Universidade de Brasília – UnB
Faculdade de Direito
Graduação em Direito

ANA LUIZA ALVES RODRIGUES

A COR DO ALGORITMO: COMO O POLICIAMENTO PREDITIVO E O RECONHECIMENTO FACIAL PODEM AUTOMATIZAR O RACISMO NO SISTEMA DE JUSTIÇA CRIMINAL BRASILEIRO.

Brasília
2026

Ana Luiza Alves Rodrigues

A COR DO ALGORITMO: COMO O POLICIAMENTO PREDITIVO E O RECONHECIMENTO FACIAL PODEM AUTOMATIZAR O RACISMO NO SISTEMA DE JUSTIÇA CRIMINAL.

Monografia apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador: Me. Pedro Diogo de Carvalho Monteiro
Coorientador(a): Dra. Luana Xavier Pinto Coelho

Brasília
2026

CIP - Catalogação na Publicação

AR696c

Alves Rodrigues , Ana Luiza .
A COR DO ALGORITMO: Como O Policiamento Preditivo E O Reconhecimento Facial Podem Automatizar O Racismo No Sistema De Justiça Criminal. / Ana Luiza Alves Rodrigues ;

Orientador: Me. Pedro Diogo de Carvalho Monteiro ; co-orientador Dra. Luana Xavier Pinto Coelho. Brasília, 2026.
93 f.

Trabalho de Conclusão de Curso (Graduação - Direito) Universidade de Brasília, 2026.

1. racismo estrutural. 2. reconhecimento facial. 3. policiamento preditivo. 4. vigilância algorítmica. 5. processo penal. I. de Carvalho Monteiro , Me. Pedro Diogo , orient. II. Xavier Pinto Coelho, Dra. Luana, co-orient. III. Título.

Ana Luiza Alves Rodrigues

A COR DO ALGORITMO**:** Como O Policiamento Preditivo E O Reconhecimento Facial Podem Automatizar O Racismo No Sistema De Justiça Criminal.

Trabalho de conclusão de curso apresentado à Faculdade de Direito da Universidade de Brasília como requisito parcial para a obtenção do título de Bacharel em Direito.

Data de Aprovação:

Me. Pedro Diogo de Carvalho Monteiro – Orientador

Dra. Luana Xavier Pinto Coelho – Coorientadora

Me. Tiago Kalkmann – Membro da Banca

Dr. Tarcízio Silva – Membro da Banca

A todas as pessoas que foram vistas antes de serem conhecidas. Classificadas antes de serem ouvidas. Punidas antes de serem compreendidas. Às que tiveram suas histórias reduzidas a registros, números e categorias de suspeição. Às que foram afetadas por decisões tomadas em nome da neutralidade. Este trabalho existe porque vocês existiram. E porque o silêncio também tem um custo.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, por ter me sustentado em cada etapa desse caminho e por transformar em possível o que tantas vezes pareceu distante.

Antes que eu acreditasse ser possível, antes que eu ousasse sequer imaginar esse momento, duas pessoas já acreditavam por mim. Já oravam, já torciam, já guardavam no coração uma certeza que eu ainda não tinha encontrado em mim mesma. Por isso, os meus agradecimentos mais profundos e mais verdadeiros são para Rosimary e Gerson, meus pais.

Vocês foram o meu primeiro abrigo, a minha primeira força e a razão pela qual muitos dos meus sonhos, inclusive este, puderam deixar de ser apenas sonhos. Em cada etapa desta caminhada, mesmo quando o caminho parecia difícil demais, eu carreguei comigo o amor, a fé e os ensinamentos que recebi de ambos. A dedicação de vocês, a garra silenciosa, o cuidado diário e a confiança depositada em mim, inclusive quando eu mesma duvidei, foram essenciais para que eu chegasse até aqui.

Se hoje encerro esta etapa, é porque nunca caminhei sozinha. Caminhei sustentada pelas orações da minha mãe, pelo esforço do meu pai, pelo amor que sempre ofereceram e por tudo aquilo que, muitas vezes, fizeram em silêncio para que eu pudesse continuar. Esta conquista não é apenas minha. Ela carrega a história, os sacrifícios, a esperança e o amor da nossa família. Tudo o que sou também nasce de tudo o que recebi ao longo da vida com vocês.

Agradeço também a Roseli e Elinaldo, meus dindos, que me acolheram como filha e cuidaram de mim com tanto amor ao longo desses anos. A presença de vocês foi uma das bases que me sustentaram nesta caminhada. Em muitos momentos, o apoio, o carinho e o cuidado de vocês tornaram o caminho mais leve e me fizeram sentir amparada, mesmo nos dias mais difíceis. Sou profundamente grata por tudo o que fizeram por mim, pelas portas abertas, pelo afeto constante e pela forma generosa com que sempre estiveram ao meu lado. Sem vocês, eu também não teria chegado até aqui. Esta conquista carrega, de alguma forma, um pouco do amor e do cuidado que recebi de vocês.

Rafael, você foi minha calmaria em meio à tempestade. Em muitos momentos desta caminhada, quando o cansaço parecia maior que a força, foi o seu apoio que me ajudou a continuar. Obrigada por estar ao meu lado nos dias difíceis, por me acolher nos momentos de dúvida e por me lembrar, tantas vezes, daquilo que eu mesma esquecia: que eu era capaz. Não há palavras suficientes para traduzir tudo o que você representou nesta jornada. Seu amor, sua paciência e sua confiança foram abrigo nos dias mais pesados e impulso nos momentos em que eu precisei seguir. Obrigada, sobretudo, por nunca ter duvidado de mim, nem mesmo por um segundo.

Registro também minha gratidão às amizades que encontrei nesta caminhada e que levo comigo para além da Universidade. Sarah e Kalyani, vocês tornaram os dias mais humanos. Entre cafés, conversas, risadas e trabalhos que pareciam não ter fim, a rotina ficou mais leve e a graduação se tornou menos solitária. Foi uma honra dividir esse percurso com vocês. Foi uma honra dividir esse percurso com vocês. Não poderia deixar de agradecer também a Eduarda, Carliane, Priscila e Vilmar, que estiveram presentes em parte desta caminhada e deixaram marcas que ficam. Cada abraço, palavra de incentivo e, acima de tudo, a amizade de vocês, são coisas que carrego comigo com muito carinho.

Deixo meu muito obrigada ao professor Evandro. Entre os anos de 2023 e 2025, fui orientada por ele nesta mesma temática, período em que despertei meu interesse pelo tema e pude aprofundar minhas primeiras reflexões acadêmicas sobre ele. Sua orientação foi essencial para que eu amadurecesse o olhar crítico que hoje se reflete neste trabalho.

Agradeço ao Pedro, meu orientador, pela paciência, pela disponibilidade e pela generosidade com que acompanhou cada etapa da construção deste trabalho. Suas orientações, observações e conselhos foram fundamentais para o desenvolvimento desta pesquisa e contribuíram não apenas para a qualidade do trabalho, mas também para o meu crescimento acadêmico.

Agradeço também à minha coorientadora, Luana, pela leitura atenta, pelas observações criteriosas e pelo cuidado com que compartilhou seus conhecimentos, ajudando a aprimorar e fortalecer este estudo.

Por fim, agradeço aos avaliadores, que em meio à correria da rotina aceitaram compor a banca e participar desse momento tão marcante da minha caminhada.

Eu Só Quero É Ser Feliz

Mas eu só quero é ser feliz, feliz, feliz, feliz, feliz
Onde eu nasci, "han"
E poder me orgulhar
E ter a consciência que o pobre tem seu lugar

Minha cara autoridade, eu já não sei o que fazer
Com tanta violência eu sinto medo de viver
Pois moro na favela e sou muito desrespeitado
A tristeza e alegria aqui caminham lado a lado
Eu faço uma oração para uma santa protetora
Mas sou interrompido a tiros de metralhadora
Enquanto os ricos moram numa casa grande e bela
O pobre é humilhado, esculachado na favela
Já não aguento mais essa onda de violência
Só peço a autoridade um pouco mais de competência

Eu só quero é ser feliz
Andar tranquilamente na favela onde eu nasci, han
E poder me orgulhar
E ter a consciência que o pobre tem seu lugar
Mas eu só quero é ser feliz, feliz, feliz, feliz, feliz
Onde eu nasci, é
E poder me orgulhar
E ter a consciência que o pobre tem seu lugar

Diversão hoje em dia não podemos nem pensar
Pois até lá nos bailes, eles vêm nos humilhar
Ficar lá na praça que era tudo tão normal
Agora virou moda a violência no local
Pessoas inocentes que não tem nada a ver
Estão perdendo hoje o seu direito de viver
Nunca vi cartão postal que se destaque uma favela
Só vejo paisagem muito linda e muito bela
Quem vai pro exterior, da favela sente saudade
O gringo vem aqui e não conhece a realidade
Vai para a Zona Sul pra conhecer água de coco
E o pobre na favela vive passando sufoco
Trocaram a presidência, uma nova esperança
Sofri na tempestade, agora eu quero a bonança
O povo tem a força, precisa descobrir
Se eles lá não fazem nada, faremos tudo daqui

(Cidinho e Doca, 1995)

RESUMO

O presente trabalho analisa de que forma o policiamento preditivo e as tecnologias de reconhecimento facial, incorporados à segurança pública brasileira, podem atuar como mecanismos de reprodução e automatização do racismo estrutural. A pesquisa fundamenta-se na teoria do racismo estrutural de Silvio Almeida e no conceito de vigilância racializadora de Simone Browne, reconstruindo a trajetória histórica das práticas de controle sobre corpos negros no Brasil, desde o período escravocrata até a digitalização contemporânea da vigilância estatal. Sustenta-se que as tecnologias algorítmicas não representam ruptura com estruturas historicamente excludentes, mas sua reconfiguração sob a aparência de neutralidade técnica. O estudo examina os ciclos de retroalimentação do policiamento preditivo, a incidência de falsos positivos no reconhecimento facial e os riscos produzidos pela utilização de alertas automatizados em atividades policiais. A partir da análise das experiências da Bahia, de São Paulo, do Rio de Janeiro e do Distrito Federal, com especial atenção à Plataforma DF 360, bem como dos casos sobre ausência regulatória do México e do Chile, identificam-se tensões entre vigilância algorítmica e garantias fundamentais do processo penal, especialmente a fundada suspeita, a presunção de inocência, o contraditório e a ampla defesa. Conclui-se que tecnologias de vigilância não operam de forma neutra em sociedades estruturalmente desiguais e tendem a reproduzir padrões históricos de exclusão quando implementadas sem transparência, auditabilidade e controle democrático. O enfrentamento desse problema exige não apenas regulação adequada, mas o reconhecimento de que essas ferramentas incorporam dimensões históricas, políticas e raciais que não podem permanecer invisíveis ao debate jurídico.

Palavras-Chave: racismo estrutural; reconhecimento facial; policiamento preditivo; vigilância algorítmica; processo penal; seletividade racial.

ABSTRACT

This study analyzes how predictive policing and facial recognition technologies, when incorporated into Brazilian public security, may operate as mechanisms for the reproduction and automation of structural racism. The research is grounded in Silvio Almeida's theory of structural racism and Simone Browne's concept of racializing surveillance, reconstructing the historical trajectory of control practices directed at Black bodies in Brazil, from the slavery period to the contemporary digitalization of state surveillance. It argues that algorithmic technologies do not represent a rupture with historically exclusionary structures, but rather their reconfiguration under the appearance of technical neutrality. The study examines feedback loops in predictive policing, the occurrence of false positives in facial recognition, and the risks arising from the use of automated alerts in police activities. Based on the analysis of experiences in Bahia, São Paulo, Rio de Janeiro and the Federal District, with special attention to the DF 360 Platform, as well as comparative cases from Mexico and Chile, the research identifies tensions between algorithmic surveillance and fundamental guarantees of Brazilian criminal procedure, especially reasonable suspicion, the presumption of innocence, adversarial proceedings and the right to a full defense. It concludes that surveillance technologies do not operate neutrally in structurally unequal societies and tend to reproduce historical patterns of exclusion when implemented without transparency, auditability and democratic oversight. Addressing this problem requires not only adequate regulation, but also the recognition that these tools incorporate historical, political and racial dimensions that cannot remain invisible to legal debate.

Keywords: *structural racism; facial recognition; predictive policing; algorithmic surveillance; criminal procedure; racial selectivity.*

SUMÁRIO

1. INTRODUÇÃO..... 10
2. RAÇA E TECNOLOGIA..... 15
2.1. Do Conceito De Raça Ao Racismo Estrutural..... 15
2.2. O Avanço Tecnológico E Os Riscos Aos Direito Fundamentais..... 21
2.3. Policiamento Preditivo: A Criminalização Do Território E O Ciclo De Retroalimentação..... 29
2.4. Reconhecimento Facial: A Individualização Da Suspeita E O Falso Positivo..... 31
2.5. O Vácuo Regulatório E A Terceirização Da "Fundada Suspeita"..... 32
3. O RECONHECIMENTO FACIAL E A AUTOMAÇÃO DO RACISMO NO BRASIL. 37
3.1. Bahia: O Pioneirismo, A Opacidade E A Vigilância Racializadora..... 38
3.2. São Paulo: A Megalópole Sob Vigilância Panóptica..... 43
3.3. Rio de Janeiro: O Falso Positivo como Dado Estrutural..... 46
3.4. O Padrão Comum: expansão tecnológica e vácuo regulatório..... 49
3.5. O Horizonte Regulatório: Entre a Portaria e o Marco Legal..... 53
4. RECONHECIMENTO FACIAL E A AUTOMAÇÃO DO RACISMO NO DISTRITO FEDERAL..... 59
4.1. A Implementação do Reconhecimento Facial em Brasília..... 62
4.2. O Choque com o Processo Penal e a Conclusão do Estudo de Caso..... 67
4.2.1 O Reconhecimento Facial diante da LGPD no Contexto da Segurança Pública. 70
4.3 A Plataforma DF 360: Avanço Tecnológico, Vácuo Democrático..... 72
5. CONCLUSÃO..... 78
REFERÊNCIAS..... 85

1. INTRODUÇÃO

Há uma narrativa recorrente que acompanha o desenvolvimento das tecnologias algorítmicas de vigilância. Ela parte da ideia de que a máquina, diferentemente do ser humano, seria capaz de operar de forma neutra, livre de preconceitos, subjetividades ou condicionamentos históricos. Nessa lógica, algoritmos não enxergariam raça, classe ou estereótipos, mas apenas processariam dados, identificariam padrões e produziriam resultados supostamente objetivos. A substituição da decisão humana pela racionalidade técnica apareceria, assim, como um avanço inevitável e, mais do que isso, como uma promessa de maior justiça e imparcialidade. Este trabalho parte justamente da recusa dessa premissa.

A objetividade tecnológica não surge em um vazio social. Dados não existem de forma autônoma nem são produzidos fora das estruturas que organizam a realidade. São construídos por instituições específicas, em determinados contextos históricos e, muitas vezes, a partir de relações de poder que antecedem a própria tecnologia. A conversão da realidade em números não elimina as desigualdades que marcam sua origem.

Quando sistemas de policiamento preditivo são treinados com registros produzidos por um modelo de segurança pública historicamente seletivo, que concentra sua atuação em territórios periféricos e sobre a população negra, o algoritmo não passa a identificar a criminalidade de maneira espontânea ou neutra. Como demonstra Cathy O’Neil (2020, p. 6), tais sistemas não revelam realidades objetivas, mas “programam preconceitos, equívocos e vieses humanos nos sistemas de *software*” (O’Neil, 2020, p. 6). No contexto do policiamento, esse mecanismo produz aquilo que a autora identifica como um ciclo de retroalimentação, em que "a própria polícia gera novos dados, o que justifica mais policiamento" (O'Neil, 2020, p. 83), direcionando a vigilância para bairros empobrecidos e majoritariamente negros. Assim, "mesmo que um modelo não enxergue a cor da pele, o resultado o faz" (O'Neil, 2020, p. 83).

Nesse contexto, a neutralidade deixa de representar uma qualidade técnica e passa a exercer outra função. Sua invocação frequentemente opera como mecanismo de legitimação. A aparência de objetividade científica pode ocultar escolhas institucionais anteriores, naturalizar desigualdades historicamente construídas e conferir nova autoridade a práticas já marcadas pela seletividade. Pesquisadoras como Ruha Bejamin (2019) e Cathy O’Neil (2020) têm demonstrado que a invocação da neutralidade tecnológica frequentemente opera como mecanismo de legitimação institucional.

A aparência de objetividade científica pode ocultar escolhas políticas anteriores, naturalizar desigualdades historicamente construídas e conferir nova autoridade a práticas já marcadas pela seletividade (Benjamin, 2019; O'Neil, 2020). O problema, portanto, não reside apenas na tecnologia em si, mas na crença de que ela seria capaz de operar à margem da história, da política e das estruturas sociais que a produziram. Nesse sentido, Ruha Benjamin (2019) adverte que a tecnologia costuma ser apresentada como neutra, algo construído fora de contextos políticos e sociais, percepção que, segundo a autora, precisa ser constantemente questionada (Benjamin, 2019).

Este trabalho tem por objeto a análise da utilização de tecnologias algorítmicas de vigilância no sistema de segurança pública brasileiro, especialmente o reconhecimento facial e o policiamento preditivo, e seus impactos sobre a população negra em um sistema marcado pelo racismo, à luz dos princípios constitucionais do processo penal. A questão central que orienta a pesquisa consiste em compreender em que medida a incorporação dessas tecnologias, dentro de um sistema de justiça criminal historicamente marcado pela seletividade racial, representa uma ruptura com práticas discriminatórias ou, ao contrário, automatiza e reforça mecanismos já existentes sob uma nova roupagem técnica.

A hipótese que orienta o percurso argumentativo parte da premissa de que essas tecnologias não operam de maneira neutra. Apoiando-se na teoria crítica da raça e nos estudos sobre racismo estrutural e algorítmico, em especial nas contribuições de Almeida (2019), Benjamin (2019), Browne (2015) e O'Neil (2020), sustenta-se que a aparente objetividade matemática desses sistemas não elimina desigualdades estruturais; em muitos casos, apenas as reproduz, intensifica e torna menos visíveis.

Quando algoritmos aprendem a partir de dados historicamente produzidos por um sistema penal seletivo, que direciona sua atuação de forma desproporcional a determinados territórios e corpos, não identificam padrões naturais de criminalidade. Aprendem, na realidade, os mesmos critérios históricos de vigilância utilizados pelo Estado. Ao reproduzir esse olhar em escala automatizada e revesti-lo de aparente neutralidade científica, acabam atribuindo nova legitimidade a estruturas já existentes.

A relevância do estudo apresenta dimensão jurídica e política. Sob a perspectiva jurídica, a expansão dessas tecnologias cria tensões diretas com garantias processuais fundamentais, especialmente a exigência de fundada suspeita para abordagens sem mandado, prevista no artigo 244 do Código de Processo Penal, além da presunção de inocência, do

contraditório e da ampla defesa. Sob a perspectiva política, a insuficiência regulatória, analisada neste trabalho não como falha episódica, mas como elemento estrutural, cria um ambiente propício à ampliação do poder de vigilância estatal sem mecanismos adequados de transparência, auditabilidade e prestação de contas, sobretudo sobre populações historicamente marginalizadas.

O recorte temporal privilegia o período compreendido entre 2018 e 2026, fase em que o reconhecimento facial deixou de ocupar posição meramente experimental e passou a integrar, de forma progressiva, políticas de segurança pública em diferentes unidades federativas brasileiras. O recorte espacial articula duas escalas de análise. A primeira concentra-se no cenário nacional, especialmente nos casos da Bahia, de São Paulo e do Rio de Janeiro, experiências que permitem observar diferentes formas de implementação, seletividade, opacidade e produção de falsos positivos. A segunda recai sobre o Distrito Federal, escolhido em razão de características particularmente relevantes relacionadas à segregação urbana, à concentração territorial da vigilância e à implementação recente da Plataforma DF 360, que intensifica a integração entre videomonitoramento, inteligência artificial, reconhecimento facial, leitura de placas e câmeras públicas e privadas.

A metodologia adotada possui caráter qualitativo e interdisciplinar. A pesquisa mobiliza bibliografia em criminologia crítica, teoria racial, processo penal, ciência política, proteção de dados e estudos sobre vigilância, além da análise documental de legislações, projetos normativos, relatórios institucionais, notas técnicas, decisões judiciais, atos administrativos e publicações oficiais. A base teórica articula as contribuições de Silvio Almeida sobre racismo estrutural, Simone Browne sobre vigilância racializante, Michel Foucault sobre as relações entre poder e disciplina e Achille Mbembe sobre necropolítica, categorias que permitem compreender as continuidades históricas dos mecanismos de controle sobre corpos racializados e sua reconfiguração contemporânea por meio da técnica.

O trabalho está estruturado em quatro capítulos. O primeiro reconstrói a formação histórica do racismo estrutural, analisando a construção da raça enquanto tecnologia de poder e suas relações com práticas históricas de vigilância, classificação e controle. Nesse momento, também se delimita o uso do conceito de racismo estrutural, a fim de evitar seu esvaziamento, isso porque, reconhecer o racismo como estrutural não significa diluir responsabilidades institucionais, mas demonstrar como normas, rotinas administrativas, práticas policiais e critérios aparentemente neutros podem reproduzir desigualdades raciais de forma sistemática.

O segundo capítulo examina o policiamento preditivo e o reconhecimento facial como tecnologias de segurança pública que operam a partir de bancos de dados produzidos em sociedades profundamente desiguais. Analisa-se, nesse contexto, o ciclo de retroalimentação pelo qual territórios historicamente mais policiados produzem mais registros, que posteriormente justificam novas camadas de vigilância. O capítulo também discute os impactos dessas ferramentas sobre o processo penal, especialmente quando a suspeição deixa de se apoiar em elementos concretos e individualizados e passa a ser mediada por classificações estatísticas, alertas automatizados ou percentuais de compatibilidade biométrica.

O terceiro capítulo sistematiza a implementação dessas tecnologias no Brasil, com enfoque nos casos da Bahia, de São Paulo e do Rio de Janeiro. A experiência baiana permite observar a concentração racial dos impactos do reconhecimento facial; o caso paulista evidencia a opacidade produzida pela ausência de dados raciais suficientes; e a trajetória fluminense demonstra a continuidade da política pública mesmo diante de falhas documentadas e falsos positivos. O capítulo também amplia a análise para experiências latino-americanas, quanto a regulação dessas tecnologias, como México e Chile, e examina o horizonte regulatório brasileiro, especialmente a Lei Geral de Proteção de Dados, a ausência de uma LGPD Penal, a Portaria MJSP nº 961/2025 e o Projeto de Lei nº 2.338/2023.

Quando essa lógica passa a operar por meio de códigos, bancos de dados e percentuais de compatibilidade biométrica, o problema não desaparece. Apenas assume novas formas. O algoritmo não precisa de intenção discriminatória para reproduzir desigualdades. Precisa apenas aprender a partir dos dados disponíveis. E, em uma sociedade marcada por profundas assimetrias históricas, os próprios dados carregam as marcas dessa trajetória. Dados também possuem história. E, no Brasil, essa história não pode ser dissociada da raça.

Por fim, o quarto capítulo aprofunda o estudo do Distrito Federal, território em que segregação urbana, expansão da vigilância biométrica e fragilidades regulatórias se entrelaçam de maneira particularmente expressiva. Analisa-se a Lei Distrital nº 6.712/2020, que disciplinou o uso do reconhecimento facial antes de sua consolidação em larga escala, mas deixou lacunas relevantes quanto à auditabilidade, aos relatórios de impacto, ao compartilhamento de dados e à fiscalização externa. Em seguida, examina-se a Plataforma DF 360, compreendida não apenas como instrumento de modernização administrativa, mas como arquitetura integrada de vigilância, capaz de articular câmeras públicas e privadas, reconhecimento facial, leitura automatizada de placas e integração entre órgãos de segurança.

No presente trabalho, nomear o problema trata-se de uma escolha metodológica e epistemológica e não apenas retórica. O racismo estrutural somente pode ser enfrentado quando deixa de ser compreendido como desvio episódico ou falha excepcional e passa a ser reconhecido como lógica de funcionamento de instituições que, mesmo sob a aparência da legalidade, da eficiência e da neutralidade técnica, produzem efeitos sistemáticos de exclusão.

Quando essa lógica passa a operar por meio de códigos, bancos de dados, câmeras inteligentes e percentuais de compatibilidade biométrica, o problema não desaparece. Apenas assume novas formas. O algoritmo não precisa de intenção discriminatória para reproduzir desigualdades. Precisa apenas aprender a partir dos dados disponíveis. E, em uma sociedade marcada por profundas assimetrias históricas, os próprios dados carregam as marcas dessa trajetória. Dados também possuem história. E, no Brasil, essa história não pode ser dissociada da raça.

2. RAÇA E TECNOLOGIA

2.1. Do Conceito De Raça Ao Racismo Estrutural

"Cabelinho duro. Parece uma vassoura. Vou pegar para varrer o chão lá de casa", estas são ofensas proferidas por adolescentes contra uma colega de turma, no Centro de Ensino Fundamental 214 Sul, na Asa Sul, Distrito Federal e circulou por vídeo nas redes sociais (Alves; Sales, 2025)[1]. Em nota, a Direção da escola informou que o aluno responsável pelo vídeo foi identificado e transferido.

Em outro episódio, a jovem Maria Otília teve seu cabelo *black power* apagado pelo sistema de reconhecimento biométrico da PCDF, durante o procedimento de emissão de documento de identidade, em uma delegacia de Polícia Civil do DF (Quirino, 2025)[2]. Em entrevista concedida ao portal Brasil de Fato DF, a jovem narra que

> O sistema não configurou meu cabelo crespo volumoso como um cabelo, me deixou careca e em outro momento esbranquiçou toda a parte do meu cabelo. Me senti violada em todos os sentidos, pediram para amarrar meu cabelo e ao amarrar o sistema aceitou na foto da identidade (Otília *apud* Quirino, 2025).

