais historicamente eivadas de seletividade e por algoritmos de visão computacional desenvolvidos sob padrões eurocêntricos, os quais apresentam severas dificuldades e taxas elevadas de erro na identificação de peles retintas (BEZERRA; COSTA, 2021). A própria escolha política de quais corpos e territórios serão prioritariamente mapeados, monitorados e classificados evidencia que a tecnologia serve à manutenção de assimetrias de poder, operando sob uma opacidade que impede o cidadão de questionar os critérios de sua própria catalogação como indivíduo "de risco" ou "suspeito" (SILVA, 2022).

Ao cruzar imagens capturadas em tempo real com bancos de dados criminais marcados pela seletividade penal, o Estado opera o que

Browne (2015) conceitua como *dark surveillance*, uma dinâmica na qual a presença de determinados sujeitos racializados em espaços urbanos centrais dispara alertas automáticos de risco. Esse fenômeno integra os mecanismos da chamada "imaginação técnica branca", uma racionalidade em que a tecnologia é projetada e mobilizada para blindar privilégios geográficos e de classe das elites, enquanto sistematiza e automatiza o controle punitivo sobre os corpos negros, independentemente da existência de qualquer conduta ilícita concreta (SILVA, 2022).

A análise preditiva introduz no cenário de segurança nacional o conceito de probabilidade criminal baseada nas chamadas "manchas criminais" urbanas. Contudo, os modelos matemáticos operados pelas agências policiais não preveem a ocorrência futura de crimes, mas sim a distribuição da atividade policial anterior. Se o policiamento ostensivo historicamente se concentra e satura os territórios periféricos e favelizados, os dados gerados por essas próprias prisões retroalimentarão o algoritmo, sugerindo o envio de mais patrulhamento para essas mesmas áreas. A crença cega na objetividade dos dados oculta o fato de que eles são resíduos institucionais de práticas racistas passadas que, ao passarem pelo crivo de modelos preditivos, ganham uma aura espúria de verdade científica e neutralidade matemática (SILVA, 2022).

Essa dinâmica cria uma profecia autorrealizável: a tecnologia justifica a saturação policial de territórios racializados, conferindo uma "objetividade matemática" à criminalização da pobreza. Esse processo de "infraestruturação do racismo" faz com que o preconceito deixe de ser um ato isolado do agente na ponta e passe a ser uma função sistêmica do ambiente urbano. A tecnologia, sob a égide do tecnoconservadorismo, atua como um catalisador de

prisões arbitrárias baseadas em semelhanças fenotípicas superficiais, legitimando o que se pode chamar de cidadania de dados estratificada.

A materialização dessa exclusão é documentada por dados alarmantes. Segundo dados da Rede de Observatórios da Segurança, divulgados por Galvani(2023), cerca de 90% das pessoas presas por reconhecimento facial no Brasil são negras. Este dado é a prova empírica de que a seletividade dos sistemas de monitoramento opera sob a lógica da supremacia branca digital. Silva (2022) argumenta que esses sistemas operam uma "hierarquização de humanidades", onde o erro contra o corpo negro é aceito como um "custo colateral" aceitável para a manutenção da ordem pública.

Para além da segurança pública e do perfilamento criminal, a reprodução do racismo algorítmico e a centralidade da branquitude manifestam-se de forma capilar em outras infraestruturas digitais aparentemente cotidianas, como os algoritmos de relevância pública que gerenciam bancos de imagens digitais (AMARAL; MARTINS; ELESBÃO, 2021). Pesquisas exploratórias comparativas indicam que a busca por termos genéricos e pretensamente "neutros", como a palavra *family*, gera como resultado majoritário e esmagador imagens de famílias brancas, operando uma hiper-ritualização da branquitude como o padrão universal e invisível de humanidade (AMARAL; MARTINS; ELESBÃO, 2021).

A delegação da suspeição a sistemas digitais que operam em milissegundos remove o debate do campo ético-político e o desloca para o campo puramente técnico-gerencial, blindando o Estado de responsabilizações diretas. A automação do racismo converte-o em

uma variável infraestrutural invisível e, portanto, de difícil ataque pelas ferramentas tradicionais do direito e das garantias constitucionais (SILVA, 2022). Diante disso, para o avanço das ciências criminais e da segurança pública, torna-se imperativo reconhecer que a inovação tecnológica desprovida de uma profunda revisão crítica e descolonizadora atuará apenas como o aperfeiçoamento técnico dos mecanismos históricos de moer gente que estruturam o sistema penal brasileiro.