Em ambas as situações, as vítimas sofreram racismo. No primeiro caso, porém, houve uma manifestação mais aberta e explícita da violência racial. Já no segundo, contudo, o racismo assume contornos mais sutis e dissimulados. Ele se configura, por vezes, como um mero erro tecnológico, quando, na realidade, trata-se de uma violência própria do racismo emaranhado na sociedade, que agora é mediado e perpetuado pela tecnologia.

Trata-se de um processo em que o racismo não desaparece, mas se reescreve no código, sendo mascarado sob a aparência de modernidade. Desta forma, ele adquire uma camada de invisibilidade conferida pela suposta objetividade algorítmica. É nesse sentido que a socióloga Ruha Benjamin (2019, p. 10) desenvolve o conceito de *New Jim Code*:

> Argumento que as soluções tecnológicas frequentemente ocultam, aceleram e até aprofundam a discriminação, enquanto aparentam ser neutras ou benevolentes em comparação com o racismo de uma era anterior. Este conjunto de práticas que denomino *New Jim Code* abrange uma série de projetos discriminatórios, alguns que explicitamente amplificam hierarquias, muitos que ignoram e, assim, replicam

[1]Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2025/09/30/adolescente-e-vitima-de-ofensas-racistas-em-video-publicado-por-colega-nas-redes-sociais.ghtml. Acesso em: 6 de jan. de 2026

[2]Discponível em: https://www.brasildefato.com.br/2025/07/24/foi-racismo-sistema-de-identificacao-do-df-apaga-cabelo-de-jovem-negra/. Acesso em: 6 de jan. 2026

> divisões sociais, e outros que visam corrigir o viés racial, mas acabam fazendo o oposto. (Tradução Própria)[3]

Esse disfarce encontra terreno fértil nas tecnologias contemporâneas devido à construção cuidadosa e intencional do conceito de vigilância, tendo como parâmetro a raça, a qual, por sua vez, teve o seu significado moldado durante as mais diferentes civilizações, mas que, no fim, coloca o branco como ser ideal a ser alcançado.

O termo raça constitui-se como uma construção social utilizada para legitimar relações de poder e dominação. Para Munanga (2004, p. 6), trata-se de "um conceito carregado de ideologia" cujo campo semântico é determinado pelas relações de poder que governam a estrutura social, e não por distinções biológicas ou genéticas. Em complemento, Almeida (2019, p. 18) destaca que o significado da raça está inevitavelmente ligado às circunstâncias históricas em que é utilizado, sendo sempre associado a contingência, conflito e poder. Assim, a categoria racial é resultado de uma construção intencional e histórica, constantemente atualizada nos diferentes contextos sociais, inclusive, agora, no campo tecnológico.

Nesse sentido, Silvio Almeida (2019, p.18) afirma que:

> Raça não é um termo fixo, estático. Seu sentido está inevitavelmente atrelado às circunstâncias históricas em que é utilizado. Por trás da raça sempre há contingência, conflito, poder e decisão, de tal sorte que se trata de um conceito relacional e histórico. Assim, a história da raça ou das raças é a história da constituição política e econômica das sociedades contemporâneas. (Almeida, 2019, p.18)

Deste modo, a construção de categorias raciais e de hierarquias entre povos ganhou novo impulso a partir do século XVIII, especialmente com o advento do Iluminismo. Como observa Almeida (2019), foi nesse período que o ser humano passou a ser concebido como objeto do conhecimento científico. A pretensão iluminista de ordenar, classificar e explicar racionalmente o mundo também alcançou os próprios indivíduos, inaugurando processos de categorização que buscavam diferenciar grupos humanos e estabelecer distinções hierárquicas

---

[3] *"I argue that tech fixes often hide, speed up, and even deepen discrimination, while appearing to be neutral or benevolent when compared to the racism of a previous era. This set of practices that I call the New Jim Code encompasses a range of discriminatory designs – some that explicitly work to amplify hierarchies, many that ignore and thus replicate social divisions, and a number that aim to fix racial bias but end up doing the opposite."* (Benjamin, 2019, p.10)

entre eles. A compreensão da raça como categoria histórica e relacional permite perceber que ela ultrapassa o mero marcador identitário e opera, de fato, como dispositivo de poder.

A razão iluminista, ao mesmo tempo em que se apresentava como símbolo de emancipação e progresso, serviu também como instrumento de dominação ao estabelecer padrões universais de humanidade. Sob essa lógica, o modelo europeu tornou-se a régua universal, excluindo todos os que não se adequavam a ele e consolidando distinções entre o civilizado e o selvagem (Almeida, 2019).

A colonização se instituiu como um projeto de salvação, progresso e civilização, no qual o homem europeu, tomado como ideal de racionalidade e humanidade, se coloca na posição de guia e redentor dos povos que ainda não conheciam a civilização nos moldes ocidentais. Mas, por trás dessa narrativa, encontrava-se um projeto de dominação orientado pela apropriação de territórios, pela exploração de povos subjugados e pela extração de riqueza em benefício das potências europeias. Como destaca Fanon (1961), a relação entre colonizador e colonizado foi construída e mantida pela violência, tendo a exploração como seu elemento central.

Desta forma, sob o argumento que os demais povos deveriam se adequar à civilização eurocristã, abriu-se caminho para que comunidades inteiras fossem exploradas, oprimidas e classificadas como inferiores. Essa lógica, que recebeu o disfarce de missão civilizatória, legitimou séculos de violência material e simbólica. Para Quijano (2005), essa herança não se encerra com o fim do colonialismo enquanto período histórico, pois o eixo racial de classificação social que o sustentava "provou ser mais duradouro e estável que o colonialismo em cuja matriz foi estabelecido" (Quijano, 2005, p.1), configurando o que o autor denomina colonialidade do poder, um padrão de dominação que segue estruturando as relações sociais, políticas e cognitivas no mundo contemporâneo.

Essa estrutura de dominação, fundada na racialização dos corpos e na hierarquização das culturas, não se limitou ao continente europeu, ela se expandiu pelas Américas e se enraizou profundamente na formação social brasileira.

No Brasil, o período escravagista foi decisivo para tornar o corpo negro hipervisível e construir, como aponta a socióloga Simone Browne, uma vigilância racionalizadora, isto é, uma forma de controle que utiliza a raça como parâmetro de poder (Browne *apud* Monteiro, 2022). Desde o navio negreiro, onde homens e mulheres eram marcados e subjugados, até as ruas e

instituições do pós-abolição, o olhar que vigia e define quem deve ser suspeito ou punido permanece orientado pela lógica herdada do colonialismo (Monteiro, 2022).

Essa vigilância foi construída com base no terror, na violência e opressão. Os indivíduos traficados eram marcados por ferro em brasa com o brasão da família a qual pertencia e durante o trabalho eram, por vezes, obrigados a usarem máscaras e outros aparelhos que tinham por objetivo única e exclusivamente humilhar, torturar e subjugar essas pessoas.

> O que a chave da vigilância racializadora permite compreender é que esses aparatos de terror e monitoramento tinham um papel produtivo nos processos de racialização fundamentada em posicionar o negro como o não-humano em face da sociedade civil, mesmo considerando que a presença negra era condição de existência material e subjetiva desta mesma sociedade. (Monteiro, 2022, p.22)

Desta forma, é claro que a vigilância sobre corpos negros não se limitava ao controle físico, mas também à construção simbólica da desumanização. A violência não era apenas meio de dominação, mas um modo de produzir subjetividades racionalizadoras, definindo quem poderia ser reconhecido como humano e quem seria reduzido à condição de objeto de vigilância.

A lógica de vigilância e controle construída durante a escravidão não se encerrou com a abolição formal. Ao contrário, os mecanismos de gestão e contenção da população negra foram reelaborados e incorporados às instituições estatais, especialmente ao sistema penal. Nesse contexto, Flauzina (2006, p. 58) observa que:

> O que esse dispositivo visa é que os escravizados passem da tutela dos senhores diretamente para a do Estado. A vadiagem é, em última instância, a criminalização da liberdade. Ou, podemos dizer, aos negros não é facultado o exercício de uma liberdade sem as amarras da vigilância. Assim, longe da cidadania, a sociedade imperial apreende os negros no desempenho de dois papéis: o de escravos ou criminosos. (Flauzina, 2006, p.58)

A observação de Flauzina (2006) demonstra que a abolição não representou uma ruptura com as estruturas de controle racial, mas sua reorganização sob novas bases institucionais. Essa permanência demonstra que a raça não se reduz a uma construção histórica situada no passado, mas se configura como um princípio estruturante das relações sociais desde a modernidade. Embora destituída de fundamento biológico, opera como categoria político-econômica apta a legitimar hierarquias e sustentar práticas discriminatórias.

Ao estabelecer quais corpos seriam dignos de reconhecimento e quais seriam reduzidos à condição de objeto, a noção de raça consolidou-se como instrumento central da dominação

colonial. Essa estrutura de classificação, fundada na diferença e na desigualdade, é o que permite compreender o racismo não como um comportamento individual, mas como uma lógica histórica e social que atravessa instituições, práticas e discursos, ou seja, como um elemento estrutural da sociedade.

Silvio Almeida, em sua obra *Racismo Estrutural* (2019), explica que o racismo pode ser compreendido a partir de três concepções. A primeira é a concepção individualista, na qual o racismo é entendido como uma patologia moral, uma forma de desvio de conduta ou irracionalidade individual (Almeida, 2019, p. 25). Nessa perspectiva, o racista é visto como alguém que, por ignorância ou má índole, reproduz comportamentos discriminatórios, restringindo o problema ao campo da moral pessoal.

A segunda é a concepção institucional, em que o poder ocupa papel central nas relações raciais. Diferentemente da anterior, essa concepção reconhece que os conflitos raciais não são fatos isolados, mas expressões de um sistema sustentado e reproduzido por instituições, como o Estado, a polícia, o sistema de justiça e o mercado de trabalho. Assim, o racismo ultrapassa o âmbito da ação individual e passa a ser compreendido como um fenômeno coletivo e estruturado (Almeida, 2019, p.26).

Por fim, a concepção estrutural aprofunda esse entendimento. Nela, Almeida (2019) propõe que as instituições não produzem desigualdades raciais por estarem isoladamente desviadas de uma ordem social neutra. Elas o fazem porque integram uma sociedade cuja própria organização histórica foi constituída pelo racismo como elemento estruturante (Almeida, 2019, p. 31). O racismo, portanto, não é um desvio da estrutura social. Ele participa de sua formação e de seu funcionamento. Trata-se de um modo de socialização em que a racialização organiza a distribuição de poder, de valor e de humanidade.

Essa afirmação, contudo, exige uma delimitação importante. Reconhecer o racismo como estrutural não significa afastar a responsabilidade das instituições, dos agentes públicos ou das práticas concretas que o reproduzem. Ao contrário, a força do conceito está justamente em demonstrar que o racismo não depende apenas de manifestações individuais explícitas para produzir efeitos. Ele também atua por meio de rotinas administrativas, critérios aparentemente neutros, decisões institucionais e práticas estatais que distribuem, de forma desigual, proteção, suspeição e violência.

Essa ressalva é necessária porque o conceito de racismo estrutural tem sido frequentemente esvaziado no debate público. Em alguns usos, a referência à estrutura acaba

funcionando como uma abstração conveniente, capaz de reconhecer a existência do problema sem identificar os mecanismos concretos que o reproduzem. A estrutura passa a aparecer como se fosse sujeito autônomo da discriminação, enquanto instituições, agentes e políticas públicas permanecem preservados de qualquer responsabilização. Essa leitura, porém, deturpa o sentido da formulação de Silvio Almeida. O racismo é estrutural não porque não tenha responsáveis, mas porque se reproduz no funcionamento ordinário das instituições, inclusive quando elas atuam sob a linguagem da legalidade, da técnica e da neutralidade.

A partir dessa concepção, o racismo deixa de ser compreendido como fenômeno episódico ou como resultado de práticas isoladas e passa a ser reconhecido como lógica de funcionamento da sociedade moderna. Ele está inscrito nas formas de produção, nas relações de trabalho, na política criminal, nas representações culturais e, sobretudo, nas instituições que naturalizam a desigualdade racial. Manifesta-se nos critérios de mérito, na distribuição desigual da violência e na invisibilidade cotidiana das exclusões.

Por estar entranhado nas estruturas, o racismo não precisa se manifestar abertamente para produzir efeitos. Ele atua na normalização das desigualdades e das discriminações, inclusive em situações aparentemente técnicas, como quando um sistema utilizado por órgão do Poder Executivo Estadual deixa de reconhecer cabelos *black power* como parte da identidade corporal de uma pessoa negra. Justamente por isso, reconhecer sua dimensão estrutural não afasta a responsabilidade institucional. Pelo contrário, permite compreender como essas desigualdades ganham concretude por meio de normas, práticas, critérios decisórios e formas de atuação estatal.

No campo da segurança pública, essa compreensão permite deslocar o debate da intenção individual para os padrões institucionais de atuação. A seletividade penal não depende apenas de manifestações abertamente racistas. Ela também se expressa na definição dos territórios mais policiados, nos critérios de suspeição, na distribuição desigual da vigilância e na forma como determinados corpos são reiteradamente tratados como ameaça. Nesse sentido, abordagens policiais seletivas, sub-representação de pessoas negras em espaços de poder e naturalização da violência estatal não podem ser lidas como fatos isolados. São expressões de uma lógica que atravessa as instituições e contribui para a manutenção de hierarquias raciais historicamente construídas.

Na segurança pública brasileira, essa dinâmica pode ser observada em dados empíricos. Estudo realizado pelo Instituto de Defesa do Direito de Defesa (2022) demonstra

que pessoas negras possuem 4,5 vezes mais chances de serem abordadas por policiais no Rio de Janeiro e em São Paulo (IDDD; Data Labe, 2022). O dado evidencia que a suspeição não se distribui de forma aleatória. Ela incide com maior intensidade sobre determinados corpos e territórios, reproduzindo padrões históricos de controle racializado.

Como observa Almeida (2019), o racismo estrutural não se mantém apesar das transformações sociais, mas por meio delas. Ele se reinventa em novas linguagens, práticas e tecnologias, ajustando-se às mudanças econômicas, políticas e institucionais. A promessa de neutralidade, objetividade e eficiência, tão presente nas instituições modernas, pode funcionar como um véu que encobre a permanência das desigualdades raciais. Assim, o discurso da técnica, do mérito ou da segurança muitas vezes substitui o discurso abertamente racista, mas mantém intacto o resultado: a produção sistemática da exclusão.

Ele não precisa de ofensas explícitas ou leis formalmente segregacionistas para operar, pois se incorpora à própria ideia de normalidade. Sua força está justamente em se apresentar como funcionamento natural das coisas (Almeida, 2019). Desse modo, o racismo deixa de ser exceção e se torna critério invisível que orienta quem é visto, ouvido e reconhecido, e quem permanece à margem.

É a partir dessa chave que se torna possível analisar o reconhecimento facial. A tecnologia não inaugura o racismo na segurança pública, nem cria sozinha a seletividade que marca o sistema penal brasileiro. O que ela pode fazer, em determinadas condições, é automatizar padrões já existentes de suspeição, conferindo-lhes nova aparência de objetividade. A linguagem técnica dos algoritmos pode ocultar a origem social dos dados que os alimentam e transformar desigualdades historicamente produzidas em critérios aparentemente impessoais de decisão. O problema, portanto, não está apenas na falha técnica da máquina, mas na estrutura social e institucional que define sobre quais dados ela aprende, quais corpos identifica com maior frequência e quais territórios ajuda a vigiar.

2.2. O Avanço Tecnológico E Os Riscos Aos Direito Fundamentais

Os mecanismos de controle e subjulgação da escravidão não desapareceram, apenas se reconfiguraram. Como explica Monteiro (2022), as tecnologias de identificação corporal e comunicação, como a antropometria e os telégrafos policiais, sucederam as marcas corporais e mantiveram a lógica de captura e controle de corpos negros.

Nas palavras do professor e pesquisador Evandro Pizza Duarte (1998, p. 210), o olhar vigilante da colônia foi substituído por uma prática "policialesca" que transformava a polícia urbana no novo feitor, agora a serviço do Estado:

> o desmando senhorial vai sendo substituído por uma prática policialesca que transformava a polícia urbana no novo feitor, agora do Estado que era constituído de senhores proprietários. A rua passa a integrar a periferia da propriedade privada desses senhores, um espaço cotidianamente dominado pelo seu mando; novos lugares para a "escravaria" são criados. (Silva *apud* Duarte, 1998, p. 210)

Nesse contexto, o olhar vigilante da colônia cede lugar ao olhar pretensamente científico do Estado moderno, que passa a legitimar a desigualdade racial sob o discurso da segurança e da racionalidade técnica. Assim, os mesmos processos que outrora legitimaram o açoite e a marca a ferro continuam operando, mas em linguagens digitais, mediadas por algoritmos e bancos de dados. É nesse deslocamento de forma, e não de finalidade, que se evidencia a permanência estrutural do controle racial, pois o desejo de vigilância sobre corpos racializados não se dissipou com o fim da escravidão; ao contrário, a preservação das hierarquias sociais impôs ao Estado o aperfeiçoamento contínuo de seus instrumentos de vigilância e coerção.

Em sua gênese colonial e escravagista, a tecnologia de controle operava de forma brutal e analógica, incidindo diretamente sobre a carne. O corpo negro foi o primeiro território de experimentação tecnológica da vigilância no Brasil. O ferro em brasa, a corrente, a máscara de flandres e o próprio navio negreiro operavam como as tecnologias de ponta de um sistema projetado para aniquilar a subjetividade e transformar a pessoa humana em mercadoria rastreável e subjugada (Monteiro, 2022).

Como observa Foucault (2014), a passagem das formas soberanas de punição para o poder disciplinar não representou mera alteração dos instrumentos de controle, mas uma transformação na racionalidade do exercício do poder. O suplício público, fundado na violência explícita sobre o corpo, gradualmente cede espaço a mecanismos contínuos de vigilância, observação e normalização voltados à produção de corpos dóceis e úteis.

Mas, tal transição não ocorreu de forma homogênea nem linear. No contexto brasileiro, marcado pela herança escravocrata e pela seletividade racial do sistema penal, a centralidade do corpo como espaço privilegiado de controle e violência não desaparece integralmente. Ao contrário, práticas disciplinares passam a coexistir com formas persistentes de sujeição corporal, revelando a sobreposição de tecnologias de poder que incidem de maneira desigual

sobre determinados grupos sociais (Mbembe, 2018). Para Mbembe (2018, p. 41), essa sobreposição revela uma das características centrais da experiência colonial e de suas permanências na contemporaneidade. Trata-se da articulação entre mecanismos disciplinares, biopolíticos e necropolíticos que, atuando de forma complementar, viabilizam formas profundas de controle, gestão e submissão de determinados grupos sociais.

A experiência brasileira, contudo, apresenta particularidades que desafiam uma compreensão linear desse processo. A formação social estruturada pela escravidão racializada não eliminou a centralidade do corpo como espaço direto de exercício da violência. Durante o período escravocrata, a vigilância operava mediante presença constante do feitor, do capitão do mato e da punição física como instrumento cotidiano de disciplina e contenção. O corpo negro não era apenas força de trabalho; constituía também objeto permanente de vigilância, suspeição e controle.

Com a abolição formal da escravidão e a transição para a ordem republicana, não se verifica a ruptura dessa racionalidade de controle, mas sua reconfiguração em novas bases institucionais. Embora deixassem de ocupar a condição jurídica de escravizados, homens e mulheres negros permaneceram excluídos do pleno exercício da cidadania. A nova ordem republicana não foi acompanhada de mecanismos capazes de assegurar sua participação efetiva na vida política e social.

Como demonstra Carvalho (2002, p. 35), a Lei Saraiva, de 1881, excluiu os analfabetos do direito ao voto, restrição que permaneceu em vigor após a proclamação da República. Em uma sociedade marcada pelos efeitos da escravidão e pela ausência de políticas de inclusão, tal medida manteve grande parte da população negra à margem da participação política formal.

Embora avanços pontuais tenham ocorrido ao longo do século XX, a ampliação mais abrangente dos direitos de cidadania somente se consolidaria com a Constituição Federal de 1988, que universalizou o sufrágio e consolidou direitos civis, políticos e sociais até então inacessíveis para parcelas significativas da população brasileira. Até lá, as estruturas de exclusão herdadas do período escravista continuaram operando sob novas formas. Nesse contexto, Flauzina (2006, p. 67) observa que o sistema penal republicano não rompeu com a lógica de controle racial, mas a reorganizou. Impedido de recorrer à escravidão como instrumento formal de dominação, o Estado passou a desenvolver mecanismos mais sofisticados de vigilância, contenção e criminalização direcionados à população negra.

A permanência dessas dinâmicas evidencia que a exclusão racial não pode ser compreendida como resultado de práticas isoladas ou de comportamentos individuais. Como sustenta Almeida (2019), o racismo integra o próprio funcionamento das instituições, influenciando a distribuição de direitos, oportunidades e formas de punição. Trata-se de uma lógica que atravessa a organização social brasileira e contribui para a reprodução de desigualdades raciais mesmo após o fim formal da escravidão.

A permanência dessas dinâmicas evidencia que a exclusão racial não decorre de condutas individuais isoladas. Como sustenta Almeida (2019), o racismo estrutura o funcionamento das instituições e influencia a distribuição de direitos, oportunidades e formas de punição. Nesse cenário, os mecanismos de vigilância e controle direcionados à população negra não podem ser compreendidos como desvios ocasionais, mas como manifestações de uma lógica institucional que atravessa a formação social brasileira.

Sob a forte influência da Criminologia Positivista europeia de Cesare Lombroso, pensadores e médicos legistas brasileiros, com destaque para as formulações de Nina Rodrigues, adaptaram o determinismo biológico ao contexto nacional, atribuindo à população negra e racializada uma suposta propensão à criminalidade. Como aponta Juliana Borges (2019), esse processo foi fundamental para a consolidação de um sistema penal seletivo, que, desde suas origens, opera como mecanismo de gestão e contenção de corpos racializados.

A tecnologia punitiva, portanto, não desaparece, mas se transforma. O que antes se realizava pela marca a fogo passa a operar por meio da fita métrica, do compasso e da fotografia criminal. Trata-se de uma mudança de técnica, não de finalidade. Como evidência Achille Mbembe (2018), nas sociedades contemporâneas, o poder de decidir quem deve viver e quem pode morrer assume formas difusas e tecnicamente mediadas, mantendo, contudo, sua base histórica de hierarquização racial.

Com o encerramento formal do período escravocrata, as formas de legitimação do controle racial não desapareceram. Elas passaram por um processo de reorganização discursiva. Se antes a inferiorização da população negra encontrava justificativa na própria estrutura jurídica da escravidão, após a abolição novas teorias buscaram conferir aparência científica às mesmas hierarquias. Nesse contexto, a antropometria e a frenologia passaram a ocupar papel central na produção de discursos que pretendiam explicar diferenças sociais e comportamentais a partir de características biológicas.

Como demonstra Flauzina (2006), esse deslocamento permitiu que o sistema de justiça criminal reformulasse os fundamentos da suspeição racial. A periculosidade atribuída ao corpo negro deixou de ser justificada por sua antiga condição jurídica de propriedade e passou a ser associada a supostas predisposições naturais, anomalias físicas e determinismos biológicos. Sob o discurso da neutralidade científica, médicos e juristas, como Nina Rodrigues (1894), forneceram sustentação teórica para práticas de controle social voltadas à gestão de determinadas populações.

O racismo encontrava, nesse movimento, nova forma de legitimação. A violência estatal deixava de ser apresentada como exercício arbitrário de poder e passava a ser justificada pelo discurso técnico da defesa social, da prevenção e da profilaxia criminal (Batista, 2011)[4].

Com o avanço do século XX e, sobretudo, com a revolução da microinformática, essa racionalidade de controle não se rompe, mas se reconfigura em novas bases tecnológicas. O controle penal adentra, então, a fase da digitalização e da datificação, na qual a gestão dos corpos passa a ocorrer por meio do processamento massivo de informações. Os antigos arquivos físicos, compostos por fichas datilografadas, fotografias e registros biométricos rudimentares, cedem lugar a bancos de dados integrados, capazes de cruzar, armazenar e recuperar informações em escala inédita.

Paralelamente, o espaço urbano passa a ser progressivamente capturado por dispositivos de vigilância, como os circuitos fechados de televisão (CFTV), ampliando a capacidade de monitoramento estatal sobre a circulação dos indivíduos. O panoptismo descrito por Foucault (2014) constitui uma racionalidade de vigilância fundada na possibilidade permanente de observação e na internalização do controle pelos próprios indivíduos. No contexto contemporâneo, essa lógica não se altera em sua estrutura fundamental, mas passa a ser operacionalizada por instrumentos tecnológicos cada vez mais sofisticados. O monitoramento eletrônico amplia a capacidade de coleta, processamento e circulação de dados, expandindo os mecanismos de vigilância para além dos espaços institucionais tradicionais e transformando, nesse processo, indivíduos em perfis informacionais continuamente identificáveis e rastreáveis.

[4] O conceito de “profilaxia social”, recorrente na criminologia positivista e na medicina legal do final do século XIX, insere-se em uma racionalidade higienista que buscava prevenir a “degeneração” social por meio da vigilância e contenção de indivíduos classificados como perigosos (Batista, 2011). Tal noção operava como estratégia de legitimação da intervenção penal, frequentemente ancorada em pressupostos raciais e eugenistas, convertendo desigualdades sociais em supostas anomalias biológicas (Schwarcz, 1993).

Nesse novo estágio, o corpo negro, historicamente construído como objeto de suspeição pela dogmática jurídica e pelas pseudociências raciais, é traduzido em sequências de bytes, pixels e metadados. O olhar do Estado torna-se eletrônico, contínuo e silencioso, operando por meio de sistemas que aparentam neutralidade, mas que, como aponta Vera Malaguti Batista, estruturam historicamente a atuação do sistema penal brasileiro.

Ainda assim, nesse momento, a tecnologia permanece majoritariamente reativa: serve para registrar, catalogar e localizar indivíduos que já foram previamente capturados pelas engrenagens do sistema penal. Trata-se de uma vigilância que, embora mais sofisticada, continua ancorada em padrões históricos de seletividade, incidindo de forma desproporcional sobre os mesmos corpos que, desde o período escravocrata, figuram como alvos preferenciais do controle estatal.

A verdadeira virada de paradigma, que eleva o potencial lesivo desse controle a patamares inéditos, ocorre no século XXI, com a consolidação das tecnologias algorítmicas e preditivas. Se, até então, o aparato punitivo operava predominantemente como um repositório de informações pretéritas, limitado ao registro e à recuperação de dados, passa agora a reivindicar uma capacidade qualitativamente distinta, a qual trata-se de antecipar comportamentos futuros.

Essa inflexão está diretamente associada ao desenvolvimento da Inteligência Artificial (IA), compreendida como um conjunto de sistemas capazes de interpretar dados externos, aprender a partir deles e, com base nesse processo, executar tarefas de forma autônoma ou semiautônoma, aprimorando progressivamente seu desempenho (Kaplan e Haenlein, 2019, *apud* Paula, 2025, p. 15).

Nesse contexto, os algoritmos assumem papel central. Em termos simplificados, eles consistem em sequências lógicas de instruções que orientam o processamento de dados e a tomada de decisões por sistemas computacionais. Nos modelos contemporâneos de aprendizado de máquina, essas instruções não se limitam a regras fixas previamente definidas, mas passam a ser ajustadas dinamicamente a partir dos dados utilizados no treinamento do sistema.

Nesse sentido, Paula (2025), explica que:

> Um dos conceitos centrais para compreender os sistemas artificialmente inteligentes é o de algoritmo, que poderia ser definido como uma sequência finita de regras formais (operações lógicas e instruções) destinadas a tornar possível obter um resultado a partir de um conjunto de dados informados. Os algoritmos seriam como que “o centro de gravidade cognitivo” dos sistemas IA. (...) Um dos recursos fundamentais para a

> otimização dos algoritmos é o aprendizado de máquina (*machine learning*), por meio do qual o sistema se aprimora com base em sua experiência passada, sem ter sido explicitamente programado para assimilá-la de modo específico.

É precisamente nesse ponto que se insere a problemática do viés algorítmico. Como destaca Silvio Almeida, as estruturas sociais não são externas às tecnologias, mas se reproduzem por meio delas. Assim, quando sistemas algorítmicos são alimentados por bases de dados historicamente marcadas pela seletividade penal e racial, tendem a incorporar e reproduzir esses padrões sob a aparência de neutralidade técnica.

É precisamente essa combinação, capacidade preditiva e base de dados estruturalmente desigual, que inaugura uma nova etapa do controle penal. O cruzamento massivo de informações (Big Data), aliado a técnicas estatísticas avançadas, permite ao Estado não apenas reagir ao crime, mas mapear probabilidades, identificar "zonas de risco" e classificar indivíduos segundo graus de periculosidade presumida.

Nesse contexto, ganham protagonismo as tecnologias de reconhecimento facial e os sistemas de policiamento preditivo. No primeiro caso, algoritmos de visão computacional convertem características faciais em vetores matemáticos, comparando-os com bases de dados previamente armazenadas para fins de identificação. No segundo, modelos preditivos analisam padrões históricos de ocorrência criminal para indicar onde e quando a atuação policial deve ser intensificada.

A novidade decisiva dessa fase reside na reconfiguração do próprio processo decisório. O sistema deixa de ser apenas um instrumento de apoio e passa a exercer uma função orientadora, indicando territórios, corpos e condutas dignos de suspeição. Como resultado, o tirocínio policial é progressivamente deslocado para sistemas automatizados, que passam a influenciar e, em certos contextos, a determinar quem será abordado, vigiado ou neutralizado. Trata-se, em última análise, da delegação da suspeita a estruturas algorítmicas que, embora revestidas de tecnicidade, permanecem ancoradas nas mesmas lógicas históricas de seleção e controle.

Portanto, ao serem treinados por bases de dados forjadas ao longo de décadas de abordagens seletivas, hiperencarceramento e racismo estrutural, esses algoritmos não inovam; limitam-se a reproduzir, em alta velocidade e escala, os vieses das instituições que os alimentam. A suposta neutralidade matemática revela-se ilusória: a "cor" do algoritmo corresponde à mesma que historicamente preenche o sistema prisional brasileiro.

O racismo, nesse contexto, não apenas persiste, mas é automatizado e legitimado sob o discurso da objetividade técnica. Para Benjamin (2019, p. 54), os softwares de policiamento preditivo direcionarão sempre com maior probabilidade a polícia para bairros predominantemente negros, pois os dados que alimentam esses sistemas refletem prioridades de vigilância historicamente seletivas. A autora afirma que "os algoritmos de predição de crimes deveriam ser mais precisamente chamados de algoritmos de produção de crimes"[5] (Benjamin, 2019, p. 55, tradução própria). Forma-se, assim, um ciclo de retroalimentação no qual predições enviesadas orientam práticas policiais igualmente seletivas, que por sua vez produzem novos dados que reforçam as mesmas distorções.

É nesse cenário que emerge, de forma particularmente sensível, o problema regulatório. A rápida incorporação dessas tecnologias de vigilância, especialmente no contexto latino-americano e brasileiro, não tem sido acompanhada por mecanismos normativos capazes de impor limites, assegurar transparência ou viabilizar controle democrático.

Mais do que um simples descompasso entre inovação tecnológica e produção legislativa, essa lacuna revela uma funcionalidade política: a ausência de regulação rigorosa permite a expansão de sistemas opacos, sem exigência de auditabilidade, sem controle sobre vieses discriminatórios e sem garantias efetivas de contraditório frente a resultados automatizados.

Nesse contexto, o avanço tecnológico deixa de representar apenas inovação e passa a operar como instrumento de intensificação de práticas historicamente seletivas. O vácuo normativo converte-se, assim, em condição de possibilidade para a reprodução ampliada do controle racial, agora mediado por sistemas algorítmicos.

É sob essa lógica que se compreende a permanência de práticas de vigilância, controle e exclusão direcionadas a corpos racializados. A estrutura racista, que outrora se sustentava na escravidão e na hierarquia colonial, hoje se reatualiza sob os discursos da segurança, do progresso e da eficiência tecnológica. A forma se transforma, mas a lógica permanece, ainda se define quem deve ser vigiado, punido e silenciado a partir da raça.

---

[5] "*crime prediction algorithms should more accurately be called crime production algorithms*" (Benjamin, 2019, p. 55)

2.3. Policiamento Preditivo: A Criminalização Do Território E O Ciclo De Retroalimentação

Na era digital, o controle penal é um processamento de informações, desta forma o policiamento preditivo representa o momento em que o Estado decide utilizar esses dados não mais para reagir ao delito, mas para tentar se antecipar a ele.

Essa tentativa de antecipação denomina-se como policiamento preditivo (*predictive policing*), o qual fundamenta-se no uso de Inteligência Artificial e na análise de *Big Data* para identificar padrões em crimes passados e, a partir de modelos estatísticos, calcular probabilidade de ocorrências futuras (Perry et al., 2013). A grande promessa, que tem chamado atenção das autoridades é o fato de que se promete, em teoria, alocar recursos de segurança pública de forma mais eficiente, enviando viaturas para locais específicos antes mesmo que o crime ocorra (Lucena, 2020).

Essa suposta eficiência repousa sobre a perigosa premissa ilusória da neutralidade matemática. Pois, para gerar essas previsões, o algoritmo precisa ser alimentado com vastas bases de dados históricos, como registros de chamadas de emergência, boletins de ocorrência e relatórios de patrulhamento.

Contudo, os dados criminais não são um reflexo neutro e objetivo da criminalidade real de uma sociedade; eles são, antes de tudo, um registro da atividade policial. Em um país estruturalmente racista e desigual, a polícia historicamente patrulha, aborda e encarcera com muito mais frequência em bairros periféricos e populações negras (Flauzina, 2006). Se o sistema de justiça criminal sempre direcionou seu olhar punitivo para determinados territórios, a base de dados gerada por esse sistema será invariavelmente enviesada.

Quando uma base de dados viciada passa a alimentar o sistema, o algoritmo aprende a identificar as periferias como zonas de maior risco. Com isso, institucionaliza-se uma espécie de profecia autorrealizável, conhecida como ciclo de retroalimentação (Silva, 2022). O próprio sistema passa a direcionar um contingente desproporcional de policiais a esses territórios. Essa presença intensificada, por sua vez, eleva o número de abordagens e prisões, muitas vezes relacionadas a infrações de menor potencial ofensivo, como o porte de drogas para consumo próprio, condutas que dificilmente recebem a mesma atenção em bairros mais abastados.

Essas novas prisões são então inseridas no sistema como novos dados criminais daquela região, e o algoritmo, ao processar esses novos dados, confirma sua previsão inicial e eleva mais o suposto risco do local, justificando o envio de ainda mais viaturas no dia seguinte

(Lucena, 2020). O policiamento preditivo atua, assim, como uma engrenagem de criminalização territorial. A máquina não está descobrindo onde o crime vai acontecer; ela está apenas automatizando e acelerando a hipervigilância sobre os mesmos corpos e CEPs que o Estado sempre perseguiu (Silva,2022).

Essa engrenagem de criminalização territorial representa tensão profunda com as bases do Direito Penal democrático, aproximando-se daquilo que a doutrina denomina política criminal atuarial (Dieter, 2012). Nesse modelo, a atuação estatal deixa de se orientar exclusivamente pelo fato pretérito e pela culpabilidade individual, passando a incorporar critérios de cálculo probabilístico, gestão de riscos e antecipação da suspeita (Wermuth, 2017).

Quando essa racionalidade preditiva é transposta para a prática policial e forense, o impacto recai diretamente sobre as garantias do processo penal brasileiro. A fundada suspeita exigida pelo artigo 244 do Código de Processo Penal pressupõe elementos concretos e individualizados que justifiquem a intervenção estatal. O problema surge quando a suspeição passa a ser construída a partir de padrões estatísticos, territórios previamente classificados como perigosos ou perfis extraídos de bases de dados historicamente marcadas pela seletividade penal.

Na prática, esse deslocamento altera a própria forma de construção da suspeita policial. Quando uma área periférica é classificada como mancha criminal de alto risco, a abordagem tende a se apoiar menos em elementos concretos da conduta do cidadão e mais na leitura estatística do território. A suspeição passa a ser mediada por dados que, embora apresentados como técnicos, podem carregar o histórico de policiamento seletivo que alimentou o próprio sistema.

O agravante dessa criminalização automatizada reside na opacidade constitutiva desses sistemas. Os algoritmos de policiamento preditivo são desenvolvidos, em sua esmagadora maioria, por corporações privadas que protegem seus modelos de predição sob o argumento do segredo industrial. Isso, em casos concretos, resulta em violação de direitos. Nem o acusado, nem sua defesa técnica, e, muitas vezes, nem os próprios magistrados têm acesso aos critérios matemáticos, às variáveis consideradas ou ao peso atribuído a cada dado histórico utilizado na geração do chamado “mapa de calor”.

Sem a possibilidade de auditar o código e aferir a existência de vieses discriminatórios, sejam territoriais ou raciais, princípios constitucionais basilares, como o contraditório e a ampla defesa, tornam-se esvaziados diante da aparente infalibilidade do cálculo algorítmico.

2.4. Reconhecimento Facial: A Individualização Da Suspeita E O Falso Positivo

Se o policiamento preditivo opera na dimensão macroestrutural, criminalizando o território e direcionando o aparato repressivo do Estado para as periferias, o passo seguinte dessa engrenagem ocorre na dimensão microfísica: a individualização da suspeita. Uma vez que a força policial é enviada à zona de risco definida pela máquina, é importante que se questione como se decide quem será o alvo da abordagem.

É neste exato momento que o viés sai do mapa e recai diretamente sobre o rosto do indivíduo negro, materializando-se por meio das Tecnologias de Reconhecimento Facial (TRF). O panóptico digital, que antes calculava a probabilidade no espaço (Bruno, 2013), agora foca suas lentes na biometria, automatizando a decisão de quem deve ser capturado e resultando em um encarceramento massivo e enviesado da população negra brasileira (Nunes, 2024).

O funcionamento das TRFs baseia-se na visão computacional, que mapeia vetores geométricos e distâncias no rosto humano para encontrar correspondências (matches) em gigantescos bancos de dados criminais (Oliveira, 2020). No entanto, a concepção desses sistemas carrega em seu código-fonte o que a literatura contemporânea classifica como racismo algorítmico (Silva, 2022). As ferramentas de Inteligência Artificial não nascem em um vácuo social ou ético; elas são programadas por corporações de tecnologia do Norte Global, formadas majoritariamente por homens brancos, e treinadas em bases de dados profundamente homogêneas (Oliveira, 2020).

Quando o sistema é ensinado a reconhecer feições humanas utilizando milhares de imagens de rostos brancos e uma amostragem ínfima de rostos negros, sua acuidade visual torna-se racista por design. O algoritmo, operando sob proteção de segredo industrial em uma verdadeira caixa-preta opaca e inauditável, demonstra uma incapacidade estrutural de ler com precisão a pluralidade fenotípica da população negra, especialmente de mulheres negras. O sistema não enxerga o indivíduo; ele enxerga um borrão estatístico.

A consequência dessa falha arquitetônica ultrapassa a mera ineficiência tecnológica corporativa; no Brasil, ela se converte em violência de Estado por meio da explosão de falsos positivos (Nunes, 2024). O que para a empresa desenvolvedora do software representa apenas uma margem de erro aceitável no laboratório, no sistema de justiça criminal traduz-se em abordagens truculentas, constrangimentos públicos e prisões cautelares flagrantemente ilegais (Silva, 2022). Um cidadão negro e inocente tem seu rosto confundido com o de um foragido da

justiça simplesmente porque a máquina foi incapaz de distinguir seus traços. A tecnologia emite um alerta e, imediatamente, a presunção de inocência é aniquilada (Lopes JR., 2023).

Agrava-se a essa aniquilação a subversão dos ditames da própria metodologia forense. Quando o alerta algorítmico fundamenta a restrição de liberdade, ele adquire a natureza de vestígio digital. Contudo, a praxe inquisitória ignora as diretrizes processuais da cadeia de custódia da prova (arts. 158-A a 158-F do CPP).

O Estado instrumentaliza a captura, mas não preserva os metadados, o grau de confiabilidade do pareamento (*threshold*) ou o log de auditoria do sistema para escrutínio defensivo. Institucionaliza-se, de forma velada, um retorno ao arcaico sistema de prova tarifada, no qual o "match" da Inteligência Artificial ganha status de verdade absoluta e inquestionável, superior a qualquer elemento material ou testemunhal que a defesa possa produzir.

O impacto devastador do falso positivo subverte a lógica fundamental do processo penal democrático, operando uma verdadeira inversão probatória. A máquina reveste a suspeição policial de uma aura de infalibilidade matemática, fazendo com que o "match" algorítmico atue, na prática forense, como uma prova pericial inquestionável. Cabe ao indivíduo negro, muitas vezes já encarcerado injustamente em decorrência do erro do software, o ônus diabólico de provar para as instituições que ele não é a pessoa que o algoritmo afirma ser. O reconhecimento facial consagra, portanto, a automação do erro, conferindo ao racismo estrutural um selo de modernidade e eficácia irrefutável.

2.5. O Vácuo Regulatório E A Terceirização Da "Fundada Suspeita"

A convergência entre o policiamento preditivo e o reconhecimento facial deságua em uma crise na dogmática processual penal brasileira. Quando a máquina assume o papel de apontar o território violento e identificar o indivíduo perigoso, o que se observa na prática é a usurpação tecnológica de um instituto central do Estado Democrático de Direito: a fundada suspeita, exigida pelo artigo 244 do Código de Processo Penal para legitimar abordagens e buscas pessoais sem mandado judicial. Essa usurpação não é acidental. Ela é o produto de uma arquitetura de omissões, normativas, institucionais e políticas, cuja lógica não é de descuido, mas de conveniência.

A jurisprudência recente das Cortes Superiores, com destaque para as decisões da Sexta Turma do Superior Tribunal de Justiça, a exemplo do RHC 158.580/BA, tem realizado um esforço histórico para frear o perfilamento racial, exigindo que a abordagem policial seja

motivada por elementos objetivos e verificáveis, e não pelo tirocínio policial subjetivo que frequentemente encobre o preconceito.

A inserção da inteligência artificial, contudo, subverte esse esforço com uma sofisticação perturbadora. O algoritmo terceiriza o tirocínio, ou seja, o agente policial passa a justificar a intervenção no direito de ir e vir do cidadão com base exclusivamente no alerta emitido pelo sistema. O preconceito racial não desapareceu, ele tem sido apresentado ao operador do direito sob o disfarce de um dado estatístico aparentemente inquestionável. O que antes era um juízo subjetivo contestável torna-se, agora, uma saída objetiva de sistema e, por isso mesmo, muito mais difícil de impugnar.

As consequências jurídico-processuais desse deslocamento são graves e precisam ser nomeadas com clareza. Se a abordagem policial é deflagrada exclusivamente pelo alerta de um sistema de reconhecimento facial, sem qualquer outro elemento objetivo que a fundamente, ela carece do suporte normativo exigido pelo art. 244 do CPP e pela jurisprudência consolidada do STJ. Trata-se, portanto, de abordagem ilegal. E sendo ilegal a abordagem, contaminadas estão todas as provas dela decorrentes, nos termos do art. 157 do CPP e da doutrina dos frutos da árvore envenenada, consagrada no direito processual penal brasileiro.

A pergunta que o sistema de justiça criminal ainda não respondeu com a seriedade que o problema exige é que quando um cidadão é preso em flagrante com base em identificação feita por reconhecimento facial que mais tarde se revela um falso positivo, quem irá responder. A resposta, até o momento, tem sido o silêncio e esse silêncio é, ele próprio, uma forma de política.

Essa transferência da suspeita do agente público para o sistema computacional esbarra, inevitavelmente, no problema da opacidade. Os softwares de predição e reconhecimento facial adotados pelo Estado são, em sua esmagadora maioria, desenvolvidos e comercializados por empresas privadas, cujas lógicas de funcionamento, bases de treinamento e métricas de acerto são protegidas sob o manto do segredo industrial e da propriedade intelectual.

A opacidade algorítmica não é uma falha técnica tolerável, mas uma ruptura estrutural com os princípios que sustentam o Estado de Direito, como demonstra Pasquale (2015, p. 56), do ponto de vista jurídico, "inúmeras penalidades são impostas sem sequer uma aparência de devido processo legal"[6] (tradução própria), revelando que a lógica das caixas-pretas

[6] "*myriad penalties are imposed without even a semblance of due process"* (Pasquale, 2015, p. 56, tradução própria)

algorítmicas é fundamentalmente incompatível com as garantias processuais básicas. Sem acesso ao código-fonte, às bases de dados utilizadas no treinamento do modelo ou aos índices de erro por grupo demográfico, a defesa técnica se vê impossibilitada de contestar a validade da identificação algorítmica, tornando o contraditório e a ampla defesa formalidades vazias de conteúdo real.

Quando o cidadão não pode conhecer os critérios pelos quais foi identificado como suspeito, o contraditório e a ampla defesa deixam de ser garantias reais para se tornarem formalidades vazias. Se o sistema acusa um indivíduo, como a defesa técnica pode contestar a validade dessa identificação sem acesso ao código-fonte, às bases de dados utilizadas no treinamento do modelo ou aos índices de erro por grupo demográfico?

Sem a possibilidade de auditar a máquina, de demonstrar seus vieses, suas falhas sistêmicas, sua taxa de falsos positivos, a paridade de armas é estruturalmente inviabilizada. O algoritmo atua, simultaneamente, como denunciante e perito infalível e essa acumulação de funções, em qualquer outro contexto processual, seria imediatamente reconhecida como inaceitável.

O quadro se agrava porque essas violações operam sob um vácuo regulatório que, quanto mais examinado, menos parece casual. A Lei Geral de Proteção de Dados excluiu, de forma expressa, o tratamento de dados para fins de segurança pública e investigação criminal, nos termos do art. 4º, III. A prometida legislação específica para o setor, frequentemente chamada de “LGPD Penal”, segue paralisada no Congresso Nacional, sem perspectiva concreta de avanço.

Há iniciativas pontuais, como a Resolução nº 457/2022 do Conselho Nacional de Justiça, que trata do uso de inteligência artificial no Judiciário, e a Resolução nº 001/2021 do Conselho Nacional de Direitos Humanos, que recomenda a suspensão do reconhecimento facial na segurança pública até a edição de marco regulatório próprio. Ainda assim, são medidas insuficientes. São fragmentadas, não possuem força vinculante ampla e não enfrentam, de forma estrutural, a lacuna deixada pelo legislador.

O resultado é um espaço juridicamente desregulado, em que a ausência de proibição expressa passa a operar, na prática, como autorização implícita. Nesse ambiente, o Estado implementa sistemas de vigilância biométrica em larga escala sem dever claro de transparência, auditoria ou prestação de contas.

Esse vácuo, como já se indicou, não se explica por inércia legislativa. Ele cumpre uma função. E, como todo arranjo funcional, produz beneficiários claros. Empresas que fornecem sistemas de reconhecimento facial ao poder público operam sem dever de transparência sobre taxas de erro, sem responsabilização efetiva por danos decorrentes de falsos positivos e sem obrigação de adequar seus modelos às características demográficas da população brasileira. Por outro lado, gestores públicos que contratam e implementam essas tecnologias permanecem, em larga medida, imunes a mecanismos mais rigorosos de controle e responsabilização institucional. Enquanto isso, o sistema penal preserva sua seletividade estrutural, agora recoberta por uma aparência de neutralidade estatística.

As consequências desse cenário não são hipotéticas. No Brasil, casos como o do vigilante, que em 2022, na cidade de Salvador, foi preso e permaneceu 26 dias detido sob a acusação de ter praticado um roubo em 2012[7]. Segundo reportagem do G1, a prisão decorreu da existência de um mandado judicial vinculado ao nome do trabalhador, após o sistema de reconhecimento facial apontar uma suposta correspondência entre sua imagem e a da pessoa procurada. À época, a Secretaria de Segurança Pública da Bahia informou que o sistema havia identificado aproximadamente 95% de similaridade entre as imagens. Conforme noticiado pelo G1, a Secretaria não explicou como a imagem do vigilante passou a integrar a base de dados do sistema, apesar de ele não possuir histórico criminal. Questionada sobre os critérios de formação do banco de imagens utilizado pelo reconhecimento facial, a instituição também não apresentou informações que permitissem compreender os parâmetros adotados para a inclusão de pessoas nessa base de dados.

Casos como esse, expõem o custo concreto da ausência de regulação. Não se trata de risco abstrato. Trata-se de privação indevida de liberdade decorrente de erro tecnológico, sem que haja resposta institucional rápida e eficaz para corrigi-lo. Episódios dessa natureza não destoam do sistema. Ao contrário, são compatíveis com um modelo que transforma populações negras e periféricas em campo de aplicação dessas tecnologias, sem transparência, sem consentimento e sem responsabilização.

A máquina de suspeitar não substituiu o racismo do sistema de justiça criminal brasileiro. Ela o tornou mais eficiente, mais veloz e, sobretudo, mais difícil de ver. Garantir que a vigilância, o controle e o encarceramento continuem tendo uma cor e que essa cor permaneça

[7] Disponível em: https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoes-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-preso-por-26-dias.ghtml. Acesso em: 30 de abr. 2026.

escondida nas linhas de um código de computador é, precisamente, o que o vácuo regulatório foi construído para assegurar.

3. O RECONHECIMENTO FACIAL E A AUTOMAÇÃO DO RACISMO NO BRASIL

O Atlas da Violência 2025, elaborado pelo Instituto de Pesquisa Econômica Aplicada em parceria com o Fórum Brasileiro de Segurança Pública, demonstrou que, nos últimos anos, houve redução consistente nos índices de homicídio e de determinadas modalidades de violência letal no Brasil. Porém, de forma proporcionalmente inversa, a pesquisa demonstra que o fenômeno não foi acompanhado por diminuição equivalente da sensação coletiva de insegurança. Ao contrário, a pesquisa indica que a percepção social do medo permanece elevada, revelando um aparente descompasso entre os indicadores objetivos de violência e a experiência subjetiva da população (IPEA; FBSP, 2025).

À medida em que a sensação de insegurança se intensifica no imaginário coletivo, a segurança pública passa a ocupar uma posição de destaque, assumindo o protagonismo no debate político. Nesse processo, medidas estruturais voltadas ao enfrentamento das causas mais profundas da violência, como a redução das desigualdades sociais e a implementação de políticas preventivas, perdem força diante da busca por respostas rápidas e de efeito imediato. Ganham destaque, então, propostas associadas ao aumento do aparato policial, ao endurecimento das respostas penais, à ampliação do encarceramento e ao fortalecimento do poder estatal.

Sob a pressão por respostas imediatas à criminalidade, ferramentas como o reconhecimento facial e o policiamento preditivo passam a ser apresentadas como instrumentos capazes de antecipar riscos, identificar suspeitos e tornar a atuação estatal mais eficiente. Em um contexto atravessado pelo medo e pela urgência, a tecnologia costuma ser recebida sob a promessa de neutralidade e precisão, o que muitas vezes obscurece os riscos, limites e escolhas políticas que acompanham sua implementação.

Entretanto, à medida que o medo passa a orientar a formulação de políticas públicas, o debate tende a perder densidade crítica. A discussão deixa de se concentrar nos limites jurídicos, éticos e sociais dessas tecnologias e passa a privilegiar sua suposta eficácia. O perigo da implementação dessas tecnologias de forma acrítica reside no risco de reprodução, em linguagem tecnológica, de seletividades históricas já tão presentes não só na sociedade mas também no sistema penal.