7. CONSIDERAÇÕES FINAIS E CAMINHOS PROPOSITIVOS DE RESISTÊNCIA

A investigação empreendida neste artigo demonstra que a transição para modelos de segurança orientados por dados no Brasil não constitui apenas uma modernização administrativa, mas a consolidação de uma nova racionalidade política: o tecnoconservadorismo. Ao desconstruir a "mística da objetividade" algorítmica, conclui-se que o código computacional, no contexto da segurança pública brasileira, opera como uma ferramenta de atualização e intensificação da seletividade penal. O que se apresenta como neutralidade técnica é, na realidade, a institucionalização de vieses históricos que transmutam o racismo estrutural em probabilidade estatística.

Os eixos analisados revelam que o fenômeno da plataformentalização e a adoção do *The New Jim Code* criaram uma infraestrutura de exclusão que é, ao mesmo tempo, opaca e onipresente. A automação da suspeição racializada evidenciada pelas falhas sistemáticas do reconhecimento facial e pela "profecia autorrealizável" do policiamento preditivo retira a responsabilidade ética do agente humano e a deposita na "caixa-preta" dos

algoritmos. Esse deslocamento dificulta a contestação jurídica e política, tornando a violência estatal menos suscetível a mecanismos tradicionais de controle de direitos humanos.

Para que este trabalho avance para além do diagnóstico crítico e descolonizador, propondo saídas acadêmicas, políticas e sociais concretas para interromper o avanço da tecnocracia punitiva no Brasil, apontam-se três desdobramentos e eixos propositivos urgentes:

1. **litigância Estratégica Interseccional e Banimento**

Tecnológico: O direito tradicional deve ser municiado por auditorias sociotécnicas independentes. Propõe-se a articulação de defensorias públicas, organizações da sociedade civil e movimentos negros para a propositura de ações civis públicas que exijam o banimento imediato do uso de tecnologias de reconhecimento facial em tempo real na segurança pública, uma vez comprovada a impossibilidade de extirpar o viés racial de bases de dados estruturalmente seletivas. O erro algorítmico contra o corpo negro deve ser tipificado juridicamente como violação de direitos humanos, gerando nexos de causalidade para a nulidade imediata de prisões efetuadas sob o exclusivo comando de alertas automatizados.

2. **desenvolvimento de Contra-Infraestruturas e Práticas de**

Data Sovereignty. Face à extração colonialista de dados biométricos das populações periféricas, urge fomentar redes comunitárias de soberania de dados. Isso implica a criação de laboratórios de tecnologia cidadã nas periferias urbanas voltados ao desenvolvimento de ferramentas de código aberto

para o mapeamento e a denúncia da violência policial (*counter-surveillance*). A população deve deter o controle sobre os registros e metadados de seus territórios, subvertendo a lógica vertical de captação e transformando o dado em um instrumento de proteção coletiva e salvaguarda de direitos fundamentais contra os abusos do Estado.

3. institucionalização de Avaliações de Impacto de Direitos

Humanos (AIDH): Nenhuma ferramenta algorítmica ou sistema de inteligência artificial deve ser adquirido ou implementado por secretarias de segurança pública sem a realização prévia de uma Avaliação de Impacto de Direitos Humanos, conduzida por comitês independentes, paritários e multidisciplinares, com participação obrigatória de representantes de movimentos sociais e da academia. Essas avaliações devem possuir caráter vinculante, impedindo a compra de softwares de policiamento preditivo cujo funcionamento interno esteja protegido por cláusulas de segredo comercial que gerem opacidade ou que utilizem variáveis geográficas e raciais discriminatórias.

Em última análise, o desafio posto à democracia brasileira no século XXI é o de impedir que a tecnologia seja o verniz que torna o racismo infraestrutural e inatacável. Para que a segurança pública cumpra sua função social, é necessária uma revisão descolonizadora de suas ferramentas digitais, garantindo que a inovação não seja apenas o refinamento técnico do aparato punitivo, mas um instrumento subordinado aos princípios fundamentais da dignidade humana e da justiça social.

REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, Augusto Jobim do; MARTINS, Fernanda; ELESBÃO, Ana Clara. Racismo algorítmico: uma análise da branquitude nos bancos de imagens digitais. **Pensar - Revista de Ciências Jurídicas**, Fortaleza, v. 26, n. 4, p. 1-9, out./dez. 2021.

BENJAMIN, Ruha. **Race after technology**: abolitionist tools for the New Jim Code. Medford: Polity Press, 2019.

BEZERRA, Arthur Coelho; **COSTA**, Sued de Castro. Vigilância e reconhecimento facial no Brasil: entre a "neutralidade" técnica e o perfilamento racial. **Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, Rio de Janeiro, v. 15, n. 4, 2021.