A experiência brasileira ilustra como essa lógica tem se materializado na prática. O país não tem implementado essas tecnologias de forma coordenada. Sua adoção ocorreu de maneira fragmentada, impulsionada por iniciativas estaduais e municipais que, nos últimos

anos, avançaram em ritmo acelerado sobre um terreno normativo ainda em construção, influenciado por restrições orçamentárias, pressões eleitorais por eficiência policial e pela oferta cada vez mais agressiva de soluções tecnológicas instantâneas pelo mercado privado de segurança.

Ao final de 2024, ao menos 17 unidades federativas brasileiras encontravam-se em estágio de teste, utilização em larga escala ou em fase avançada de aquisição de sistemas de reconhecimento facial voltados à segurança pública e à persecução penal (Nunes et al., 2025). A amplitude dessa expansão demonstra que a incorporação dessas tecnologias ocorreu em ritmo significativamente superior ao desenvolvimento de parâmetros normativos capazes de definir seus limites, estabelecer critérios de funcionamento e assegurar mecanismos efetivos de controle e responsabilização.

O caso brasileiro demonstra uma grande heterogeneidade, manifestada nas escalas de operação, nos protocolos adotados, nos modelos de governança e nos impactos concretos produzidos, que o tornam um objeto particularmente complexo de análise. Estados como a Bahia operam sistemas de grande porte, com contratos que superam R$ 66 milhões e mais de 2.000 prisões mediadas pela tecnologia, enquanto outros entes federativos ainda se encontram em fase de teste ou sequer responderam às solicitações de informação encaminhadas pela Defensoria Pública da União e pelo CESeC (Nunes et al., 2025).

Cada estado contratou um tipo distinto de tecnologia e de empresa fornecedora, adotou critérios próprios para a formação de listas de procurados e definiu, de forma autônoma, os procedimentos de abordagem das pessoas identificadas pelos sistemas (Nunes et al., 2025). A fragmentação da implementação não apenas dificulta a construção de parâmetros uniformes de controle, como também revela que os efeitos dessas tecnologias não decorrem exclusivamente de sua arquitetura técnica, mas igualmente das estruturas institucionais e das dinâmicas sociais sobre as quais elas passam a operar.

3.1. Bahia: O Pioneirismo, A Opacidade E A Vigilância Racializadora

Em 2021, na Bahia, um assistente administrativo foi abordado por policiais militares na Avenida Paralela, em Salvador, enquanto esperava o ônibus após o trabalho. Em entrevista ao portal Intercept Brasil, ele conta que foi informado pelos agentes que o sistema de reconhecimento facial havia emitido alerta ao identificar similaridades entre seu rosto e o de um foragido da justiça registrado no banco de dados da Secretaria de Segurança Pública

enquanto passava pela Estação da Lapa do metrô[8] (Falcão, 2021). Após o alerta do sistema de reconhecimento, Davi foi monitorado por 15 estações. Ao final da abordagem, os policiais constataram o erro. Davi era inocente.

O Estado da Bahia é pioneiro na adoção de tecnologias de reconhecimento facial no Brasil (Santana, 2026). A utilização das TRFs pelo estado teve início em dezembro de 2018, por meio do projeto piloto de Vídeo-Policiamento, operacionalizado pela Secretaria de Segurança Pública da Bahia (Hosana, 2018). Segundo dados divulgados pelo próprio governo estadual, em 2026 o sistema teria auxiliado na localização e captura de 836 pessoas com mandados de prisão em aberto (Santana, 2026).

Os números, frequentemente mobilizados como indicativo de eficiência operacional, passaram a ocupar posição central no discurso institucional de legitimação da tecnologia. Entretanto, para além dos indicadores apresentados, é necessário compreender o contexto histórico, institucional e social no qual essa tecnologia foi incorporada, especialmente em um território marcado por profundas desigualdades raciais e por práticas históricas de controle seletivo.

Como demonstra Monteiro (2022), a introdução do reconhecimento facial na Bahia não constituiu uma ruptura institucional ou uma inovação isolada. Ao contrário, integrou um processo mais amplo e gradual de modernização tecnológica da arquitetura de vigilância estatal, cuja intensificação pode ser identificada a partir dos megaeventos esportivos realizados entre 2013 e 2014. A preparação para a Copa das Confederações de 2013 e para a Copa do Mundo de 2014 marcou um período de significativa expansão da infraestrutura de vigilância no país, impulsionando investimentos em sistemas de monitoramento, centros integrados de comando e tecnologias voltadas à circulação de imagens em tempo real entre diferentes órgãos de segurança pública (Brasil, 2014).

Tais investimentos consolidaram uma nova racionalidade de gestão da segurança, fundada na ampliação da capacidade de monitoramento permanente dos espaços urbanos e na centralização de informações em grandes estruturas de inteligência estatal. O legado mais expressivo desse processo foi a inauguração, em junho de 2016, do Centro de Operações e Inteligência 2 de Julho (COI), complexo de quatro andares construído com investimento

[8] Disponível em: https://www.intercept.com.br/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/. Acesso em: 30 de abr. 2026.

estadual de aproximadamente R$260 milhões, posteriormente convertido em núcleo estratégico da vigilância biométrica baiana (Monteiro, 2022).

A referência ao percurso histórico que antecede a implementação do reconhecimento facial evidencia que a tecnologia não emerge em um vazio institucional, tampouco inaugura formas inteiramente novas de controle social. Sua incorporação ocorre sobre estruturas preexistentes de vigilância, seletividade e gestão de populações consideradas suspeitas, aspecto especialmente relevante em um estado cuja composição demográfica e dinâmica urbana tornam incontornável a discussão acerca dos impactos racialmente diferenciados dessas ferramentas.

É nesse ambiente institucional previamente estruturado que o software de reconhecimento facial da empresa chinesa *Huawei* foi incorporado ao aparato tecnológico da Secretaria de Segurança Pública da Bahia (Senna, 2023). O processo de aquisição da ferramenta revela, nesse ponto, uma escolha administrativa cujas implicações jurídicas, políticas e éticas não podem ser ignoradas.

Em vez da instauração de procedimento licitatório autônomo, o governo estadual optou por incluir a tecnologia como aditivo a um contrato já existente com a empresa espanhola *El Corte Inglés Brasil Ltda*., responsável pela gestão do sistema de videomonitoramento empregado nos megaeventos esportivos. O expediente adotado permitiu contornar mecanismos mais amplos de publicidade e debate público acerca da implementação da tecnologia, viabilizando investimento de aproximadamente R$18 milhões para a fase piloto do projeto (Monteiro, 2022).

A forma de incorporação do sistema revela a lógica que passaria a marcar sua implementação. Conforme observa Monteiro (2022), o procedimento ocorreu sem a elaboração de qualquer instrumento equivalente a um Relatório de Impacto à Proteção de Dados. Ainda que a ausência possa ser parcialmente explicada pelo fato de a implementação anteceder a vigência da Lei Geral de Proteção de Dados, o dado permanece relevante.

A inexistência de mecanismos prévios de avaliação evidencia não apenas uma lacuna regulatória, mas uma postura institucional de baixa preocupação com os potenciais efeitos estruturais da tecnologia sobre a população submetida ao monitoramento. Antes mesmo da discussão acerca de precisão algorítmica ou eficiência operacional, chama atenção a ausência de reflexão sobre quem seria monitorado, sob quais critérios e quais grupos sociais suportariam, de forma mais intensa, os custos dessa expansão tecnológica.

O banco de dados responsável por alimentar o sistema biométrico baiano também fornece elementos relevantes para a compreensão crítica do modelo adotado. Inicialmente, a tecnologia foi alimentada por dois repositórios distintos: o Banco Nacional de Mandados de Prisão do Conselho Nacional de Justiça, responsável pelo fornecimento de registros fotográficos de indivíduos com ordens de prisão em aberto, e a Base de Registro Civil da Bahia, cujas imagens de maior qualidade foram incorporadas para reduzir a incidência de falsos alertas durante a fase inicial do projeto (Monteiro, 2022). A escolha dessas fontes está longe de representar uma decisão tecnicamente neutra.

Isso porque bancos de dados criminais não surgem de processos aleatórios de produção de informação estatal. São construídos historicamente a partir de dinâmicas específicas de abordagem policial, investigação e persecução penal, processos que, no contexto brasileiro, apresentam seletividades raciais e territoriais amplamente documentadas.

Quando sistemas algorítmicos passam a operar sobre bases produzidas em contextos marcados por filtragens sociais prévias, não ocorre uma ruptura com essas distorções históricas. Ao contrário, há a possibilidade de sua tradução para uma linguagem tecnológica revestida de aparente objetividade. O risco, portanto, não consiste apenas na automatização do reconhecimento, mas na automatização de padrões históricos de suspeição direcionados, de forma desproporcional, a corpos negros e territórios periféricos.

A fase posterior de expansão, denominada Projeto Vídeo Polícia Expansão, representou não apenas um aumento quantitativo da estrutura existente, mas uma transformação significativa em sua escala de atuação. Em julho de 2021, a empresa Oi Soluções foi contratada pelo valor de R$665 milhões para fornecer câmeras equipadas com reconhecimento facial e leitura automática de placas destinadas à capital e a outros setenta e sete municípios baianos, pelo prazo de sessenta meses (Monteiro, 2022). A ampliação do sistema, contudo, novamente não foi acompanhada por um debate público à altura de seus riscos.

Em sua pesquisa, Monteiro (2022) identifica que o Termo de Referência do projeto, composto por cento e cinquenta e cinco páginas, não faz qualquer menção a expressões como "viés", "falso positivo", "raça" ou "gênero", categorias que ocupam posição central nas discussões nacionais e internacionais sobre reconhecimento facial e discriminação algorítmica. Tal omissão não se trata de falha redacional. O silêncio sobre os riscos mais sensíveis associados à tecnologia restringe o escrutínio público e compromete a construção de

mecanismos democráticos de controle, revelando uma forma de implementação que faz da opacidade não um efeito colateral, mas um traço constitutivo do próprio modelo adotado.

A dimensão mais sensível da experiência baiana com o reconhecimento facial não está, propriamente, no número de capturas amplamente divulgado pela Secretaria de Segurança Pública, mas no perfil das pessoas alcançadas pelo sistema. Ainda nos primeiros meses de operação, entre março e outubro de 2019, o monitoramento realizado pela Rede de Observatórios da Segurança já apontava um padrão difícil de ignorar: 90,5% das pessoas abordadas eram negras, 87,9% eram homens e a idade média era de 35 anos (Nunes; Lima; Cruz, 2023). Desde então, o sistema acumulou ao menos 5.310 prisões até maio de 2026 (Santana, 2026), sem que tenham sido disponibilizados dados públicos atualizados sobre o perfil racial das pessoas abordadas.

Embora a realidade demográfica baiana exija cautela na interpretação isolada desses números, o dado assume maior relevância quando analisado em conjunto com a dinâmica historicamente seletiva do sistema de justiça criminal. A questão central não consiste apenas em identificar a presença majoritária de pessoas negras entre os indivíduos capturados, mas compreender porque determinados grupos seguem aparecendo, de forma recorrente, como principais destinatários das estratégias de vigilância e intervenção penal.

A análise das circunstâncias relacionadas às prisões reforça essa percepção. Entre os casos com informações disponíveis, crimes patrimoniais (especialmente roubos e furtos) representaram mais de 40% das capturas; delitos relacionados ao tráfico de entorpecentes corresponderam a aproximadamente 24%; e homicídios ocuparam a terceira posição, com cerca de 14% dos registros (Monteiro, 2022). O perfil encontrado reproduz, em larga medida, a composição historicamente conhecida da clientela do sistema penal brasileiro, sem indicar qualquer ruptura com os padrões seletivos que o caracterizam.

A promessa de neutralidade frequentemente atribuída às tecnologias algorítmicas passa a exigir maior cautela analítica. Algoritmos não aprendem a partir de dados neutros ou descontextualizados, eles operam, em verdade, sobre informações produzidas em estruturas institucionais preexistentes, atravessadas por décadas de abordagens seletivas e mecanismos historicamente desiguais de produção da suspeição penal.

Deste modo, a noção de vigilância racializadora, desenvolvida por Simone Browne, adquire especial relevância interpretativa. A categoria parte da compreensão de que tecnologias biométricas não constituem instrumentos neutros de identificação, mas dispositivos

historicamente situados, inseridos em processos mais amplos de administração, classificação e controle de corpos racializados. Sob essa perspectiva, o reconhecimento facial implementado na Bahia não representa uma ruptura disruptiva com práticas anteriores. Ao contrário, insere-se em uma longa genealogia de tecnologias de vigilância direcionadas ao corpo negro, que atravessa diferentes momentos históricos e diferentes formas de racionalização do controle social.

Do ferro em brasa ao registro antropométrico, do daguerreótipo criminal aos bancos contemporâneos de dados biométricos, alteram-se os instrumentos e a sofisticação técnica dos mecanismos empregados. Permanecem, contudo, questões estruturais relacionadas a quem é observado, quem se torna alvo preferencial da suspeição e quais grupos são continuamente transformados em objeto privilegiado das práticas de vigilância estatal. O que se modifica não é a lógica do controle, mas sua escala, sua velocidade e a legitimidade adicional produzida pelo discurso da objetividade tecnológica.

O caso baiano demonstra, portanto, que o debate sobre reconhecimento facial não pode permanecer restrito à sua capacidade de identificação ou aos números de capturas divulgados pelo poder público. Mais importante do que perguntar quantas pessoas foram localizadas é compreender quem são os indivíduos mais frequentemente submetidos à vigilância, quais territórios concentram a atuação desses sistemas e quais padrões históricos de suspeição são incorporados às novas tecnologias de controle.

3.2. São Paulo: A Megalópole Sob Vigilância Panóptica

Na cidade de São Paulo, Ailton Alves de Sousa, foi detido quatro vezes, no período de sete meses, por repetidos erros no sistema de reconhecimento facial[9] (Souza; Silva, 2026). Questionados pela equipe de reportagem do G1, “nem a Prefeitura nem a Secretaria de Segurança Pública souberam dizer quem poderia ter incluído a imagem do paulistano no sistema” (Souza; Silva, 2026).

Na mesma reportagem, a Prefeitura informou ainda que:

> ‘não houve qualquer falha no funcionamento do programa Smart Sampa’ e que a ‘atuação da Guarda Civil Metropolitana (GCM) ocorreu de forma regular, a partir de um alerta emitido pelo sistema de reconhecimento facial, seguido da confirmação de

[9] Disponível em: http://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: 30 de abr. 2026

> mandado de prisão ativo no Banco Nacional de Mandados de Prisão (BNMP)'. (Souza; Silva, 2026)

Já a Secretária Municipal de Segurança Urbana esclareceu que a inclusão de imagens é de responsabilidade dos órgãos do Poder Judiciário, informando ainda que a SSP foi comunicada para que tomasse as medidas cabíveis diante da situação (Souza; Silva, 2026).

Para além da disputa burocrática sobre competências institucionais, o caso do Ailton evidencia uma problemática mais profunda: a inexistência de qualquer agente ou órgão capaz de assumir a responsabilidade pela inserção indevida da imagem de um homem inocente em um sistema que o levou a ser detido quatro vezes em apenas sete meses, ao sair de casa, durante o trabalho, em um hospital e até mesmo enquanto participava de uma corrida de rua. A opacidade, aqui, não se limita ao funcionamento da tecnologia. Ela alcança as próprias instituições encarregadas de operá-la. Quando nenhum órgão sabe explicar, ou admite saber, como aquela fotografia ingressou no sistema, o erro perde sua autoria. E, sem autoria, dilui-se também qualquer possibilidade concreta de responsabilização.

No ano de 2014, a Secretaria de Segurança Pública do Estado apresentou o Sistema Detecta. O programa operava mediante câmeras equipadas com tecnologia de Reconhecimento Óptico de Caracteres (*OCR*), capazes de realizar leitura automática de placas veiculares e cruzar essas informações com registros de mandados de prisão, pessoas desaparecidas e restrições judiciais ativas. O sistema inaugurou uma lógica de gestão baseada na integração contínua de bancos de dados e na centralização de informações, possibilitando a localização de indivíduos já procurados pelo Estado (Peron *apud* Mello, 2024).

Essa racionalidade alcançou sua expressão mais abrangente no Programa Smart Sampa, contratado pela Prefeitura de São Paulo no segundo semestre de 2023. Operado por um consórcio formado pelas empresas Ellan, CLD e Grupo Protege, o projeto consolidou a maior infraestrutura de vigilância algorítmica urbana da América Latina (São Paulo, 2026). Em abril de 2026, o sistema já processava, de forma contínua, imagens provenientes de 50 mil câmeras espalhadas pela cidade, sendo 20 mil equipamentos públicos, 30 mil geridos por empresas privadas, com a possibilidade ainda de integração de câmeras particulares mediante requisitos específicos (São Paulo, 2026).

O dado revela aspecto particularmente relevante do modelo paulistano. Diferentemente de sistemas integralmente administrados pelo poder público, o *Smart Sampa* estrutura-se a partir de uma arquitetura híbrida que incorpora equipamentos privados à

infraestrutura estatal de monitoramento. A vigilância deixa, assim, de constituir atividade concentrada exclusivamente em órgãos públicos e passa a operar por meio de uma rede ampliada de atores institucionais e privados, cujos termos de compartilhamento de dados permanecem opacos para os titulares das informações coletadas. Pessoas que transitam por condomínios, estabelecimentos comerciais e sistemas de transporte integrados à plataforma dificilmente sabem que suas imagens podem integrar fluxos de processamento associados à segurança pública, circunstância que produz tensão evidente com os princípios da finalidade e da transparência previstos pela LGPD.

Segundo relatório institucional apresentado pelo município, os alertas produzidos pelo sistema não gerariam intervenções automáticas, exigindo etapa posterior de validação humana (São Paulo, 2026). A Prefeitura chegou a afirmar, em nota oficial de junho de 2025, que o Smart Sampa teria atingido taxa de assertividade de 99,5%, sem registrar "nenhuma pessoa presa por erro ou falha do sistema" (São Paulo, 2025). O caso de Ailton Alves de Sousa, no entanto, confronta diretamente essa narrativa.

A nota técnica elaborada pelo LAPIN em parceria com o Instituto de Referência Negra Peregum e a Rede Liberdades apresenta elementos que tornam mais complexa a narrativa institucional sobre os resultados do Smart Sampa. Entre as abordagens realizadas pelo sistema nas quais havia informação racial disponível, 25,09% das pessoas presas eram negras. O dado, por si só, já merece atenção, mas adquire relevância ainda maior quando observado que 58,9% dos registros não continham qualquer identificação racial (LAPIN; Peregum; Rede Liberdades, 2026).

Essa lacuna está longe de ser um detalhe meramente administrativo. Quando mais da metade dos registros não informa a raça das pessoas abordadas, torna-se inviável aferir com precisão a dimensão dos impactos raciais produzidos pela tecnologia. A ausência de dados, nesse contexto, não representa neutralidade. Ao contrário, limita o controle público, dificulta a fiscalização independente e enfraquece qualquer tentativa de identificar padrões discriminatórios. A opacidade, portanto, não é apenas técnica. Ela também se manifesta no plano estatístico, obscurecendo justamente as informações necessárias para avaliar quem suporta os custos mais elevados da expansão desses mecanismos de vigilância.

Não por acaso, o próprio Tribunal de Justiça do Estado de São Paulo manifestou preocupação com o funcionamento do sistema diante do percentual de prisões envolvendo pessoas negras (LAPIN; Peregum; Rede Liberdades, 2026). O questionamento revela que as

dúvidas sobre os efeitos discriminatórios da ferramenta não se restringem ao campo acadêmico ou às organizações da sociedade civil, alcançando também instituições responsáveis pelo controle e pela fiscalização da atividade estatal.

Se, na Bahia, o reconhecimento facial tornou visíveis os efeitos seletivos de uma tecnologia inserida em estruturas historicamente racializadas, em São Paulo o problema assume contornos distintos. Os dados disponíveis já apontam padrão preocupante, pessoas negras representam 25,09% das prisões realizadas pelo sistema nos registros com informação racial disponível, e o próprio Tribunal de Justiça do Estado manifestou preocupação com esse percentual. Mas 58,9% dos registros simplesmente não informam a raça das pessoas abordadas. A cidade que abriga a maior infraestrutura de vigilância algorítmica da América Latina é também aquela que não produz, ou não divulga, os dados necessários para avaliar plenamente quem suporta os custos desse sistema. O que os números revelam já é suficiente para inquietar. O que ocultam pode ser ainda mais.

3.3. Rio de Janeiro: O Falso Positivo como Dado Estrutural

A trajetória fluminense reproduz, sob diferentes contornos, a dinâmica já observada no caso baiano. Megaeventos funcionam como mecanismo de aceleração tecnológica e favorecem a implementação de soluções de vigilância em contextos de excepcionalidade, nos quais o debate público tende a ser reduzido, ou até mesmo, inexistentes. Permitindo, deste modo, que instrumentos de monitoramento passem a integrar estruturas permanentes sem que mecanismos equivalentes de transparência e avaliação de impacto sejam desenvolvidos.

Diferentemente da experiência baiana, o caso fluminense não chama atenção apenas pelos resultados produzidos pela tecnologia, mas pela sua continuidade apesar das limitações já documentadas. Entre 2019 e 2024, a Polícia Militar do Rio de Janeiro ampliou e retomou o uso de sistemas de reconhecimento facial mesmo após o registro de índices expressivos de erro. Em vez de provocar uma revisão mais ampla da política pública, as limitações documentadas coexistiram com a expansão da ferramenta, evidenciando a fragilidade dos mecanismos de avaliação e controle que deveriam anteceder sua utilização em larga escala.

O estudo *Um Rio de câmeras com olhos seletivos* (2022), elaborado pelo Centro de Estudos de Segurança e Cidadania, identificou que, durante testes realizados nos arredores do estádio do Maracanã em 2019, sete das onze pessoas detidas pela Polícia Militar não possuíam mandado de prisão em aberto, o que representava taxa inicial de erro superior a 60% (Nunes; Silva; Oliveira, 2022). Os resultados obtidos indicaram não apenas desempenho técnico

problemático, mas também ausência de evidências consistentes de que a tecnologia contribuísse para redução da criminalidade ou aprimoramento significativo da atividade policial cotidiana.

Apesar dos resultados registrados nos primeiros testes, a Polícia Militar retomou a utilização do sistema em 31 de dezembro de 2023, durante as comemorações de Réveillon, desta vez com 137 câmeras distribuídas pela capital fluminense. Em audiência pública realizada na Assembleia Legislativa do Estado do Rio de Janeiro, em setembro de 2024, o diretor de Infraestrutura de Tecnologia do Centro Integrado de Comando e Controle informou que, desde a reimplantação, o sistema acumulava taxa aproximada de 10% de falsos positivos (Continentino, 2024).

Embora números percentuais frequentemente sejam tratados como simples indicadores estatísticos, seus efeitos concretos exigem outra leitura. Das 330 prisões realizadas com auxílio do reconhecimento facial até aquele momento, aproximadamente 33 podem ter envolvido pessoas equivocadamente identificadas pelo sistema (Continentino, 2024). Em termos abstratos, a margem pode parecer residual. No plano concreto, contudo, cada erro representa a possibilidade de abordagem policial indevida, restrição de liberdade e submissão de indivíduos inocentes a mecanismos formais de suspeição estatal.

O número abstrato de falsos positivos adquire dimensão concreta quando observado a partir dos casos efetivamente documentados. Em abril de 2024, Daiane de Souza Melo, psicóloga e coordenadora de Promoção da Igualdade Racial do município de Nova Iguaçu, foi abordada por agentes do programa Segurança Presente enquanto participava da Conferência Estadual de Igualdade Racial, realizada no Liceu de Artes e Ofícios, no centro do Rio de Janeiro[10] (Braga, 2024). O sistema havia associado sua imagem à de uma mulher com mandado de prisão em aberto. Apesar de as diferenças físicas entre ambas serem imediatamente perceptíveis, inclusive para os próprios agentes envolvidos na abordagem, a liberação somente ocorreu após a apresentação de documento oficial de identificação (Braga, 2024).

O episódio ultrapassa a dimensão estatística e expõe, em escala individual, os efeitos concretos produzidos por sistemas automatizados de identificação. Em depoimento prestado à Defensoria Pública do Estado do Rio de Janeiro, Daiane descreveu que:

[10] Disponível em: https://defensoria.rj.def.br/noticia/detalhes/29955-Erro-em-reconhecimento-facial-constrange-psicologa-em-conferencia. Acesso em: 23 de mai. 2026.

> Eu já tinha lido sobre as câmeras não reconhecerem adequadamente rostos negros. É muito complicado a gente pensar que a segurança não está para todos. Eu acredito que a grande maioria das pessoas pretas, negras e pardas nascem, vivem e morrem com medo da polícia (Melo *apoud* Braga, 2024).

Para além da precisão estatística ou dos índices de desempenho algorítmico, emergem impactos subjetivos, psicológicos e sociais que dificilmente aparecem nos relatórios institucionais. O erro produz constrangimento, reforça experiências historicamente acumuladas de suspeição e reafirma percepções de vulnerabilidade já presentes na relação entre determinados grupos sociais e os aparatos de segurança estatal.

Sob essa perspectiva, o caso aproxima-se do que a literatura identifica como epidermização digital, conceito mobilizado por Simone Browne e retomado por Monteiro (2022) para descrever a continuidade de mecanismos históricos de classificação racial no ambiente tecnológico. O algoritmo passa a reproduzir, em linguagem computacional, estruturas de suspeição anteriormente exercidas pelo olhar policial. A diferença talvez não esteja na lógica do processo, mas na forma de sua legitimação. O que antes aparecia como seletividade humana passa a surgir revestido pela aparente neutralidade da técnica, tornando mais difusa a identificação dos responsáveis e mais complexa a atribuição de responsabilidade pelos danos produzidos.

As preocupações decorrentes desse modelo de vigilância ganharam novos contornos com o escândalo envolvendo o Sistema Córtex. Desenvolvido pelo Ministério da Justiça e Segurança Pública como uma plataforma de integração de dados para atividades de segurança pública, o sistema tornou-se alvo de questionamentos após a divulgação de informações sobre o uso massivo de suas bases de dados por credenciais vinculadas a órgãos de inteligência e à Polícia Militar do Estado do Rio de Janeiro.

Segundo reportagem do G1, aproximadamente 200 milhões de consultas foram realizadas em apenas oito meses, alcançando cerca de 69,2 milhões de CPFs (Barreira; Costa; Seehausen, 2025)[11]. O episódio evidenciou os riscos associados à concentração de grandes volumes de dados pessoais em sistemas de vigilância que operam com reduzidos níveis de transparência e controle externo, reforçando preocupações já apontadas pela literatura quanto aos impactos dessas tecnologias sobre direitos fundamentais.

[11] Disponível em: http://g1.globo.com/rj/rio-de-janeiro/noticia/2025/11/25/governo-federal-anuncia-suspensao-de-sistema-de-vigilancia.ghtml. Acesso em: 24 mar. 2026

No plano legislativo, a experiência fluminense também passou a produzir respostas institucionais relevantes. A Lei Estadual nº 10.141/2023 já estabelecia restrições a prisões fundamentadas exclusivamente em reconhecimento fotográfico, enquanto o Projeto de Lei nº 2.476/2024 propõe a exigência de Relatório de Impacto à Proteção de Dados para sistemas de reconhecimento biométrico facial em funcionamento no estado.

A experiência fluminense revela um fenômeno distinto daquele observado nos demais estados analisados. Se na Bahia o problema se manifesta na seletividade racial explicitada pelos dados e, em São Paulo, na insuficiência de transparência para aferi-la, no Rio de Janeiro a principal preocupação decorre da persistência institucional de uma tecnologia cujas limitações já haviam sido documentadas pelo próprio poder público. A continuidade e expansão do sistema, mesmo após sucessivos registros de falsos positivos, evidenciam um modelo de governança que naturaliza riscos conhecidos e transfere seus custos para os indivíduos indevidamente identificados.

3.4. O Padrão Comum: expansão tecnológica e vácuo regulatório

Os casos da Bahia, de São Paulo e do Rio de Janeiro revelam problemas distintos, mas convergem para um mesmo ponto. Na Bahia, os dados disponíveis permitiram visualizar a concentração dos impactos da tecnologia sobre a população negra. Em São Paulo, a insuficiência de informações raciais dificultou a própria aferição desses efeitos. No Rio de Janeiro, a manutenção e expansão do sistema ocorreram mesmo após o reconhecimento público de falhas relevantes em seu funcionamento. Embora cada experiência apresente particularidades, todas compartilham um elemento comum: a incorporação de tecnologias de reconhecimento facial em ritmo superior ao desenvolvimento de mecanismos capazes de assegurar transparência, auditabilidade e controle democrático.

Essa dinâmica não constitui fenômeno exclusivamente brasileiro. Em diferentes países da América Latina, a expansão de tecnologias de reconhecimento facial foi acompanhada por dificuldades semelhantes relacionadas à transparência, à supervisão institucional e à construção de salvaguardas capazes de limitar seus riscos. Embora inseridos em contextos sociais e jurídicos distintos, México e Chile oferecem exemplos particularmente relevantes desse processo e demonstram que o vácuo regulatório observado no Brasil integra uma tendência mais ampla de incorporação acelerada dessas ferramentas na região.

É importante esclarecer, desde logo, que México e Chile se inserem em contextos raciais distintos daquele que estrutura a realidade brasileira. Nesses países, a raça não ocupa o

mesmo papel organizador das relações sociais e institucionais discutido ao longo deste trabalho. Ainda assim, ambos enfrentam problemas relacionados à segregação territorial, à vulnerabilidade social e à insuficiência de mecanismos regulatórios, fatores que favorecem a expansão de tecnologias de vigilância sem controles adequados. A análise dessas experiências demonstra que a ausência de regulação não constitui uma particularidade brasileira, mas integra um fenômeno mais amplo observado em diferentes países da América Latina, revelando o caráter estrutural desse problema.

No México, a implementação de tecnologias de reconhecimento facial por órgãos estaduais e municipais ocorreu de forma acelerada e sem a criação de marcos normativos específicos destinados a disciplinar aspectos centrais de sua utilização. Levantamento realizado pela organização R3D, em parceria com o consórcio Al Sur, identificou a adoção desses sistemas em pelo menos quinze estados mexicanos, sem que houvesse regulamentação clara acerca de armazenamento de dados, auditoria independente, critérios de acesso às bases biométricas ou responsabilização em caso de erro (Ibarreche; Elebi; Di Lorenzo, 2025).

A experiência mexicana evidencia problema semelhante ao observado no contexto brasileiro. A expansão da capacidade de vigilância foi acompanhada por reduzidos mecanismos de fiscalização e controle. Além disso, organizações da sociedade civil documentaram a utilização dessas ferramentas para monitoramento de manifestações e protestos políticos, deslocando o reconhecimento facial para um campo especialmente sensível sob a perspectiva das liberdades civis e dos limites constitucionais ao exercício do poder estatal (Ibarreche; Elebi; Di Lorenzo, 2025).

O paralelo com México e Chile revela-se particularmente relevante não porque os contextos sejam idênticos, mas porque as fragilidades institucionais observadas apresentam notável convergência. A singularidade histórica do Distrito Federal, marcada por segregação territorial e seletividade espacial do policiamento, não afasta sua inserção em dinâmica regional mais ampla. Ao contrário, evidencia como diferentes realidades nacionais podem reproduzir mecanismos semelhantes de implementação tecnológica sob a lógica da urgência securitária.

O dado mais relevante, contudo, não reside apenas na expansão territorial da tecnologia, mas na inexistência de instrumentos jurídicos capazes de disciplinar aspectos centrais de sua utilização. Em nenhum dos casos examinados havia regulamentação específica definindo critérios de acesso aos bancos de dados, limites para armazenamento de imagens,

mecanismos independentes de auditoria ou parâmetros claros de responsabilização em hipóteses de erro.

O exemplo mais expressivo é o da Cidade do México, cujo Centro de Comando, Controle, Cómputo, Comunicações e Contato Ciudadano (C5) administra uma das maiores infraestruturas de videomonitoramento da América Latina. Desde 2019, o sistema opera mecanismos de reconhecimento facial em áreas estratégicas da cidade e incorporou soluções baseadas em inteligência artificial à política local de segurança pública.

Embora a Constituição mexicana contenha previsões relacionadas à proteção da privacidade, a ausência de pronunciamentos específicos da Suprema Corte sobre reconhecimento facial em larga escala produziu cenário de indefinição regulatória. Em contextos de rápida expansão tecnológica, esse silêncio institucional tende a produzir efeitos práticos relevantes, reduzindo parâmetros objetivos de controle sobre a utilização estatal dessas ferramentas.

A organização Al Sur documentou que tecnologias de reconhecimento facial no México passaram a ser utilizadas não apenas para identificação de pessoas com interesse investigativo ou mandados em aberto, mas também para monitoramento de participantes de manifestações e protestos políticos (AL SUR apud R3D, 2021). O dado possui relevância que ultrapassa discussão meramente operacional. A ampliação do uso dessas tecnologias para contextos relacionados ao exercício de direitos civis e políticos desloca o reconhecimento facial para zona especialmente sensível sob a perspectiva das garantias democráticas e dos limites constitucionais do poder estatal.

Segundo o levantamento, todo o ciclo de implementação da tecnologia, desde a contratação até sua operacionalização cotidiana, desenvolve-se em ambiente marcado por reduzida transparência institucional, ausência de protocolos claros de proteção de direitos e insuficiência de mecanismos efetivos de controle público. O relatório também chama atenção para os problemas associados ao desempenho técnico dos sistemas utilizados. As margens de erro identificadas apresentaram incidência desproporcional sobre determinados grupos populacionais, especialmente mulheres, jovens, pessoas não brancas e indivíduos transgênero ou não binários.

A relevância do caso mexicano para a presente pesquisa não reside apenas nas particularidades nacionais da experiência analisada, mas na recorrência dos mecanismos institucionais identificados. O paralelo com o Distrito Federal revela-se particularmente

significativo nesse ponto. Em fevereiro de 2026, a Plataforma DF 360 passou a incorporar imagens provenientes de câmeras privadas ao sistema público de monitoramento mediante procedimento simplificado de cadastramento eletrônico, descrito institucionalmente como processo passível de conclusão em poucos dias (Alves, 2026).

Mais do que coincidência operacional, a aproximação entre as experiências revela lógica estrutural semelhante. A incorporação progressiva da infraestrutura privada ao aparato estatal de vigilância amplia significativamente a capacidade de monitoramento sem que mecanismos equivalentes de auditoria, fiscalização independente ou avaliação prévia de impacto acompanhem essa expansão. Embora os atores institucionais sejam distintos, a estrutura do problema permanece substancialmente semelhante. A ampliação tecnológica ocorre em velocidade superior à construção das salvaguardas destinadas a limitar seus riscos.

O Chile, por sua vez, oferece paralelo distinto, mas igualmente revelador. Diferentemente de outras experiências latino-americanas, a preocupação institucional com os riscos do reconhecimento facial surgiu ainda em estágio inicial de implementação. Em 2019, o Consejo para la Transparencia (CPLT), órgão chileno responsável pela proteção de dados e transparência pública, manifestou preocupação formal diante da utilização de sistema de reconhecimento facial em um shopping center localizado em Las Condes, em Santiago.

O aspecto mais significativo do episódio reside no fato de que a avaliação técnica conduzida pela Polícia de Investigações do Chile (PDI), isto é, pelo próprio aparato estatal encarregado da segurança pública, concluiu que a tecnologia ainda não apresentava níveis satisfatórios de precisão e efetividade. O estudo identificou índices elevados de falsos positivos e levou o CPLT a formular diagnóstico particularmente expressivo: sistemas biométricos instalados em espaços públicos acabam por fazer "pagar justos por pecadores", uma vez que submetem indistintamente toda a população circulante a processos de coleta e análise de dados biométricos (CPLT, 2019).

A experiência chilena possui relevância analítica particular para o presente estudo por ao menos duas razões. A primeira consiste em evidenciar que o problema do falso positivo não representa especificidade do contexto racial brasileiro. Trata-se de limitação estrutural da própria tecnologia de reconhecimento facial, amplamente documentada pela literatura científica internacional, especialmente quanto ao desempenho sobre mulheres, pessoas não brancas, idosos e crianças (BUOLAMWINI; GEBRU, 2018). A segunda razão reside no fato de que o Chile produziu alertas institucionais antes da expansão massiva desses sistemas, circunstância

que evidencia que o simples reconhecimento dos riscos não é suficiente para impedir a difusão tecnológica.

O padrão regional que emerge dessas experiências é consistente. A tecnologia avança mais rapidamente do que os instrumentos jurídicos destinados a disciplinar sua utilização, e os custos dessa assimetria recaem, de forma desproporcional, sobre grupos historicamente submetidos a maiores níveis de vigilância estatal.

No Distrito Federal, a implantação da Plataforma DF 360 sem divulgação de relatório de impacto à proteção de dados, sem critérios transparentes para definição dos territórios prioritários de vigilância e sem mecanismos independentes de auditoria reproduz condições institucionais semelhantes às observadas nas experiências mexicana e chilena. O Planalto, portanto, não constitui exceção regional. Insere-se em dinâmica latino-americana mais ampla, na qual a expansão tecnológica frequentemente antecede a construção das garantias destinadas a limitá-la.

3.5. O Horizonte Regulatório: Entre a Portaria e o Marco Legal

As experiências examinadas ao longo deste capítulo revelam que os riscos associados ao reconhecimento facial não decorrem apenas das limitações técnicas da tecnologia, mas também da ausência de mecanismos jurídicos capazes de disciplinar sua utilização. A seletividade racial identificada na Bahia, a opacidade dos dados observada em São Paulo, a persistência de falsos positivos no Rio de Janeiro e as preocupações suscitadas pelo Sistema Córtex demonstram que a expansão dessas ferramentas foi acompanhada por um déficit de transparência, supervisão e controle institucional.

Embora o reconhecimento facial tenha sido progressivamente incorporado às políticas de segurança pública, a construção de salvaguardas jurídicas não ocorreu no mesmo ritmo. Em diversos casos, sistemas biométricos passaram a operar em larga escala sem a realização de avaliações prévias de impacto, sem mecanismos claros de fiscalização externa e sem parâmetros uniformes para tratamento dos dados coletados. O resultado foi a consolidação de um cenário em que a tecnologia avançou mais rapidamente do que a capacidade institucional de regular seus efeitos.

A insuficiência regulatória torna-se particularmente sensível quando observada à luz da Lei Geral de Proteção de Dados Pessoais. Embora a LGPD tenha estabelecido um regime abrangente de proteção de dados no ordenamento brasileiro, o legislador optou por excluir de sua incidência atividades relacionadas à segurança pública, à defesa nacional e à persecução

penal. A exclusão foi acompanhada da previsão de futura legislação específica destinada a disciplinar esses setores. Entretanto, passados vários anos desde a entrada em vigor da lei, esse marco regulatório ainda não foi aprovado.

Essa lacuna produz consequências relevantes. Enquanto empresas privadas e diversos órgãos públicos passaram a submeter-se a obrigações relacionadas à transparência, finalidade, necessidade e responsabilização pelo tratamento de dados pessoais, tecnologias biométricas empregadas em atividades de segurança pública continuaram operando em ambiente normativo significativamente menos estruturado. Forma-se, assim, uma situação paradoxal. Embora a LGPD tenha estabelecido parâmetros detalhados para o tratamento de dados pessoais em diversos setores, a utilização de tecnologias biométricas em atividades de segurança pública e persecução penal continua sem regulamentação específica equivalente. O resultado é que justamente nos contextos em que decisões estatais podem produzir restrições mais intensas à liberdade, à privacidade e à presunção de inocência, os mecanismos de proteção e controle permanecem mais frágeis.

O movimento mais concreto ocorreu em 24 de junho de 2025, com a publicação da Portaria MJSP nº 961/2025. Em seu artigo 11, o ato vedou expressamente a utilização, por órgãos vinculados à União, de softwares e sistemas de inteligência artificial destinados à realização de identificação biométrica à distância, em tempo real, em espaços acessíveis ao público, admitindo exceções apenas mediante autorização judicial prévia ou em hipóteses relacionadas ao flagrante delito (MJSP, 2025).

A norma representa avanço relevante ao reconhecer expressamente que determinadas aplicações biométricas apresentam riscos específicos para direitos fundamentais. Em especial, a portaria estabeleceu restrições ao uso de sistemas de identificação biométrica à distância, em tempo real, em espaços acessíveis ao público, admitindo sua utilização apenas em hipóteses excepcionais e mediante requisitos específicos.

O reconhecimento da natureza sensível dessas tecnologias possui relevância jurídica significativa. Durante anos, o debate público sobre reconhecimento facial esteve concentrado em aspectos relacionados à eficiência da atividade policial e à modernização dos sistemas de segurança. A portaria desloca parcialmente essa discussão ao reconhecer que a utilização de ferramentas biométricas envolve também questões relacionadas à privacidade, à proteção de dados e à liberdade individual.

Apesar de seu caráter inovador, a medida apresenta limitações importantes. Seu alcance permanece restrito aos órgãos vinculados à administração federal, sem incidência direta sobre estados e municípios, responsáveis pela maior parte das experiências de reconhecimento facial atualmente em funcionamento no país. Além disso, a norma não estabelece mecanismos permanentes de auditoria independente nem disciplina de forma aprofundada questões relacionadas à transparência algorítmica, à responsabilização por erros ou ao compartilhamento de dados biométricos entre diferentes instituições.

Paralelamente ao debate sobre reconhecimento facial, o Brasil passou a discutir a construção de um marco regulatório mais amplo para sistemas de inteligência artificial. Nesse contexto, o Projeto de Lei nº 2.338/2023 ocupa posição central. Inspirado em experiências internacionais, especialmente no modelo europeu de regulação por níveis de risco, o projeto classifica sistemas de identificação biométrica entre as aplicações consideradas de alto risco. A partir dessa classificação, prevê obrigações relacionadas à governança, à gestão de riscos e à realização de avaliações de impacto.

O reconhecimento de que determinadas aplicações exigem controles mais rigorosos representa avanço importante. Afinal, nem todos os sistemas de inteligência artificial produzem os mesmos efeitos nem apresentam os mesmos riscos. Tecnologias capazes de influenciar decisões estatais, restringir direitos ou produzir consequências relevantes para indivíduos demandam níveis mais elevados de supervisão e responsabilização.

Ainda assim, a proposta legislativa não elimina integralmente as preocupações já identificadas pela literatura especializada. Questões relacionadas à transparência dos modelos utilizados, à fiscalização independente dos sistemas e à efetiva capacidade de contestação dos resultados produzidos pelas ferramentas permanecem como desafios centrais. Em outras palavras, a discussão regulatória avança, mas ainda não responde integralmente às dificuldades concretas reveladas pela experiência brasileira.

Parte significativa do debate regulatório costuma concentrar-se na ideia de transparência. Embora esse aspecto seja fundamental, ele não esgota os desafios produzidos pelo reconhecimento facial.

Saber que determinado sistema está em funcionamento não significa necessariamente compreender como ele opera. A divulgação de informações genéricas sobre a existência da tecnologia não permite verificar quais bases de dados são utilizadas, quais critérios orientam os

processos de identificação ou quais índices de erro são efetivamente registrados durante sua operação.

É nesse contexto que emerge a importância da auditabilidade. Diferentemente da mera transparência formal, a auditabilidade pressupõe a possibilidade de fiscalização efetiva do funcionamento dos sistemas, permitindo a verificação independente de seus resultados, limitações e potenciais vieses.

A ausência desses mecanismos esteve presente em diferentes experiências analisadas ao longo deste trabalho. Em São Paulo, a insuficiência de dados raciais dificultou a própria aferição dos impactos produzidos pelo Smart Sampa. No Rio de Janeiro, a continuidade da política pública ocorreu mesmo após a identificação de falhas relevantes em seu funcionamento. No caso do Sistema Córtex, as controvérsias surgiram justamente em razão da limitada visibilidade sobre a forma de utilização e compartilhamento dos dados armazenados.

As implicações dessa opacidade tornam-se ainda mais relevantes quando sistemas biométricos passam a produzir efeitos na esfera penal. Nesses casos, o problema deixa de envolver apenas proteção de dados pessoais e passa a alcançar garantias processuais fundamentais.

A impossibilidade de acesso aos parâmetros técnicos utilizados pelos sistemas dificulta a verificação da confiabilidade das identificações realizadas e limita a capacidade de questionamento por parte da defesa. Sem mecanismos adequados de explicação, documentação e fiscalização, torna-se mais difícil exercer plenamente o contraditório e submeter os resultados produzidos pela tecnologia ao controle judicial efetivo.

As preocupações observadas no contexto brasileiro não constituem fenômeno isolado. Em diferentes países, a expansão de tecnologias biométricas também foi acompanhada por debates relacionados à proteção de direitos fundamentais e aos limites da vigilância estatal.

Nesse cenário, merece destaque o Regulamento Europeu de Inteligência Artificial (AI Act), que passou a tratar sistemas de identificação biométrica remota em tempo real como aplicações particularmente sensíveis. A regulamentação europeia estabeleceu restrições rigorosas para sua utilização em espaços públicos, admitindo exceções apenas em hipóteses específicas e sujeitas a controles reforçados.

Embora os contextos institucionais sejam distintos, a experiência europeia oferece parâmetro relevante para o debate brasileiro. A preocupação central não reside apenas na

precisão técnica dos sistemas, mas nos efeitos produzidos por sua utilização em ambientes caracterizados pela coleta massiva de dados e pelo monitoramento contínuo da população.

A experiência comparada demonstra que a discussão regulatória contemporânea tem se deslocado gradualmente da questão da eficiência tecnológica para a análise dos limites jurídicos necessários à sua utilização. Em outras palavras, o problema deixou de ser apenas o que a tecnologia é capaz de fazer e passou a envolver aquilo que uma sociedade democrática está disposta a permitir que ela faça.

Apesar dos avanços observados nos últimos anos, o cenário regulatório brasileiro permanece marcado por importantes lacunas.

Ainda inexistem mecanismos abrangentes de auditoria independente dos sistemas utilizados pelo poder público. Também permanecem insuficientemente disciplinadas questões relacionadas à realização de avaliações prévias de impacto, à transparência dos modelos empregados, à integração de bases biométricas e à responsabilização por erros decorrentes de identificações equivocadas.

Persistem, igualmente, dúvidas sobre os limites do compartilhamento de dados entre diferentes órgãos estatais, sobre as garantias disponíveis aos indivíduos submetidos à vigilância biométrica e sobre os mecanismos efetivos de controle judicial dessas tecnologias.

As experiências analisadas ao longo deste capítulo demonstram que tais preocupações não são meramente hipotéticas. Elas já se manifestaram de forma concreta em diferentes contextos brasileiros, seja por meio da produção de falsos positivos, da insuficiência de dados para avaliação de impactos discriminatórios ou da dificuldade de fiscalização das estruturas tecnológicas atualmente em funcionamento.

O principal desafio regulatório brasileiro talvez não resida mais na ausência absoluta de normas. As primeiras respostas institucionais já começaram a surgir. O problema consiste, antes, na distância existente entre essas iniciativas e os riscos concretos já evidenciados pela experiência empírica. A regulação avança, mas continua acompanhando a tecnologia em vez de orientá-la.

4. RECONHECIMENTO FACIAL E A AUTOMAÇÃO DO RACISMO NO DISTRITO FEDERAL

A fundação de Brasília, em 21 de abril de 1960, foi apresentada ao imaginário nacional como a materialização de um projeto de modernidade marcado pela promessa de racionalidade, integração e igualdade espacial. Posteriormente reconhecida como Patrimônio Cultural da Humanidade pela UNESCO, a capital federal passou a representar não apenas a construção de uma nova cidade, mas a projeção de um ideal civilizatório voltado para o futuro. O traçado concebido por Lúcio Costa e a arquitetura monumental de Oscar Niemeyer expressavam a expectativa de uma cidade planejada, organizada e supostamente livre das desigualdades e desordens associadas aos grandes centros urbanos. O projeto urbanístico original, vencedor do concurso de 1957, não previa favelas, periferias ou hierarquias socioespaciais. Idealizava uma cidade estruturada em superquadras funcionalmente integradas e servidas por equipamentos públicos distribuídos de forma homogênea (Holanda, 2017).

A cidade efetivamente construída, contudo, desenvolveu-se sob dinâmica profundamente distinta daquela concebida no plano urbanístico original. A construção da capital mobilizou grande contingente de trabalhadores migrantes, majoritariamente negros e oriundos da região Nordeste, responsáveis por erguer materialmente a nova capital. Os chamados "candangos", termo posteriormente ressignificado pela historiografia, foram inicialmente instalados em acampamentos provisórios próximos às obras. À medida que a construção avançava, entretanto, esses trabalhadores passaram a ser progressivamente removidos para núcleos habitacionais cada vez mais distantes do centro político e administrativo.

O processo foi acompanhado pela criação da denominada "faixa sanitária", estabelecida pela Novacap ao redor do Plano Piloto. Apresentada oficialmente como mecanismo de proteção ambiental e controle da expansão urbana, a medida desempenhou papel central na política de remoção de favelas e na transferência da população trabalhadora para cidades-satélites, contribuindo para a consolidação da segregação socioespacial que marcaria a formação de Brasília (Derntl, 2025).

Mais do que reorganização territorial, o processo consolidou o padrão de distribuição espacial cujos efeitos permanecem perceptíveis na estrutura contemporânea do Distrito Federal. Formou-se a dinâmica urbana marcada pela concentração de infraestrutura, serviços públicos e oportunidades em determinadas áreas centrais, paralelamente à constituição de regiões

periféricas caracterizadas por maiores índices de vulnerabilidade social e significativa presença de população negra.

Essa dimensão histórica ultrapassa interesse meramente urbanístico. Sua relevância decorre do fato de que tecnologias contemporâneas de reconhecimento facial e policiamento preditivo não operam em territórios neutros. Sistemas algorítmicos aprendem a partir de registros produzidos em espaços historicamente organizados por desigualdades raciais, econômicas e territoriais. No Distrito Federal, a segregação urbana não constitui apenas elemento periférico da formação da cidade. Ela produziu padrões específicos de circulação, incidência policial, distribuição de recursos estatais e concentração espacial do controle.

Quando tecnologias preditivas passam a utilizar registros produzidos nesse contexto, o problema não reside apenas na continuidade de desigualdades historicamente construídas. Há também o risco de que essas assimetrias sejam convertidas em padrões estatísticos aparentemente objetivos, conferindo legitimidade técnica a práticas discriminatórias já existentes.

Os dados demográficos apresentados pelo IBGE (2022) reforçam a permanência dessas dinâmicas históricas. O Distrito Federal possui população majoritariamente negra, sendo aproximadamente 57,8% composta por pessoas autodeclaradas pretas e pardas, enquanto cerca de 42% se autodeclaram brancas, conforme levantamento realizado no censo demográfico de 2022 (IBGE, 2022). Entretanto, a distribuição espacial desses grupos permanece profundamente desigual.