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

COLLINS, Patricia Hill; **BILGE**, Sirma. **Interseccionalidade**. Tradução de Rane Souza. São Paulo: Boitempo, 2021.

FACIOLI, Lara; **PADILHA**, Maria Helena L. Algoritmos e sociedade: a mediação tecnológica nas interações sociais. **Revista de Ciências Sociais**, Fortaleza, v. 51, n. 2, 2020.

GALVANI, Giovanna. 90% das pessoas presas por reconhecimento facial são negras, diz estudo. **Carta Capital**, [S. l.], 22 nov. 2023. Política. Disponível em: <https://www.cartacapital.com.br/politica/90-das-pessoas-presas-por-reconhecimento-facial-sao-negras-diz-estudo/>. Acesso em: 24 abr. 2026.

GONÇALVES, Rodrigo. Algoritmos como mediadores da informação digital e o impacto na democracia. **Revista Brasileira de Ciência Política**, Brasília, n. 42, 2024.

LYON, David. The culture of surveillance: watching as a way of life. Cambridge: Polity Press, 2018.

NOBLE, Safiya Umoja. Algoritmos da opressão: como os mecanismos de busca reforçam o racismo. Tradução de Alice Martins de Moraes. Santo André: Editora Poli-Logos, 2021.

O'NEIL, Cathy. Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça a democracia. Tradução de Rafael Abraham. Santo André: Editora Poli-Logos, 2020.

PASQUALE, Frank. The Black Box Society: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PESSI, Diego; SOUZA, Leonardo Giardin de. Bandidolatria e democídio: ensaios sobre garantismo penal e a criminalidade no Brasil. Santa Catarina: Editora Resistência Cultural, 2017.

ROSA, Pablo Ornelas. Governamentalidade algorítmica: a gestão do risco no capitalismo de dados. São Paulo: LiberArs, 2019.

ROSA, Pablo Ornelas; ANGELO, Tiago Rafael dos Santos; ALMEIDA, Paulo Ricardo de; VIEIRA, Vanessa Maria. Criminologia tecnoconservadora e governamentalidade algorítmica: o sistema de justiça criminal e as políticas de controle de drogas no Brasil. Cadernos do CEAS, Salvador/Recife, v. 50, n. 264, p. 238-262, jan./abr. 2025.

ROSA, Pablo Ornelas; JOBIM, Marco Antônio; NEMER, David. Plataformentalização: a nova racionalidade do tecnoconservadorismo. Revista Sociedade e Estado, v. 38, n. 2, 2023.

SABARIEGO, Jesus. Tecno-política, algoritmos e movimentos sociais: uma análise crítica. **Revista de Estudos Sociais**, v. 20, n. 40, 2018.

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

SOUZA, Aknaton Toczek. Entre algoritmos e poder: reflexões de Pablo Ornelas Rosa acerca do tecnoconservadorismo e conflitos sociais. **Revista Temáticas**, Campinas, v. 33, n. 65, 2024.

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**, São Paulo, 26 mar. 2026. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2026/03/26/apos-ser-identificado-por-cameras-do-smart-sampa-morador-da-zona-sul-de-sp-e-detido-4-vezes-por-engano-em-7-meses.ghtml>. Acesso em: 13 abr. 2026.

¹ Doutoranda no programa de pós-graduação em Segurança Pública na Universidade Vila Velha- UVV. Mestra em Sociologia Política (Universidade Vila Velha- UVV). Bacharel em Direito (Universidade Vila Velha- UVV). Assessora Jurídica DT vinculada a Secretária de Justiça do Estado do Espírito Santo. E-mail: [acesse o artigo original para visualizar o e-mail](#). ORCID: <https://orcid.org/0000-0001-7748-294X>

² Doutoranda em Segurança Pública PPGSEG/UVV. Mestre em Sociologia Política (Bolsista CAPES) pela Universidade de Vila Velha (UVV). Possui uma sólida formação em Pedagogia pelo Centro Capixaba de Ensino Superior, complementada por múltiplas Pós-Graduações lato sensu em áreas estratégicas da Educação: Gestão

Educacional (Administração, Supervisão, Orientação e Inspeção Escolar). Combina a prática profissional com a pesquisa acadêmica, participando do Núcleo de Pesquisa em Ativismos, Resistências e Conflitos (NUPARC/UVV), sob a coordenação do Prof. Dr. Pablo Ornelas Rosa. Foco em temas que interseccionam a Segurança Pública, Sociologia Política, Gestão Escolar, Coordenação Pedagógica, Educação e a prática pedagógica na Educação Básica.

E-mail: [acesse o artigo original para visualizar o e-mail](#). Orcid:

<https://orcid.org/0000-0003-2958-8226>