Regiões de maior renda, como Plano Piloto, Lago Sul, Lago Norte e Sudoeste, concentram parcelas mais expressivas da população branca. Segundo o estudo apresentado pela pela Diretoria de Estudos e Políticas Sociais (DIPOS) do Instituto de Pesquisa e Estatística do Distrito Federal (IPEDF Codeplan) o Lago Sul lidera esse perfil, possuindo apenas 21,8% de moradores autodeclarados negros, seguido por Sudoeste/Octogonal, Lago Norte e Plano Piloto, todos com mais de 60% de população branca (IPEDF CODEPLAN, 2024). O padrão se inverte nas regiões administrativas periféricas, classificadas nas faixas de menor renda. O estudo mostra que a população negra é amplamente majoritária na Região Administrativa de Arapoanga (75,4%), Fercal (72,4%), Planaltina (71,2%), São Sebastião (70%).

Essas desigualdades não permanecem restritas à distribuição da população no território. Elas também influenciam a forma como determinadas regiões passam a ser percebidas pelas instituições responsáveis pela segurança pública. Nesse contexto, Ceilândia

assume especial relevância analítica. Além de concentrar a maior população do Distrito Federal, a região reúne características que a tornam exemplar das dinâmicas discutidas até aqui: origem vinculada às políticas de remoção, predominância de população negra e recorrente associação institucional a problemas de segurança pública. Atualmente trata-se da maior Região Administrativa do Distrito Federal, abriga o conjunto Sol Nascente/Pôr do Sol, frequentemente descrito por agentes estatais e veículos de comunicação como espaço associado à criminalidade e à vulnerabilidade social. Mais do que simples caracterização territorial, essa representação contribui para compreender a distribuição contemporânea de práticas de vigilância e policiamento.

O critério oficialmente adotado pela Secretaria de Segurança Pública do Distrito Federal para a instalação de câmeras de videomonitoramento consiste na identificação de áreas consideradas de maior incidência criminal, definidas a partir de levantamentos que mapeiam locais, horários e padrões de ocorrência delitiva (SSP-DF, 2025). Em uma primeira leitura, o parâmetro parece estritamente técnico. Contudo, sob perspectiva criminológica crítica, sua aparente neutralidade merece problematização.

Os dados utilizados para definir áreas prioritárias de vigilância não surgem em contexto historicamente desprovido de seletividades. São registros produzidos ao longo de décadas de policiamento ostensivo concentrado sobre determinados territórios urbanos. A incidência criminal atribuída a regiões como Ceilândia não corresponde exclusivamente a fenômeno espontâneo ou natural. Em alguma medida, ela também reflete a concentração histórica de investimentos em práticas de controle e monitoramento sobre determinados espaços em detrimento de outros. Quando algoritmos operam sobre esses registros como se representassem retratos objetivos da realidade social, há o risco de transformar desigualdades historicamente produzidas em parâmetros aparentemente neutros de gestão tecnológica (O'Neil, 2020; Noble, 2018).

Essa dinâmica circular, analisada no Capítulo 1.3 a partir da categoria do ciclo de retroalimentação (*feedback loop*) do policiamento preditivo, encontra terreno fértil em contextos marcados por forte desigualdade socioespacial. Quando determinados territórios são historicamente submetidos a maior intensidade de vigilância e policiamento, os registros produzidos por essa atuação tendem a reforçar sua própria classificação como áreas prioritárias para futuras intervenções estatais. No Distrito Federal, operações permanentes da PMDF desenvolvidas em regiões como Ceilândia, Sol Nascente, Paranoá, São Sebastião e Brazlândia

ilustram como a concentração territorial do controle pode influenciar continuamente a produção dos dados que orientam novas estratégias de segurança pública.

Os efeitos dessa dinâmica não se manifestam apenas na distribuição espacial das ações policiais. Eles também influenciam a construção social da suspeição. Relatos documentados e levantamentos locais indicam que moradores de regiões periféricas frequentemente associam suas interações com os aparatos de segurança a formas diferenciadas de vigilância e controle (MPDFT, 2026). Nesse contexto, a suspeição deixa de decorrer exclusivamente de comportamentos específicos e passa a ser influenciada, ainda que de forma implícita, pelo próprio território de pertencimento.

É precisamente sobre esse espaço historicamente estratificado, seletivamente policiado e socialmente estigmatizado que sistemas de reconhecimento facial começam a ser incorporados à política de segurança pública do Distrito Federal. A conexão com o policiamento preditivo analisado anteriormente revela-se direta. Quando tecnologias biométricas passam a ser implementadas em áreas previamente definidas como prioritárias a partir de registros produzidos por décadas de persecução penal seletiva, a tecnologia não necessariamente rompe com os vieses do policiamento tradicional.

4.1. A Implementação do Reconhecimento Facial em Brasília

Sob o aspecto formal, o Distrito Federal ocupa posição relativamente singular no cenário nacional. Diferentemente da maior parte das unidades federativas brasileiras, a regulamentação local do reconhecimento facial precedeu a implantação efetiva da tecnologia em larga escala. A Lei Distrital nº 6.712, sancionada em 11 de novembro de 2020 pelo então governador Ibaneis Rocha, constituiu o primeiro instrumento normativo local voltado especificamente à disciplina do uso da Tecnologia de Reconhecimento Facial (TRF) pelos órgãos de segurança pública distritais.

A iniciativa possui relevância própria porque não se limitou a autorizar a utilização da ferramenta. A norma procurou definir juridicamente o que se entende por tecnologia de reconhecimento facial e enfrentar alguns dos riscos associados à sua utilização. Entre eles, merece destaque a preocupação com a denominada "vigilância contínua", conceituada em seu artigo 2º, § II:

> Art. 2º Para os efeitos desta Lei, considera-se:
> (...)
> II – vigilância contínua: a utilização de TRF para envolver-se em um esforço contínuo de rastreamento dos movimentos físicos de um indivíduo identificado em um ou mais

> locais públicos onde esses movimentos ocorrem, durante um período de tempo superior a 72 horas, seja em tempo real, seja por meio da aplicação dessa tecnologia para registros históricos (Distrito Federal, 2020).

Em vez de concentrar-se exclusivamente na coleta de dados faciais, a lei buscou enfrentar também um dos aspectos mais intrusivos da vigilância biométrica: a possibilidade de acompanhar continuamente os deslocamentos de indivíduos em espaços públicos. O problema não reside apenas na identificação de uma pessoa em determinado momento, mas na capacidade de transformar sua rotina, seus percursos e seus hábitos de circulação em informações permanentemente monitoradas pelo Estado. Não por acaso, após definir a vigilância contínua, no artigo 3º o legislador optou por vedá-la expressamente em qualquer hipótese (Distrito Federal, 2020).

A lei também condicionou o uso da tecnologia à existência de sinalização ostensiva nos locais monitorados, determinou que toda identificação positiva fosse submetida à revisão de um agente público antes da adoção de qualquer medida, visando impedir que medidas potencialmente restritivas de direitos fossem adotadas exclusivamente com base na resposta fornecida por um algoritmo. A previsão constitui salvaguarda relevante, mas seus efeitos práticos não devem ser superestimados.

A experiência brasileira, a exemplo dos casos documentados em São Paulo e Bahia, demonstram que a presença de um agente humano no processo decisório não elimina, por si só, os riscos de erro. Em diversos episódios envolvendo reconhecimento facial, abordagens indevidas ocorreram mesmo após validação prévia realizada por operadores do sistema, o que sugere que a revisão humana pode, em determinadas circunstâncias, funcionar mais como etapa de confirmação do alerta algorítmico do que como mecanismo efetivo de controle de sua confiabilidade.

Por fim, reconheceu expressamente a natureza sensível dos dados biométricos coletados, submetendo seu tratamento às disposições da Lei Geral de Proteção de Dados. Além disso, estabeleceu prazo máximo de cinco anos para armazenamento dessas informações e autorizou seu compartilhamento com órgãos integrantes do Sistema Único de Segurança Pública.

Apesar do pioneirismo da iniciativa, a existência de disciplina normativa prévia não elimina preocupações relevantes acerca das salvaguardas efetivamente incorporadas ao modelo adotado. A própria estrutura da lei revela que, embora o legislador tenha buscado enfrentar questões relacionadas à transparência, à revisão humana das decisões automatizadas e à

proteção de dados biométricos, temas centrais para a governança algorítmica contemporânea permaneceram sem regulamentação específica.

Em nota técnica publicada em 2021, o Laboratório de Políticas Públicas e Internet (LAPIN) apontou que a lei permaneceu silenciosa sobre aspectos centrais da governança algorítmica, como a exigência de Relatório de Impacto à Proteção de Dados, a realização de auditorias independentes e a definição de critérios mais precisos para o compartilhamento de informações biométricas entre órgãos públicos. A observação evidencia uma limitação recorrente das iniciativas regulatórias voltadas à inteligência artificial: embora frequentemente estabeleçam regras para o uso da tecnologia, nem sempre criam mecanismos adequados para fiscalizar seu funcionamento (LAPIN, 2021).

As preocupações apontadas pelo LAPIN ganhariam ainda mais relevância nos anos seguintes. O episódio envolvendo o Sistema Córtex demonstrou, em escala nacional, os riscos associados à centralização massiva de dados pessoais, à opacidade institucional e à fragilidade dos mecanismos de supervisão sobre sistemas integrados de vigilância. Embora a experiência distrital possuísse disciplina normativa própria, parte dessas preocupações permanecia igualmente presente.

A regulamentação distrital também não surgiu em um contexto de ausência tecnológica. Meses antes da promulgação da Lei nº 6.712/2020, a Secretaria de Segurança Pública já havia realizado experiências piloto com reconhecimento facial durante as festividades do Carnaval de Brasília. As imagens captadas em áreas de grande circulação eram confrontadas com bancos de dados de mandados de prisão em aberto. O dado é relevante porque demonstra que a construção do modelo distrital ocorreu simultaneamente em dois planos: de um lado, a elaboração de um marco regulatório pioneiro; de outro, a experimentação prática de ferramentas biométricas em eventos de massa.

A análise da implementação do reconhecimento facial no Distrito Federal exige, contudo, que se ultrapasse o plano estritamente normativo. Isso porque, paralelamente à aprovação da Lei nº 6.712, consolidava-se uma infraestrutura de vigilância muito mais ampla, responsável por sustentar materialmente a expansão dessas tecnologias no espaço urbano.

A principal estrutura desse sistema é o Programa de Videomonitoramento Urbano (PVU), administrado pela Secretaria de Segurança Pública desde 2013. Com investimentos superiores a setenta milhões de reais, o programa opera a partir do Centro Integrado de Operações de Brasília (CIOB), responsável pela centralização e distribuição, em tempo real,

das imagens captadas pela rede de monitoramento (Miranda; Umbelino, 2025). O sistema conecta dez Centrais de Monitoramento Remoto instaladas em unidades da Polícia Militar e integra informações provenientes de dezenas de instituições públicas.

Segundo a própria Secretaria de Segurança Pública, a finalidade do programa consiste em ampliar a capacidade de resposta estatal diante de situações consideradas relevantes para a segurança pública. Em manifestações institucionais da Secretaria de Segurança Pública, o Programa de Videomonitoramento Urbano foi descrito como instrumento destinado a multiplicar o olhar das forças de segurança em todo o Distrito Federal (Distrito Federal, 2022). A expressão merece atenção porque evidencia que a finalidade atribuída ao sistema não se restringe ao registro de imagens ou ao apoio pontual a investigações. Trata-se da ampliação da capacidade estatal de vigilância sobre o espaço urbano por meio da incorporação permanente de dispositivos tecnológicos ao cotidiano das atividades de segurança pública.

A expansão dessa infraestrutura tecnológica não ocorreu de forma isolada. Ela integra o movimento mais amplo de modernização e integração das políticas de segurança pública distritais, materializado em iniciativas como o Programa DF Mais Seguro – Segurança Integral, conhecido como Programa 360°. Estruturado a partir da articulação entre videomonitoramento, análise de dados, inteligência policial e integração institucional, o programa evidencia a centralidade assumida pelas tecnologias de informação na formulação contemporânea das estratégias de segurança pública do Distrito Federal. Embora não tenha sido concebido especificamente para disciplinar o uso do reconhecimento facial, o Programa 360° contribui para consolidar o ambiente tecnológico e institucional no qual ferramentas biométricas passam a ser progressivamente incorporadas às atividades de monitoramento e investigação.

Esse processo de integração ganhou novo impulso em 2026 com o lançamento da Plataforma DF 360, concebida pela Secretaria de Segurança Pública como ambiente unificado de monitoramento e inteligência. A plataforma passou a concentrar imagens provenientes da rede de videomonitoramento distrital e a possibilitar seu cruzamento com diferentes bases de dados utilizadas pelos órgãos de segurança pública. Mais do que um novo sistema informacional, a iniciativa representa a consolidação de uma estrutura capaz de centralizar, correlacionar e processar informações em larga escala, ampliando significativamente a capacidade estatal de vigilância e monitoramento do espaço urbano. A plataforma também passou a operar de forma integrada a bases nacionais de segurança pública, ampliando a capacidade de cruzamento automatizado entre imagens captadas pela rede de monitoramento e registros mantidos por diferentes órgãos estatais.

Entre 2023 e 2024, novas câmeras foram instaladas em regiões como Varjão, Paranoá, Lago Sul, Lago Norte, Vicente Pires e Arniqueira. Em janeiro de 2025, o Governo do Distrito Federal anunciou a instalação de novos equipamentos de alta resolução no Sol Nascente/Pôr do Sol, preparados para futura integração com tecnologias de reconhecimento facial.

O dado merece atenção porque a expansão não ocorre em território socialmente neutro. Como visto no tópico anterior, regiões como Ceilândia e Sol Nascente concentram significativa população negra e ocupam posição central nas políticas de segurança pública desenvolvidas no Distrito Federal. São também espaços historicamente marcados por maior presença policial e por recorrente classificação institucional como áreas prioritárias para ações de controle e monitoramento.

O critério oficialmente adotado para instalação das câmeras consiste na identificação de áreas consideradas de maior incidência criminal. Em princípio, trata-se de parâmetro técnico. Entretanto, os dados utilizados para definir essas prioridades não são produzidos em contexto desprovido de seletividades históricas. Eles resultam de décadas de atuação policial concentrada sobre determinados territórios, o que exige cautela quando são utilizados como fundamento para orientar novas camadas de vigilância tecnológica.

A questão torna-se ainda mais relevante quando observada à luz da dinâmica descrita pela literatura como ciclo de retroalimentação do policiamento preditivo. Territórios submetidos a maior intensidade de controle tendem a produzir mais registros; esses registros passam a justificar novas intervenções; e as novas intervenções reforçam a classificação inicial daqueles espaços como áreas prioritárias de vigilância. Nesse cenário, a tecnologia não necessariamente rompe com padrões históricos de seletividade. Em determinadas circunstâncias, pode contribuir para sua reprodução sob aparência de neutralidade técnica.

Paralelamente à expansão da infraestrutura de monitoramento, a Polícia Civil do Distrito Federal também passou a investir no desenvolvimento interno de ferramentas baseadas em inteligência artificial. A iniciativa amplia a autonomia tecnológica da instituição, mas também reforça preocupações relacionadas à transparência e ao controle democrático. Quando sistemas são desenvolvidos internamente e seus critérios de funcionamento permanecem inacessíveis ao escrutínio externo, torna-se mais difícil avaliar seus índices de erro, seus parâmetros operacionais e seus potenciais impactos sobre direitos fundamentais.

A experiência do Distrito Federal evidencia, assim, uma tensão que atravessa boa parte do debate contemporâneo sobre reconhecimento facial. De um lado, observa-se a tentativa de

construção de salvaguardas jurídicas destinadas a limitar alguns dos riscos associados à tecnologia. De outro, verifica-se a expansão contínua da infraestrutura de vigilância em territórios historicamente marcados pela desigualdade racial, pela segregação urbana e pela concentração do controle estatal.

Nesse contexto, a questão não se restringe à existência ou não de uma lei específica. Ela envolve compreender onde essas tecnologias são implementadas, sobre quais populações incidem com maior intensidade e quais mecanismos efetivamente existem para fiscalizar seu funcionamento. O caso do Distrito Federal revela que a existência de uma regulação específica não elimina, por si só, os riscos associados ao reconhecimento facial. Embora a Lei nº 6.712/2020 tenha antecipado preocupações que somente anos depois passariam a ocupar o centro do debate nacional, a expansão da infraestrutura de vigilância ocorreu em contexto marcado por desigualdades territoriais historicamente consolidadas.

Nesse cenário, a discussão deixa de se limitar às capacidades técnicas da ferramenta e passa a envolver a forma como tecnologias biométricas são incorporadas a estruturas de controle historicamente marcadas por seletividades raciais e espaciais. A questão central deixa de ser apenas o que a tecnologia é capaz de fazer e passa a ser sobre quem é mais intensamente vigiado por ela, em quais territórios e sob quais mecanismos de controle democrático.

4.2. O Choque com o Processo Penal e a Conclusão do Estudo de Caso

A tensão entre o reconhecimento facial como instrumento de segurança pública e os princípios fundamentais do processo penal brasileiro não se limita ao plano teórico nem constitui preocupação projetada para um futuro distante. Trata-se de uma contradição já produtora de consequências concretas, documentadas em casos que alcançaram os tribunais superiores. Em termos processuais, o problema pode ser sintetizado na necessidade de definir quais limites jurídicos devem disciplinar a utilização de alertas biométricos produzidos por sistemas algorítmicos, especialmente quando deles decorrem abordagens, prisões ou elementos utilizados para sustentar uma persecução penal.

O ponto de partida para essa discussão encontra-se na jurisprudência consolidada do Superior Tribunal de Justiça acerca do reconhecimento pessoal. O paradigma estabelecido pelo HC 598.886, julgado pela Sexta Turma, fixou a exigência de observância estrita do artigo 226 do Código de Processo Penal. O reconhecimento deve ser precedido por descrição pormenorizada do suspeito pela vítima ou testemunha e realizado mediante alinhamento com outros indivíduos de características semelhantes. A inobservância desses requisitos deixou de

ser compreendida como mera irregularidade procedimental e passou a ser tratada como vício apto a comprometer a validade da prova.

A Resolução CNJ nº 484/2022 avançou nessa direção ao impor aos magistrados a necessidade de uma filtragem epistêmica prévia antes da convalidação de abordagens ou prisões decorrentes de identificação visual, reconhecendo a insuficiência do reconhecimento fotográfico isolado para justificar restrições à liberdade. Esses parâmetros, contudo, foram construídos a partir de hipóteses tradicionais de reconhecimento humano, em que uma vítima ou testemunha identifica determinado indivíduo. O reconhecimento facial algorítmico desloca a questão para um cenário distinto, em que a identificação decorre de sistemas computacionais que processam imagens em tempo real e realizam cruzamentos automáticos com bancos de dados.

Sob a ótica das garantias constitucionais do processo penal, essa transposição normativa parece revelar insuficiências relevantes. O alerta produzido pelo algoritmo não constitui prova em sentido próprio, mas elemento indiciário que demanda validação humana qualificada antes da adoção de qualquer medida coercitiva. Entretanto, a operacionalização prática dos sistemas, inclusive no Distrito Federal, cujo programa DF 360º emite alertas automáticos acompanhados de dados de localização e acionamento de equipes em campo, sugere uma dinâmica em que a velocidade da automação tende a reduzir o espaço destinado à revisão humana efetiva.

O problema assume contornos ainda mais delicados diante da incidência de falsos positivos. Se parte das abordagens decorre de erros reconhecidos pelo próprio aparato policial, cada falha não representa mero problema estatístico, mas intervenção estatal sobre uma pessoa inocente. À medida que a infraestrutura de vigilância se expande, aumenta não apenas o número potencial de identificações realizadas, mas também a escala dos erros produzidos pelo sistema e o universo de pessoas expostas a intervenções estatais indevidas.

Nesse contexto, a defesa enfrenta uma assimetria epistêmica particularmente grave. Não possui acesso ao código-fonte do sistema, desconhece os critérios empregados para a definição dos níveis de compatibilidade biométrica, não consegue verificar a integridade das bases de dados consultadas e tampouco dispõe de mecanismos para aferir se a captura da imagem ocorreu em condições tecnicamente adequadas. A opacidade algorítmica produz, assim, obstáculo concreto ao exercício do contraditório e da ampla defesa, comprometendo a própria paridade de armas que estrutura o devido processo legal.

O lançamento da Plataforma DF 360 pelo Governo do Distrito Federal em 2026 introduz questão jurídica adicional que merece exame específico. Como desenvolvido anteriormente, a Portaria MJSP nº 961/2025 vedou a utilização, por órgãos vinculados à União, de sistemas de inteligência artificial destinados à identificação biométrica à distância, em tempo real e em espaços acessíveis ao público, ressalvadas hipóteses excepcionais de autorização judicial prévia ou flagrante delito.

No lançamento do DF 360, a SSP-DF afirmou que o tratamento das informações ocorre com fundamento em finalidade legítima voltada à segurança pública e em conformidade com a legislação de proteção de dados (SSP-DF, 2026). A alegação de conformidade regulatória, contudo, não afasta a necessidade de análise jurídica mais aprofundada. A natureza constitucional singular do Distrito Federal, situado em posição institucional distinta daquela ocupada pelos estados-membros e pelos órgãos federais propriamente ditos, suscita questionamentos relevantes acerca do alcance normativo da Portaria nº 961/2025 sobre suas estruturas administrativas.

A questão ultrapassa discussão meramente formal. Caso se entenda que as limitações impostas pela Portaria não alcançam a estrutura distrital, forma-se cenário no qual sistemas de identificação biométrica em tempo real permanecem operacionalmente disponíveis justamente em um dos entes federativos que mais investem na expansão de infraestrutura de videomonitoramento e integração de dados.

A definição do âmbito de incidência da Portaria pode impactar diretamente a forma de operacionalização do módulo de reconhecimento facial da Plataforma DF 360, especialmente diante da emissão de alertas biométricos em tempo real a partir de câmeras instaladas em espaços públicos.

O ponto assume relevância ainda maior porque o módulo de leitura de placas do DF 360 já opera integrado à Plataforma Córtex do Ministério da Justiça, sistema suspenso em 2025 após o escândalo envolvendo milhões de consultas indevidas (SSP-DF, 2026). A retomada dessa integração, ainda que em módulo tecnicamente distinto daquele envolvido na crise anterior, evidencia a permanência de uma arquitetura interoperável que, pela própria lógica de compartilhamento e integração de dados, permanece sujeita a preocupações semelhantes relacionadas à centralização de dados, à transparência institucional e aos mecanismos de supervisão.

4.2.1 O Reconhecimento Facial diante da LGPD no Contexto da Segurança Pública

A Lei Geral de Proteção de Dados (LGPD) classifica os dados biométricos como dados pessoais sensíveis, nos termos do artigo 5º, inciso II. É nessa categoria que se insere o dado facial tratado por sistemas de reconhecimento facial, especialmente quando utilizado para identificar ou autenticar uma pessoa. Esse enquadramento não é apenas formal. Ao reconhecer a sensibilidade desses dados, a LGPD impõe um regime mais rigoroso ao seu tratamento, justamente porque informações biométricas atingem uma dimensão muito íntima da identidade do indivíduo. Por isso, em regra, exige-se consentimento específico e destacado do titular ou, na ausência dele, a demonstração de fundamento legal expresso em uma das hipóteses taxativas previstas no artigo 11 (Brasil, 2018).

No âmbito da segurança pública, contudo, a LGPD apresenta particularidade relevante. O artigo 4º, inciso III, dispõe que a lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Lida isoladamente, essa exclusão poderia conduzir à interpretação de que os sistemas de reconhecimento facial empregados pelo aparato policial escapariam integralmente ao regime protetivo da legislação, conclusão que produziria consequência paradoxal: justamente nos contextos em que o Estado exerce maior poder sobre a liberdade e o corpo dos indivíduos, as salvaguardas jurídicas seriam mais frágeis.

A interpretação constitucionalmente adequada d dessa hipótese de não incidência, porém, exige leitura restritiva, pois a esta exclusão não pode ser compreendida como autorização ampla para o tratamento de dados pessoais em matéria de segurança pública. O próprio § 1º do artigo 4º prevê que o tratamento de dados realizado para fins de segurança pública, defesa nacional, segurança do Estado ou investigação e repressão de infrações penais deve ser disciplinado por legislação específica. Essa legislação, por sua vez, deve prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, com observância do devido processo legal, dos princípios gerais de proteção de dados e dos direitos do titular.

O problema está justamente na ausência dessa regulamentação. Sem a aprovação de uma disciplina normativa específica para o tratamento de dados em matéria de segurança pública e persecução penal, costuma-se falar, na literatura, em um vazio regulatório ainda significativo, frequentemente associado à chamada “LGPD Penal”. O Projeto de Lei nº 1.515/2022 busca enfrentar essa lacuna, ao propor uma lei específica para o tratamento de dados

pessoais em atividades de segurança do Estado, defesa nacional, segurança pública e investigação ou repressão de infrações penais. Ainda assim, a proposta permanece em tramitação na Câmara dos Deputados, sem consolidação normativa até o momento. Forma-se, assim, um cenário paradoxal, pois justamente os dados mais sensíveis, quando utilizados em uma das áreas de maior poder coercitivo do Estado, seguem submetidos a garantias normativas menos densas e a mecanismos de controle ainda insuficientes.

A ANPD publicou, em junho de 2024, o estudo preliminar “Biometria e Reconhecimento Facial”, integrante da série Radar Tecnológico. No documento, a instituição reconhece a centralidade do tema para a proteção de dados pessoais, especialmente diante dos riscos associados ao tratamento de dados biométricos e ao uso de sistemas de reconhecimento facial em diferentes contextos, inclusive na segurança pública (ANPD, 2024). Esse reconhecimento possui relevância institucional, mas ainda não se traduziu em regulamentação vinculante capaz de disciplinar, de forma específica, a utilização dessas tecnologias em contextos de vigilância estatal e segurança pública. A atuação da ANPD, nesse ponto, evidencia que o tema entrou na agenda regulatória, mas também revela que a proteção normativa permanece em fase de construção.

No Distrito Federal, essa lacuna produz efeitos concretos. A Plataforma DF 360 parece operar em uma zona regulatória ainda indefinida. De um lado, incorpora câmeras privadas e realiza tratamento de dados que pode se aproximar do regime geral de proteção de dados pessoais. De outro, quando utilizada para fins de segurança pública, tende a ser enquadrada na hipótese de não incidência prevista no artigo 4º da LGPD.

A ausência de critérios normativos claros para delimitar essas fronteiras amplia a insegurança institucional e dificulta o controle democrático sobre o funcionamento da tecnologia. O problema não está apenas na existência da ferramenta, mas na falta de parâmetros públicos capazes de indicar quais dados são coletados, por quanto tempo permanecem armazenados, com quem podem ser compartilhados e quais mecanismos existem para fiscalizar seu uso.

Essa fragilidade se torna ainda mais sensível diante da natureza dos dados biométricos. Diferentemente de senhas, códigos de acesso ou documentos de identificação, o dado facial não pode ser simplesmente substituído em caso de vazamento ou uso indevido. Uma senha pode ser alterada. Um documento pode ser reemitido. O rosto, não. Por isso, o comprometimento de uma informação biométrica não produz apenas um risco temporário, mas uma forma de exposição

potencialmente permanente do indivíduo. Essa irreversibilidade distingue os dados biométricos de quase todas as demais categorias de dados pessoais e torna ainda mais grave a ausência de disciplina específica para seu uso em atividades de segurança pública.

Nesse contexto, a lacuna normativa não representa apenas uma falha legislativa. Ela se torna um dos principais desafios regulatórios da expansão contemporânea das tecnologias de reconhecimento facial, sobretudo quando essas ferramentas passam a integrar estruturas estatais de vigilância.

4.3 A Plataforma DF 360: Avanço Tecnológico, Vácuo Democrático

A Plataforma DF 360 representa uma etapa mais sofisticada da política de vigilância tecnológica no Distrito Federal. Não se trata apenas da ampliação do número de câmeras instaladas no espaço urbano, mas da consolidação de uma arquitetura integrada de monitoramento, inteligência e circulação de dados entre diferentes órgãos de segurança pública. Apresentada pela Secretaria de Segurança Pública como instrumento voltado à ampliação da capacidade de prevenção e resposta estatal, a plataforma reúne imagens provenientes de equipamentos públicos, órgãos parceiros e câmeras privadas, permitindo análise em tempo real e acesso por forças como Polícia Militar, Polícia Civil e Corpo de Bombeiros (Distrito Federal, 2026).

A relevância jurídica do DF 360 decorre justamente dessa mudança de escala. O videomonitoramento urbano convencional já exige regras claras de finalidade, retenção de imagens, controle de acesso e auditoria. A leitura automatizada de placas e as ferramentas de análise de imagens acrescentam nova camada de processamento algorítmico. O reconhecimento facial, por sua vez, eleva o risco a outro patamar, pois permite a identificação nominal de indivíduos em espaços públicos. A passagem de uma camada para outra não constitui simples atualização tecnológica. Trata-se de mudança qualitativa na capacidade estatal de observar, classificar e intervir sobre a circulação das pessoas.

As lacunas democráticas da plataforma aparecem antes mesmo da análise de seus resultados operacionais. A expansão tecnológica ocorreu em velocidade superior à construção de mecanismos públicos de controle, auditoria e prestação de contas. Embora o DF possua legislação específica sobre reconhecimento facial desde 2020, a Plataforma DF 360 foi lançada sem a divulgação de Relatório de Impacto à Proteção de Dados, sem relatório público de avaliação de vieses e sem dados oficiais acessíveis sobre falsos positivos. Esse déficit é especialmente sensível porque o Laboratório de Políticas Públicas e Internet já havia advertido,

desde 2021, que a implementação de reconhecimento facial na segurança pública deveria ser acompanhada por medidas de transparência, auditoria, segurança da informação e relatórios periódicos sobre uso e resultados da tecnologia (LAPIN, 2021).

A primeira fragilidade, portanto, diz respeito à ausência de avaliação pública prévia dos impactos da plataforma. Ainda que a Lei Distrital nº 6.712/2020 tenha vedado a vigilância contínua, exigido revisão humana e reconhecido a natureza sensível dos dados biométricos, ela não estabeleceu mecanismos suficientes para fiscalizar a forma concreta de funcionamento dos sistemas posteriormente incorporados à política de segurança pública. A existência de uma lei específica, nesse contexto, não elimina o problema. Ela oferece um ponto de partida normativo, mas não substitui a necessidade de auditoria independente, transparência operacional e controle público sobre os critérios de funcionamento da tecnologia.

A segunda fragilidade diz respeito ao próprio mapa da vigilância. O Decreto nº 47.863/2025, ao reorganizar o Programa DF Segurança Integral, passou a admitir a definição de Áreas de Segurança Prioritária a partir de indicadores de segurança pública e outros dados relacionados (Distrito Federal, 2025). Em uma primeira leitura, o critério parece técnico. O problema é que tais indicadores não são produzidos em território neutro. Eles resultam de décadas de atuação policial concentrada sobre determinadas regiões, especialmente áreas periféricas historicamente associadas à vulnerabilidade social e à criminalidade.

Nesse sentido, a definição de áreas prioritárias para monitoramento precisa ser lida à luz da segregação socioespacial do Distrito Federal. Territórios como Ceilândia e Sol Nascente/Pôr do Sol, já marcados por maior presença policial, concentração de população negra e recorrente classificação institucional como áreas de risco, tendem a se tornar também espaços preferenciais para a expansão tecnológica. O dado apresentado como técnico pode, assim, funcionar como mecanismo de naturalização de desigualdades historicamente produzidas. Regiões mais policiadas produzem mais registros; esses registros justificam novas camadas de vigilância; e a vigilância reforça a classificação inicial desses espaços como prioritários. Essa é precisamente a dinâmica de retroalimentação que aproxima o DF 360 das preocupações discutidas no campo do policiamento preditivo.

A terceira fragilidade emerge da integração de câmeras privadas à estrutura pública de monitoramento. A Portaria SSP nº 19, de 23 de fevereiro de 2026, regulamentou o sistema de integração de câmeras do DF 360, permitindo o aproveitamento de imagens captadas por equipamentos já existentes e direcionados a áreas públicas ou de acesso comum. A norma

admite a participação de condomínios, estabelecimentos comerciais, universidades, agências bancárias e entidades da sociedade civil organizada, mediante formalização de termo de cessão de imagem (Distrito Federal, 2026).

A incorporação dessa infraestrutura privada altera significativamente a natureza da vigilância pública. O Estado deixa de depender apenas de câmeras instaladas diretamente pelo poder público e passa a ampliar sua capacidade de monitoramento por meio de equipamentos mantidos por particulares. Em termos práticos, fachadas de condomínios, estabelecimentos comerciais e instituições privadas podem se converter em pontos de alimentação de uma plataforma pública de segurança. O alcance territorial da vigilância estatal se expande, mas essa ampliação ocorre por meio de uma rede difusa, menos visível e de mais difícil controle social.

É verdade que a Portaria SSP nº 19/2026 prevê obrigações aos participantes, entre elas a instalação de placa padronizada informando que o local possui sistema de videomonitoramento integrado, além de medidas de segurança da informação e retenção mínima das imagens por sete dias, com possibilidade de preservação por até sessenta dias em caso de solicitação da SSP-DF (Distrito Federal, 2026). Ainda assim, essas previsões não resolvem integralmente o problema democrático. A existência de placa indicativa não esclarece, por si só, quais dados são tratados, por quais sistemas, com quais finalidades, por quanto tempo, por quais órgãos e com quais possibilidades de contestação pelo cidadão monitorado.

O problema, portanto, não está apenas na captação da imagem, mas no fluxo posterior de tratamento. Uma câmera privada pode captar a imagem de uma pessoa em área pública ou de acesso comum, transmitir esse conteúdo à estrutura da SSP-DF e permitir seu uso em atividades de monitoramento, investigação ou inteligência. A fronteira entre vigilância privada e vigilância estatal torna-se menos nítida. Também se tornam mais complexas as perguntas sobre quem controla os dados, quem responde por eventual uso indevido, quais registros de acesso são mantidos e quais mecanismos permitem ao cidadão saber se sua imagem foi incorporada ao sistema.

A quarta fragilidade diz respeito à interoperabilidade com outras bases de dados. O DF 360 foi apresentado como plataforma de integração tecnológica, com ferramentas de reconhecimento facial, leitura de placas, drones e modernização dos sistemas de atendimento 190 e 193 (Distrito Federal, 2026). No caso da leitura automatizada de placas, a integração com bases nacionais, como a Plataforma Córtex, reintroduz preocupação já examinada neste trabalho. O problema não está apenas na consulta a bancos de dados externos, mas na

centralização progressiva de informações sensíveis em estruturas interoperáveis, cujo controle público permanece limitado.

A experiência recente envolvendo o Córtex demonstrou que sistemas integrados de vigilância são especialmente vulneráveis a desvios de finalidade, acessos indevidos e dificuldades de responsabilização. Ainda que a integração do DF 360 ocorra em módulo tecnicamente distinto, a lógica institucional permanece semelhante: diferentes fluxos de dados passam a ser processados em uma arquitetura comum, acessível por múltiplos órgãos e dependente de controles internos cuja transparência pública é reduzida. A interoperabilidade amplia a eficiência estatal, mas também amplia a escala dos riscos.

A quinta fragilidade envolve a ausência de dados públicos sobre desempenho. Os anúncios institucionais tendem a enfatizar ganhos de eficiência, ampliação da capacidade de resposta e modernização das forças de segurança. Contudo, não há divulgação equivalente sobre falsos positivos, erros de correspondência, critérios de acurácia, auditorias independentes ou avaliação de impacto racial. Essa assimetria informacional compromete o controle social da tecnologia. Sem dados sobre erros, não é possível verificar quem foi indevidamente abordado, quantas identificações foram descartadas, quais grupos foram mais expostos a falhas e se os mecanismos de revisão humana funcionam de forma efetiva.

Essa ausência de transparência possui impacto processual direto. Em um sistema de reconhecimento facial, a abordagem policial pode ser iniciada a partir de um alerta produzido por uma máquina cujo funcionamento não é acessível ao cidadão, à defesa ou ao controle externo. Quando os parâmetros técnicos do sistema, os bancos de comparação e os índices de erro permanecem desconhecidos, o contraditório torna-se fragilizado. A defesa não questiona apenas uma fotografia ou um depoimento. Ela precisa enfrentar uma cadeia técnica de produção da suspeita que permanece, em grande parte, opaca.

O estudo de caso do Distrito Federal confirma, em sua especificidade territorial, os principais eixos analíticos desenvolvidos ao longo desta pesquisa. O primeiro deles diz respeito ao risco de reprodução tecnológica do racismo estrutural. A vigilância biométrica não se instala sobre um espaço neutro. Ela incide sobre uma cidade cuja formação foi marcada pela segregação racial do território, pela remoção de trabalhadores para regiões periféricas e pela consolidação de profundas desigualdades socioespaciais. Quando a distribuição das câmeras e dos sistemas de monitoramento se orienta por indicadores criminais produzidos nesse mesmo

contexto, há risco de transformar históricos de policiamento seletivo em fundamento técnico para novas formas de vigilância.

O segundo eixo refere-se à insuficiência regulatória. A Lei Distrital nº 6.712/2020 representou avanço importante ao reconhecer riscos específicos do reconhecimento facial, mas não foi acompanhada por instrumentos robustos de governança algorítmica. A Plataforma DF 360 amplia a escala da vigilância, incorpora câmeras privadas, integra diferentes órgãos e permite processamento em tempo real, sem que mecanismos equivalentes de auditoria, avaliação de impacto e transparência pública tenham sido disponibilizados na mesma proporção. A regulação existe, mas sua capacidade protetiva permanece limitada diante da complexidade da infraestrutura tecnológica que passou a operar.

O terceiro eixo envolve o choque entre reconhecimento facial e garantias fundamentais do processo penal. Quanto mais a segurança pública passa a depender de alertas automatizados, leitura de imagens e cruzamento de bases, maior se torna a necessidade de protocolos claros de validação humana, cadeia de custódia digital e controle judicial sobre a origem da suspeita. Sem isso, o risco é que a fundada suspeita seja progressivamente deslocada de elementos concretos e individualizados para sinais estatísticos produzidos por sistemas pouco auditáveis.

A tecnologia modifica a forma do controle, mas não necessariamente sua lógica. O que antes dependia da discricionariedade do olhar humano passa a operar por meio de percentuais de compatibilidade, cruzamentos automatizados e alertas em tempo real. O problema, portanto, não reside apenas na precisão do algoritmo, mas na estrutura histórica que orienta aquilo que ele aprende, reproduz e projeta sobre o futuro.

A experiência do Distrito Federal revela, assim, que o DF 360 não pode ser analisado apenas como expressão de modernização administrativa. Sua implementação amplia a capacidade estatal de vigilância em uma cidade já marcada por desigualdade racial, segregação urbana e concentração territorial do controle policial. A questão central deixa de ser apenas se a tecnologia funciona. Passa a ser quem ela observa com maior intensidade, quais territórios transforma em prioridade e quais garantias permanecem disponíveis para impedir que históricos de vigilância sejam convertidos em critérios automatizados de suspeição.

5. CONCLUSÃO

Diante do que foi desenvolvido ao longo deste trabalho, percebe-se que o debate não se limita às falhas técnicas dos sistemas de reconhecimento facial ou às insuficiências regulatórias existentes no Brasil. A questão é mais profunda. Ela atravessa toda a pesquisa e impõe ao direito um desafio que ainda não foi enfrentado com a seriedade necessária: em que momento uma tecnologia deixa de ser apenas instrumento estatal e passa a influenciar a própria forma como o Estado enxerga, seleciona e controla determinados indivíduos?

A pergunta se torna ainda mais grave quando decisões sobre suspeição, vigilância ou intervenção estatal passam a ser mediadas por sistemas algorítmicos pouco transparentes. Nesses casos, quem responde pelos erros produzidos pelo sistema? Permanece a reflexão sobre a dificuldade de reparar os danos decorrentes de uma abordagem indevida, do constrangimento público, da restrição injustificada da liberdade ou da inclusão equivocada de uma pessoa em uma lógica de suspeição.

As análises desenvolvidas ao longo deste trabalho permitem concluir, com apoio teórico e empírico, que a incorporação de tecnologias algorítmicas de vigilância no sistema de segurança pública brasileiro não representa uma ruptura com o racismo historicamente presente nesse campo. Ao contrário, revela um processo de reconfiguração. Mecanismos tradicionais de seletividade passam a operar sob uma nova linguagem, marcada por promessas de neutralidade, eficiência e precisão técnica. O resultado é a reprodução de padrões históricos de exclusão em formatos mais sofisticados e, justamente por isso, mais difíceis de identificar e contestar.

A primeira conclusão diz respeito à permanência histórica das formas de controle. Conforme demonstrado ao longo do primeiro capítulo, a vigilância dirigida a corpos negros não surge com a inteligência artificial nem com sistemas biométricos contemporâneos. Seus mecanismos precedem em muito a era digital. O que se altera ao longo do tempo são as ferramentas utilizadas e os discursos mobilizados para legitimar sua existência. Em diferentes períodos históricos, distintas formas de racionalidade foram invocadas para justificar estruturas de controle que, sob configurações diversas, mantiveram a raça como fator relevante de seleção social e penal. A questão racial não esteve ausente desses processos. Ao contrário, foi frequentemente ocultada por discursos que conferiam aparência de neutralidade e legitimidade às práticas de controle vigentes em cada contexto histórico.

Como observa Almeida (2019, p. 28), o racismo pode assumir diferentes formas a partir da ação ou da omissão das instituições, o que evidencia que a neutralidade técnica não

representa ausência de discriminação, mas pode constituir um de seus mecanismos mais eficazes de reprodução. Nesse contexto, a discriminação indireta, caracterizada pela "ausência de intencionalidade explícita de discriminar" (ALMEIDA, 2019, p. 23), manifesta-se quando normas e práticas aparentemente neutras desconsideram desigualdades raciais estruturais e produzem efeitos desproporcionais sobre a população negra.

Para Almeida (2019, p. 30), o racismo institucional designa o modo pelo qual as instituições produzem e reproduzem desvantagens raciais independentemente da intenção de seus agentes, o que torna a omissão regulatória não apenas tolerância ao dano, mas cumplicidade estrutural com ele.

A ausência de medidas destinadas a identificar, regulamentar ou corrigir esses impactos não configura postura neutra. Quando o Estado conhece os riscos de determinada tecnologia e, ainda assim, permite sua expansão sem auditoria independente, sem dados públicos sobre falsos positivos e sem avaliação de impacto racial, a omissão passa a integrar o próprio mecanismo de reprodução das desigualdades. O problema não está apenas no erro eventual do sistema, mas na decisão institucional de operar tecnologias sensíveis sem controles proporcionais aos danos que podem produzir.

É necessário também destinar atenção à forma como as novas tecnologias potencializam e reproduzem a mesma lógica por meio de mecanismos automatizados de retroalimentação. O policiamento preditivo e o reconhecimento facial não criaram a seletividade do sistema penal brasileiro. Eles a recebem como dado inicial e, posteriormente, a reproduzem em escala ampliada. Quando alimentados por registros produzidos por décadas de atuação seletiva das instituições de segurança pública, esses sistemas não identificam padrões naturais de criminalidade. Aprendem padrões históricos de vigilância. O problema torna-se particularmente sensível porque o dado produzido pela atuação estatal retorna ao próprio sistema como elemento de validação. O resultado é um processo circular no qual maior incidência policial gera maior produção estatística, que posteriormente serve de justificativa para novas intervenções. Em vez de revelar o crime, a engrenagem passa a reproduzir institucionalmente critérios de suspeição previamente estabelecidos.

Os casos analisados ao longo desta pesquisa demonstram que identificações equivocadas não podem ser tratadas como desvios estatísticos irrelevantes ou custos toleráveis do desenvolvimento tecnológico. Cada erro possui repercussões concretas sobre pessoas reais. Significa abordagem indevida, constrangimento público, restrição injustificada da liberdade e

aprofundamento de experiências históricas de suspeição. Sob perspectiva processual, o problema assume dimensão ainda mais preocupante.

Na prática, observa-se uma inversão silenciosa da lógica da presunção de inocência. O indivíduo passa a ser tratado como suspeito até conseguir demonstrar que a identificação realizada pelo sistema estava incorreta. Ainda que nenhum diploma normativo tenha autorizado tal deslocamento, sua normalização cotidiana revela tensões incompatíveis com garantias fundamentais do processo penal democrático.

Por fim, ao longo deste trabalho sustentou-se que a insuficiência normativa não pode ser compreendida apenas como atraso legislativo ou falha ocasional. Trata-se de uma condição que produz efeitos concretos. A ausência de mecanismos robustos de transparência, auditabilidade e responsabilização permite a expansão de tecnologias de vigilância sem instrumentos proporcionais de controle institucional. A exclusão da segurança pública de determinados regimes de proteção de dados, a ausência de regulamentação específica e a opacidade contratual existente em diversas experiências analisadas não representam problemas meramente técnicos.

A experiência distrital demonstra que a questão regulatória não pode ser reduzida à existência formal de uma lei. A Lei nº 6.712/2020 representou avanço ao disciplinar o reconhecimento facial antes de sua implementação em larga escala, mas não foi suficiente para acompanhar a complexidade da infraestrutura posteriormente construída. A Plataforma DF 360, com sua integração de câmeras públicas e privadas, processamento automatizado de imagens e conexão entre diferentes bases institucionais, revela que a regulação precisa alcançar não apenas a autorização para uso da tecnologia, mas também sua governança concreta: quem acessa, quem audita, quem responde, quem corrige, quem informa e quem repara.

Revelam escolhas políticas que produzem efeitos seletivos concretos. É precisamente nessas escolhas que a desumanização opera: os parâmetros de "risco" mobilizados por esses sistemas não foram calibrados para medir danos a corpos negros. A vida negra não figura como variável a ser protegida, figura como dado de entrada. Seus impactos recaem, de forma reiterada, sobre grupos historicamente marginalizados não por acaso, mas porque a ausência de proteção a esses grupos nunca foi tratada como problema a ser resolvido.

No estudo específico do Distrito Federal, essas dinâmicas assumem expressão territorial particularmente significativa. O processo histórico de formação urbana de Brasília não pode ser dissociado da produção de espaços marcados por desigualdades raciais e

socioeconômicas. A segregação territorial não permanece como elemento do passado. Ela continua produzindo efeitos concretos sobre a maneira como determinados territórios são percebidos, classificados e transformados em espaços prioritários de intervenção estatal. Nesse contexto, tecnologias de vigilância não produzem novos mapas sociais; operam sobre cartografias que já carregam marcas históricas profundas. O algoritmo não cria essas estruturas. Apenas passa a reproduzi-las em linguagem digital.

O caso do Distrito Federal tornou essa constatação ainda mais evidente. A Plataforma DF 360 não representa apenas a ampliação quantitativa de câmeras no espaço urbano, mas a consolidação de uma arquitetura integrada de vigilância, capaz de articular videomonitoramento, inteligência artificial, leitura automatizada de placas, reconhecimento facial e compartilhamento de dados entre diferentes órgãos de segurança pública. A tecnologia, nesse cenário, deixa de operar como ferramenta isolada e passa a integrar uma estrutura permanente de observação, classificação e resposta estatal. O problema não reside apenas na existência dessa infraestrutura, mas na forma como ela se expande sobre territórios já marcados por desigualdade racial, segregação urbana e maior intensidade de controle policial.

A incorporação de câmeras privadas ao DF 360 aprofunda essa preocupação. Ao permitir que equipamentos de condomínios, estabelecimentos comerciais e entidades privadas passem a alimentar a estrutura pública de monitoramento, o Estado amplia sua capacidade de vigilância sem necessariamente instalar novos equipamentos próprios. A fronteira entre vigilância privada e vigilância estatal torna-se menos nítida. Pessoas que transitam em espaços públicos ou de acesso comum podem ter sua imagem captada por equipamentos particulares e incorporada a fluxos de segurança pública, muitas vezes sem compreender quem controla esses dados, por quanto tempo são armazenados, com quais bases são cruzados e quais mecanismos existem para contestar eventual uso indevido. A expansão da vigilância, portanto, não ocorre apenas pela presença visível do Estado, mas também pela incorporação silenciosa de infraestruturas privadas ao aparato público de controle.

Diante desse cenário, o direito não pode limitar-se à produção de respostas normativas genéricas ou excessivamente otimistas. Regulamentar, por si só, não basta. A primeira exigência consiste em reconhecer que alertas produzidos por sistemas de reconhecimento facial não podem constituir fundamento autônomo suficiente para justificar abordagens policiais, restrições à liberdade ou atos de persecução penal. Essa limitação decorre das próprias garantias constitucionais e processuais já existentes, mas precisa encontrar previsão expressa e vinculante em futuros marcos regulatórios.

Também se mostra indispensável a previsão de mecanismos efetivos de auditabilidade. Sem acesso às bases de treinamento, critérios utilizados, parâmetros técnicos e taxas de erro desagregadas por raça, gênero e território, garantias como contraditório e ampla defesa tornam-se substancialmente enfraquecidas. O exercício efetivo da defesa pressupõe a possibilidade concreta de questionar o funcionamento do sistema utilizado.

Da mesma forma, determinadas aplicações exigem limites mais rigorosos. O debate internacional tem demonstrado crescente preocupação com o uso indiscriminado de sistemas biométricos em espaços públicos, sobretudo diante de riscos relacionados à vigilância massiva e à restrição desproporcional de direitos fundamentais. Algumas utilizações podem exigir não apenas regulamentação, mas limitação expressa ou até proibição.

Por fim, talvez a conclusão mais estrutural seja a necessidade de abandonar a ideia de neutralidade tecnológica como pressuposto. Tecnologias não operam em abstrato. Atuam sobre sujeitos concretos, em territórios concretos e dentro de relações históricas concretas. Ignorar essa dimensão significa reduzir o debate a uma discussão exclusivamente técnica sobre índices de precisão, parâmetros estatísticos ou taxas de erro, deslocando a atenção do verdadeiro problema: as relações de poder que estruturam o funcionamento dessas ferramentas.

O direito, diante desse cenário, encontra-se diante de uma escolha relevante. Pode limitar-se a conferir linguagem jurídica a práticas historicamente seletivas que agora se apresentam em formato automatizado. Ou pode assumir posição crítica e reafirmar que garantias fundamentais não deixam de existir porque uma decisão passou a ser mediada por sistemas tecnológicos.

Ao longo da história, o racismo estrutural demonstrou extraordinária capacidade de adaptação. Atravessou diferentes períodos, reorganizou discursos e incorporou novas formas de legitimação. A tecnologia não interrompe esse processo por si só. Em determinadas condições, pode apenas torná-lo mais eficiente, mais opaco e mais difícil de contestar.

Ao final deste trabalho, a pergunta que permanece não é apenas se o reconhecimento facial funciona, se identifica pessoas procuradas ou se amplia a capacidade operacional do Estado. Essas questões importam, mas não esgotam o problema. A pergunta mais incômoda é outra: quem paga o preço dessa eficiência?

Quando uma tecnologia de vigilância se expande sem transparência, sem auditoria independente, sem dados públicos sobre seus erros e sem mecanismos reais de contestação, a ausência de regulação deixa de ser um simples atraso legislativo. Ela passa a produzir efeitos

concretos. E, como toda omissão estatal em contextos de desigualdade, também beneficia alguém. Beneficia quem contrata sem prestar contas suficientes. Beneficia quem opera sistemas sem revelar seus critérios. Beneficia quem transforma alertas automatizados em suspeição prática, sem explicar como aquele resultado foi produzido. Beneficia, sobretudo, uma estrutura de segurança pública que historicamente se acostumou a vigiar alguns corpos com mais intensidade do que outros.

Por outro lado, essa mesma ausência de regulação não se distribui de forma abstrata. Ela recai sobre pessoas concretas, em territórios concretos, marcados por desigualdades que antecedem a própria tecnologia. São esses sujeitos que suportam o risco do falso positivo, da abordagem indevida, da exposição pública, da restrição injustificada de liberdade e da necessidade de provar que a máquina errou. Nesse cenário, o problema não está apenas no funcionamento técnico do sistema, mas na assimetria entre quem controla a tecnologia e quem é controlado por ela.

Por isso, reconhecer os riscos do reconhecimento facial não significa rejeitar toda inovação tecnológica. Significa recusar a ideia de que eficiência possa substituir legalidade, transparência e devido processo. No campo da segurança pública, nenhuma promessa de modernização pode justificar a transformação de históricos de vigilância seletiva em critérios automatizados de suspeição.

Se o racismo estrutural demonstrou, ao longo da história, enorme capacidade de adaptação, o desafio jurídico contemporâneo é impedir que ele também se atualize por meio da técnica. A tecnologia não é neutra quando opera sobre uma sociedade que nunca foi neutra. E a ausência de regulação, nesse contexto, também não é neutra. Ela escolhe, ainda que pelo silêncio, quais riscos serão tolerados, quais erros serão invisibilizados e quais vidas continuarão sendo tratadas como dados disponíveis ao controle estatal.

REFERÊNCIAS

AGÊNCIA BRASÍLIA. GDF amplia videomonitoramento com instalação de novas câmeras no Sol Nascente/Pôr do Sol. Brasília, DF: Secretaria de Estado de Segurança Pública do Distrito Federal, 9 jan. 2025. Disponível em: https://ssp.df.gov.br/gdf-amplia-videomonitoramento-com-instalacao-de-novas-cameras-no-sol-nascente-por-do-sol. Acesso em: 1 maio 2026.

ALENCAR, Itana. Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por 'racismo algorítmico'; inocente ficou preso por 26 dias. G1, Bahia, 01 set. 2023. Disponível em: https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoes-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-preso-por-26-dias.ghtml. Acesso em: 30 abr. 2026

ALMEIDA, Silvio. Racismo estrutural. Pólen Produção Editorial LTDA, 2019.

ALVES, Caio; SALES, Amanda. 'Preta nojenta' e 'cabelinho duro': adolescente de Brasília sofre ofensa racista em vídeo publicado nas redes sociais. **G1**, Brasília, 30 de set. de 2025. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2025/09/30/adolescente-e-vitima-de-ofensas-racistas-em-video-publicado-por-colega-nas-redes-sociais.ghtml. Acesso em: 06 de Jan. 2026.

ALVES, JAIME AMPARO. Topografias da violência: necropoder e governamentalidade espacial em São Paulo. Revista do Departamento de Geografia (USP) , v. 22, p. 108-134, 2011.

ALVES, JAIME AMPARO. Necropolitica racial: a producao espacial da morte na cidade de Sao Paulo. Revista da Associação Brasileira de Pesquisadores(as) Negros(as) - ABPN , v. 01, p. 89-114, 2010.

ALVES, Luiz Fellipe. **PMDF suspende licitação para compra de câmeras corporais:** a aquisição das câmeras corporais foi aprovada na CLDF em 2021, e o processo licitatório começou em 2023. *Correio Braziliense*, Brasília, DF, 14 maio 2026. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2026/05/7419133-compra-de-cameras-corporais-especialistas-avaliam-eficacia-da-medida.html. Acesso em: 1 maio 2026.

ARAÚJO, Valmir. **Aos 63 anos, Brasília é a cidade mais segregada do mundo, aponta pesquisador:** o historiador Guilherme Lemos destaca práticas que foram usadas para afastar pessoas negras do centro. Brasil de Fato, Brasília, DF, 21 abr. 2023. Disponível em: https://www.brasildefato.com.br. Acesso em: 3 abr. 2026.

BAHIA. Secretaria da Segurança Pública. Bahia apresenta resultado do reconhecimento facial na China. Salvador: SSP-BA, 14 maio 2019. Disponível em: https://www.ba.gov.br/ssp/2019/05/14/bahia-apresenta-resultado-do-reconhecimento-facial-na-china. Acesso em: 1 mai. 2026.

BAHIA. Secretaria de Comunicação Social. Bahia já alcançou mais de 5.300 foragidos da Justiça com a tecnologia de reconhecimento facial. Salvador, 6 maio 2026. Disponível em: https://www.ba.gov.br/comunicacao/noticias/2026-05/381453/pioneira-na-implementacao-da-tecnologia-de-reconhecimento-facial-no-brasil. Acesso em: 31 maio 2026.

BARBOSA OLIVEIRA, C.; DE FREIRAS FAGUNDES, M. C.; VINICIUS SPOLLE, M. Racismo digital e gestão populacional: uma análise sobre câmeras com reconhecimento facial. Mosaico, [S. l.], v. 17, n. 27, p. e1727202546, 2025. DOI: 10.12660/rm.v17n27.2025.92355. Disponível em: https://periodicos.fgv.br/mosaico/article/view/92355. Acesso em: 5 set. 2025.

BARREIRA, Gabriel; COSTA, André C.; SEEHAUSEN, Lucas Von. Governo federal anuncia suspensão de sistema de vigilância após mau uso pela PM do RJ. G1, Rio de Janeiro, 25 de nov. 2025. Disponível em: http://g1.globo.com/rj/rio-de-janeiro/noticia/2025/11/25/governo-federal-anuncia-suspensao-de-sistema-de-vigilancia.ghtml. Acesso em: 24 mar. 2026

BATISTA SPOSATO, K.; CRUZ MOITINHO, V. A bala não erra o alvo: racismo e letalidade policial no Brasil. Boletim IBCCRIM, São Paulo, v. 30, n. 360, p. 13–15, 2024. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1537. Acesso em: 7 set. 2025.

BATISTA, Vera Malaguti. *Introdução crítica à criminologia brasileira*. Rio de Janeiro: Revan, 2011.

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

BICHARA, A. A.; CASCARDO JR., A. G.; PERAZZONI, F. Racismo algorítmico, reforço de preconceitos e uso de IA: perspectivas e desafios para a investigação criminal digital. Boletim IBCCRIM, São Paulo, v. 32, n. 379, p. 23–26, 2024. DOI: 10.5281/zenodo.11175558. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1069. Acesso em: 2 set. 2025.

BORGES, Juliana. **Encarceramento em massa**. São Paulo: Pólen, 2019. (Feminismos Plurais). Disponível em: https://bibliotecadigital.mdh.gov.br/jspui/handle/192/10404. Acesso em: 29 de mar. 2026

BRAGA, Nathália. Erro em reconhecimento facial constrange psicóloga em conferência. Defensoria Pública do Estado do Rio de Janeiro, 12 de jul. de 2024. Disponível em: https://defensoria.rj.def.br/noticia/detalhes/29955-Erro-em-reconhecimento-facial-constrange-psicologa-em-conferencia. Acesso em: 24 de mai. 2026

BRASIL. Agência Nacional de Proteção de Dados. Radar Tecnológico: Biometria e Reconhecimento Facial. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/radar-tecnologico-biometria-anpd-1.pdf. Acesso em: 25 mar. 2026.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 1.515, de 2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/propostas-legislativas/2326300. Acesso em: 10 abr. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 10 abr. 2026.

BRASIL. Ministério da Justiça. Inaugurado centro de controle de segurança pública da Copa no DF. **Ministério da Justiça e Segurança Pública**, Brasília, DF, 4 abr. 2014. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/inaugurado-centro-de-controle-de-seguranca-publica-da-copa-no-df?utm_source=chatgpt.com. Acesso em: 05 jan. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria MJSP nº 961, de 24 de junho de 2025. Estabelece normas para uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. Diário Oficial da União: seção 1, Brasília, DF, edição 120, p. 104, 30 jun. 2025. Disponível em: https://www.in.gov.br/web/dou/-/portaria-mjsp-n-961-de-24-de-junho-de-2025-638661609. Acesso em: 9 fev. 2026.

BRASIL. Prefeitura de São Paulo. Relatório de Transparência do Smart Sampa comprova eficácia do sistema de reconhecimento facial. São Paulo. 2025. Disponível em: https://prefeitura.sp.gov.br/web/seguranca_urbana/w/relat%C3%B3rio-de-transpar%C3%AAncia-do-smart-sampa-comprova-efic%C3%A1cia-do-sistema-de-reconhecimento-facial?utm_source=chatgpt.com Acesso em: 6 Set. 2025

BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF: Senado Federal, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 9 jan. 2026.

BRASIL DE FATO. **Abordagens por reconhecimento facial têm 10% de falsos positivos, diz PM na Alerj**. 3 set. 2024. Rio de Janeiro. Disponível em: https://www.brasildefato.com.br/2024/09/03/abordagens-por-reconhecimento-facial-tem-10-de-falsos-positivos-diz-pm-em-audiencia-na-alerj/. Acesso em: 10 abr. 2026.

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

BRUNO, Fernanda. Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA (CESeC). **Projeto Panóptico: Reconhecimento Facial e Racismo no Brasil**. Rio de Janeiro: CESeC, 2023.

CARVALHO, José Murilo de. **Cidadania no Brasil: o longo caminho**. 3. ed. Rio de Janeiro: Civilização Brasileira, 2002.

CONTINENTINO, Leon. Abordagens por reconhecimento facial têm 10% de falsos positivos, afirma PM em audiência na Alerj. *Assembleia Legislativa do Estado do Rio de Janeiro (Alerj)*, Rio de Janeiro, 2 set. 2024. Disponível em: https://www.alerj.rj.gov.br/Visualizar/Noticia/68952. Acesso em: 31 maio 2026.

CONSEJO PARA LA TRANSPARENCIA. CPLT advierte altos niveles de “falsos positivos” en sistemas de reconocimiento facial tras promoción de dicha tecnología en Las Condes. Chile, 12 de dez. 2019. Disponível em: https://www.consejotransparencia.cl/cplt-advierte-altos-niveles-de-falsos-positivos-en-sistemas-de-reconocimiento-facial-tras-promocion-de-dicha-tecnologia-en-las-condes/. Acesso em: 5 de dez. 2025

DERNTL, Maria Fernanda. Remoção de favelas e planejamento urbano em Brasília das décadas de 1950 a 1970. *Planning Perspectives*, v. 40, n. 3, p. 499-526, 2025. DOI: https://doi.org/10.1080/02665433.2025.2466445

DIETER, Maurício Stegemann. **Política criminal atuarial:** a criminologia do fim da história. 2012. Tese (Doutorado em Direito do Estado) – Faculdade de Direito, Universidade Federal do Paraná, Curitiba, 2012.

DISTRITO FEDERAL. Administração Regional de Ceilândia. História de Ceilândia. Ceilândia, 28 out. 2024. Atualizado em 31 mar. 2026. Disponível em: https://ceilandia.df.gov.br/historia-de-ceilandia. Acesso em: 31 maio 2026.

DISTRITO FEDERAL. Lei nº 6.712, de 10 de novembro de 2020. Dispõe sobre o uso de tecnologia de reconhecimento facial – TRF na segurança pública e dá outras providências. Diário Oficial do Distrito Federal, Brasília, DF, 11 nov. 2020. Disponível em: https://www.sinj.df.gov.br/sinj/Norma/525023c5ea4e4fc284fc1bc810de69c2/Lei_6712_10_11_2020.html. Acesso em: 31 maio 2026.

DISTRITO FEDERAL. Secretaria de Estado de Segurança Pública. 140 novas câmeras de videomonitoramento reforçam segurança no DF. Brasília, DF, 7 dez. 2022. Atualizado em 29 abr. 2026. Disponível em: https://ssp.df.gov.br/140-novas-cameras-de-videomonitoramento-reforcam-seguranca-no-df/?utm_source=chatgpt.com. Acesso em: 31 maio 2026.

DUARTE, Evandro Charles Piza. **Criminologia e racismo**: introdução ao processo de recepção das teorias criminológicas no Brasil. 1998. Dissertação (Mestrado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 1998. Disponível em: http://repositorio.ufsc.br/xmlui/handle/123456789/77655. Acesso em: 12 de jan. 2026.

FALCÃO, Cíntia. Ascensão do tecnoautoritarismo. Intercept Brasil. 20 de set. 2021. Disponível em: https://www.intercept.com.br/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/. Acesso em: 10 de mar. 2026

FANON, Frantz. **Os condenados da terra.** Tradução de Serafim Ferreira. Editora Ulisseia limitada, Lisboa, Pt. 1961.

FLAUZINA, Ana Luiza Pinheiro; FREITAS, Felipe da Silva. Do paradoxo privilégio de ser vítima: terror de Estado e a negação do sofrimento negro no Brasil. Revista Brasileira de Ciências Criminais, vol. 135, ano 25, P. 49-71, São Paulo, ed. RT, set 2017

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

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Raquel Ramalhete. 42. ed. Petrópolis, RJ: Vozes, 2014.

GROSSI, Alexandre Viezzer. A APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA PÚBLICA BRASILEIRA: O CASO DE SÃO PAULO E A ANÁLISE DO PL Nº 2338/2023. Revista Políticas Públicas & Cidades, [S. l.], v. 14, n. 4, p. e2135, 2025. DOI: 10.23900/2359-1552v14n4-72-2025. Disponível em: https://journalppc.com/RPPC/article/view/2135. Acesso em: 7 set. 2025.

HOLANDA, Frederico de. **Brasília:** utopia ou segregação à brasileira? Série especial – O direito à cidade em tempos de crise. *Le Monde Diplomatique Brasil*, 26 abr. 2016. Disponível em: https://diplomatique.org.br/brasilia-utopia-ou-segregacao-a-brasileira/. Acesso em: 1 maio 2026.

HOSANA, Kelly. Vídeo policiamento vai facilitar identificação de procurados. **Secretaria de Ciência, Tecnologia e Inovação da Bahia**, Salvador, 19 dez. 2018. Disponível em: https://www.ba.gov.br/secti/noticia/2024-05/535/video-policiamento-vai-facilitar-identificacao-de-procurados. Acesso em: 1 fev. 2026.

IBARRECHE, Xavier; MARTÍNEZ ELEBI, Carolina; DI LORENZO, Camila. *Reconhecimento facial e tecnologias de vigilância na América Latina: casos, fornecedores e dinâmicas comerciais*. [S.l.]: AlSur, 2025.

INSTITUTO DE DEFESA DO DIREITO DE DEFESA; DATA_LABE. **Por que eu?: como o racismo faz com que as pessoas negras sejam o perfil alvo das abordagens policiais**. 2022.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA (IPEA); FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA (FBSP). **Atlas da violência 2025**. Brasília: Ipea, 2025. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2025/05/atlas-violencia-2025.pdf. Acesso em: 25 fev. 2026

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET (LAPIN). **Nota técnica sobre a Lei Distrital nº 6.712/2020: 10 recomendações para o uso de reconhecimento facial para segurança pública no DF**. Brasília: LAPIN, fev. 2021.

LOPES JR., Aury. **Direito Processual Penal**. 20. ed. São Paulo: Saraiva, 2023.

LUCENA, P. A. C. Viés e Racismo no Policiamento Preditivo: casos estadunidenses e os reflexos de conexão com o Brasil. Revista de Direito e as Novas Tecnologias, São Paulo, v. 7, p. 1-13, abr./jun. 2020.

MBEMBE, Achille. **Crítica da Razão Negra.** Ed. 1ª. Portugal: Antígona, 2014.

MBEMBE, Achille. **Necropolítica: biopoder, soberania, estado de exceção, política da morte**. Tradução de Renata Santini. São Paulo: n-1 edições, 2018.

MELLO, Daniel. São Paulo avança em integração de sistemas de hipervigilância: pesquisador alerta quanto a protocolos com limites para uso de dados. *Agência Brasil*, São Paulo, 27 jan.

2024. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-01/sao-paulo-avanca-em-integracao-de-sistemas-de-hipervigilancia. Acesso em: 31 maio 2026.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA (MJSP). **Portaria nº 961, de 24 de junho de 2025**. Brasília: MJSP, 2025.
MIRANDA, Thaís; UMBELINO, Thaís. GDF amplia videomonitoramento com instalação de novas câmeras no Sol Nascente/Pôr do Sol. *Agência Brasília*, Brasília, DF, 9 jan. 2025. Disponível em: https://www.agenciabrasilia.df.gov.br/w/gdf-amplia-videomonitoramento-com-instalacao-de-novas-cameras-no-sol-nascente-por-do-sol. Acesso em: 31 maio 2026.

MONTEIRO, Pedro Diogo Carvalho. **Reconhecendo faces, enclausurando corpos: terror racial, vigilância racializadora e o uso policial do reconhecimento facial na Bahia**. 2022. 252 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2022.

MONTEIRO, Pedro Diogo Carvalho; SALOMÃO, Elizandra. O Slave Ship como paradigma de análise dos aparatos de vigilância no Genocídio Antinegro pelo Estado Brasileiro. In IV Congresso de Pesquisa de Ciências Criminais, 4º CPCCRIM. Anais do IV Congresso de Pesquisas em Ciências Criminais, de 21 a 23 de outubro de 2020, São Paulo, SP [recurso eletrônico] / Organizado por Dina Alves. – São Paulo: IBCCRIM, 2020. P. 655-679.

MOURA MARTINS, A. T. Racismo estrutural e suas congruências históricas. Boletim IBCCRIM, São Paulo, v. 31, n. 363, p. 13–16, 2024. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1571. Acesso em: 7 set. 2025.

MUNANGA, Kabengele. Uma abordagem conceitual das noções de raça, racismo, identidade e etnia. Programa de Educação sobre o Negro na Sociedade Brasileira, 2004.

NOBLE, Safiya Umoja. *Algorithms of oppression: how search engines reinforce racism*. New York: NYU Press, 2018.

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

NUNES, Pablo; LIMA, Thallita G. L.; CRUZ, Thaís G. **O SERTÃO VAI VIRAR MAR**: Expansão do reconhecimento facial na Bahia. Rio de Janeiro: CESeC. 2023.

NUNES, Pablo; SILVA, Mariah Rafaela; OLIVEIRA, Samuel R. de**. Um Rio de câmeras com olhos seletivos**: uso do reconhecimento facial pela polícia fluminense. Rio de Janeiro: Centro de Estudos de Segurança e Cidadania (CESeC), 2022. Disponível em: https://cesecseguranca.com.br/wp2025/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em: 25 fev. 2026

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, SP: Editora Rua do Sabão, 2020.

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

PAULA, Gáudio Ribeiro de. **Desafios regulatórios da inteligência artificial:** *human rightis by design*. Barueri, SP: Editora Manola, 2025.

PERRY, Walter L. et al. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. Santa Monica, CA: RAND Corporation, 2013. Disponível em: https://www.rand.org/pubs/research_reports/RR233.html. Acesso em 01 de Abr. 2026.

PIRES, Thula. Do ferro quente ao monitoramento eletrônico: controle, desrespeito e expropriação de corpos negros pelo Estado Brasileiro. In: Ana Luiza Pinheiro Flauzina; Felipe da Silva Freitas. (Org.). Discursos negros: legislação penal, política criminal e racismo. 1ed.Brasília: Brado Negro, 2015, v. 1, Versão não paginada

POLÍCIA CIVIL DO DISTRITO FEDERAL (PCDF). PCDF dá salto tecnológico e entrega novas ferramentas de inteligência para o combate à criminalidade. Brasília, DF, 11 abr. 2026. Disponível em: https://www.pcdf.df.gov.br/noticias/15460/pcdf-da-salto-tecnologico-e-entrega-novas-ferramentas-de-inteligencia-para-o-combate-a-criminalidade. Acesso em: 31 maio 2026.

QUIJANO, Aníbal. Colonialidade do poder, eurocentrismo e América Latina. In: LANDER, Edgardo (org.). **A colonialidade do saber: eurocentrismo e ciências sociais**. Buenos Aires: CLACSO, 2005, p. 227-278.

QUIRINO, Flávio. 'Foi racismo': sistema de identificação do DF apaga cabelo de jovem negra. **Brasil de Fato**, Brasília, 24 de jul. de 2025. Disponível em: http://brasildefato.com.br/?s=apaga+cabelo+de+jovem. Acesso em: 6 de jan. 2026

REIS, Dyane Brito. O Racismo na Determinação da Suspeição Policial: A construção social do suspeito. Dissertação de Mestrado, Salvador, FFCH-UFBA, 2001a.

RODRIGUES, Nina. **As raças humanas e a responsabilidade penal no Brazil**. Rio de Janeiro: Waissman Koogan; Guanabara, [193-].

SANTANA, Márcia. Pioneira na implementação do reconhecimento facial no Brasil, Bahia já alcançou mais de 5.300. *Secretaria da Segurança Pública da Bahia*, Salvador, 6 maio 2026. Disponível em: https://www.ba.gov.br/ssp/noticias/2026-05/88440/pioneira-na-implementacao-da-tecnologia-de-reconhecimento-facial-no-brasil. Acesso em: 8 maio 2026.

SÃO PAULO (Município). Secretaria Municipal de Segurança Urbana. Programa Smart Sampa: o maior programa de câmeras de segurança da cidade de São Paulo. São Paulo, 6 abr. 2026. Disponível em: https://prefeitura.sp.gov.br/web/seguranca_urbana/w/smart-sampa-2. Acesso em: 31 maio 2026.

SÃO PAULO (Município). Subprefeitura Sé. Smart Sampa chega a 50 mil câmeras e já supera em 25% o previsto no Programa de Metas. São Paulo, 2 abr. 2026. Disponível em: https://prefeitura.sp.gov.br/web/se/w/smart-sampa-chega-a-50-mil-c%C3%A2meras-e-j%C3%A1-supera-em-25-o-previsto-no-programa-de-metas. Acesso em: 1 maio 2026.

SÃO PAULO (Município). Taxa de reconhecimento facial do Smart Sampa é de 99,5%, sem registro de prisão de inocentes. *Portal da Prefeitura de São Paulo*, São Paulo, 18 jun. 2025. Disponível em: https://prefeitura.sp.gov.br/w/taxa-de-reconhecimento-facial-do-smart-sampa-%C3%A9-de-99-5-sem-registro-de-pris%C3%A3o-de-inocentes. Acesso em: 31 maio 2026.

SARAIVA, Mariana. **Reconhecimento facial é um aliado da segurança pública do DF:** utilização de inteligência artificial e análise de dados transformam o trabalho das forças policiais no DF no combate à criminalidade e colocam ciência e proteção a serviço da população. *Correio Braziliense*, Brasília, DF, 1 jun. 2025. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2025/06/7159781-reconhecimento-facial-e-um-aliado-da-seguranca-publica-do-df.html. Acesso em: 1 maio 2026.

SECRETARIA DE SEGURANÇA PÚBLICA DA BAHIA (SSP-BA). **Relatório de Gestão Tecnológica: Vídeo-Polícia Expansão**. Salvador: SSP-BA, 2025.

SECRETARIA MUNICIPAL DE SEGURANÇA URBANA DE SÃO PAULO (SMSU). **Smart Sampa: Relatório de Transparência e Resultados**. São Paulo: SMSU, 2025.

SENNA, Daniel. Governador assina, na China, acordo para ampliar parceria tecnológica com a empresa Huawei. Secretaria de Desenvolvimento Econômico da Bahia, Salvador, 7 abr. 2023. Disponível em: https://www.ba.gov.br/sde/2023/04/07/governador-assina-na-china-acordo-para-ampliar-parceria-tecnologica-com-a-empresa-huawei. Acesso em: 07 jan. 2026.

SILVA, Fernanda dos Santos Rodrigues; SILVA, Tarcízio (orgs). Inteligência Artificial e Discriminação Racial no Brasil: questões principais e recomendações. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Disponível em: https://irisbh.com.br/publicacoes/inteligencia-artificial-e-discriminacao-racialno-brasil/. Acesso em: 2 set. 2025.

SIMÕES BUENO, I. “Todo camburão tem um pouco de navio negreiro”: colonialidade do poder punitivo e a produção da morte no cárcere. Boletim IBCCRIM, São Paulo, v. 31, n. 363, p. 10–12, 2024. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1570. Acesso em: 7 set. 2025.

SILVA, Tarcizio. Visão Computacional e Vieses Racializados: branquitude como padrão no aprendizado de máquina. II COPENE Nordeste: Epistemologias Negras e Lutas Antirracistas, p. 29-31, 2019.

SILVA, Tarcizio. Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código. COMUNIDADES, ALGORITMOS E ATIVISMOS DIGITAIS, p. 121, 2019.

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

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. TV Globo. 26 de mar. 2026. Disponível em: http://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: 30 de abr. 2026.

SCHWINGEL, Samara. **Distrito Federal terá tecnologia de reconhecimento facial nas ruas:** lei que regulamenta o uso do sistema foi sancionada e publicada no Diário Oficial do DF desta quarta-feira (11/11). Os dados podem ser armazenados por 5 anos, devendo ser eliminados do banco de dados após o prazo. Correio Braziliense, Brasília, DF, 11 nov. 2020. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2020/11/4888042-distrito-federal-tera-tecnologia-de-reconhecimento-facial-nas-ruas.html. Acesso em: 1 maio 2026.

TORRES CESAR, C. Política criminal e punitivismo racial. Boletim IBCCRIM, São Paulo, v. 31, n. 364, p. 4–5, 2024. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1579. Acesso em: 7 set. 2025.

TOURINHO, Helena. Uma breve história das cidades-satélites de Brasília. *Caos Planejado*, 7 abr. 2025. Disponível em: https://caosplanejado.com/uma-breve-historia-das-cidades-satelites-de-brasilia/. Acesso em: 31 maio 2026.

WERMUTH, Maiquel Ângelo Dezordi. Política criminal atuarial: contornos biopolíticos da exclusão penal / Actuarial criminal policy: biopolitical contours of criminal exclusion. Revista Direito e Práxis, [S. l.], v. 8, n. 3, p. 2043–2073, 2017. DOI: 10.12957/dep.2017.22314. Disponível em: https://www.e-publicacoes.uerj.br/revistaceaju/article/view/22314. Acesso em: 01 mai. 2026.