PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
DIREITO

LUCIANO FINOZZI MOLERO JUNIOR

RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA E O RACISMO ESTRUTURAL

Análise Constitucional do Programa Smart Sampa (Decreto Municipal nº 63.552)

SÃO PAULO – SP
2025

LUCIANO FINOZZI MOLERO JUNIOR

RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA E O RACISMO ESTRUTURAL

Análise Constitucional do Programa Smart Sampa (Decreto Municipal nº 63.552)

Trabalho de Conclusão de Curso apresentado ao curso de Direito da Pontifícia Universidade Católica de São Paulo - PUC SP, como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientador: Prof. Marcelo Buczek Bittar

SÃO PAULO – SP

2025

RESUMO

A presente pesquisa realiza uma análise crítica da utilização de tecnologias de reconhecimento facial na segurança pública, tomando como estudo de caso o Programa Smart Sampa, instituído pela Prefeitura de São Paulo por meio do Decreto Municipal nº 63.552/2024. O objetivo geral consiste em investigar a compatibilidade dessa política pública com os princípios constitucionais da igualdade, da dignidade da pessoa humana e do devido processo legal, partindo da hipótese de que o sistema contribui para a criminalização seletiva de pessoas negras e reforça práticas de racismo estrutural sob a aparência de neutralidade tecnológica.

A metodologia adotada é predominantemente qualitativa, de caráter explicativo e descritivo, com abordagem hipotético-dedutiva. O trabalho fundamenta-se em revisão bibliográfica de autores como Foucault, Deleuze e Silvio Almeida, bem como na análise documental de decretos, relatórios oficiais, jurisprudência do Supremo Tribunal Federal e dados obtidos por meio da Lei de Acesso à Informação. Foram examinados seis meses de funcionamento do programa (21/11/2024–21/05/2025), cujos resultados evidenciaram inconsistências técnicas, ausência de legislação específica e indícios de seletividade racial nas abordagens realizadas, agravados pelo viés racista presente nos algoritmos de reconhecimento facial.

Constatou-se que a coleta massiva de dados biométricos sem consentimento informado, aliada à opacidade na gestão das informações e à reprodução de vieses algorítmicos discriminatórios, compromete a legitimidade constitucional do Programa Smart Sampa e coloca em risco a efetividade dos direitos fundamentais previstos na Constituição Federal de 1988. Nesse sentido, a pesquisa busca contribuir para o debate acadêmico e jurídico acerca dos limites constitucionais da vigilância algorítmica no Brasil contemporâneo, destacando a necessidade urgente de marcos normativos capazes de assegurar a proteção dos direitos fundamentais frente à expansão das tecnologias de segurança.

Palavras-chave: Constitucionalidade. Direitos fundamentais. Racismo estrutural. Reconhecimento facial; Segurança pública.

ABSTRACT

This research conducts a critical analysis of the use of facial recognition technologies in public security, focusing on the case study of the Smart Sampa Program, established by the São Paulo City Hall through Municipal Decree nº 63.552/2024. The general objective is to investigate the compatibility of this public policy with the constitutional principles of equality, human dignity, and due process of law, based on the hypothesis that the system contributes to the selective criminalization of Black people and reinforces practices of structural racism under the guise of technological neutrality.

The methodology adopted is predominantly qualitative, with an explanatory and descriptive character, and a hypothetical-deductive approach. The research is based on a bibliographic review of authors such as Foucault, Deleuze, and Silvio Almeida, as well as on documentary analysis of decrees, official reports, decisions of the Brazilian Supreme Federal Court, and data obtained through the Access to Information Law. Six months of the program's operation (11/21/2024–05/21/2025) were examined, whose results showed technical inconsistencies, lack of specific legislation, and evidence of racial selectivity in the approaches carried out, aggravated by the racist bias present in facial recognition algorithms.

It was found that the massive collection of biometric data without informed consent, combined with opacity in data management and the reproduction of discriminatory algorithmic biases, compromises the constitutional legitimacy of the Smart Sampa Program and threatens the effectiveness of the fundamental rights enshrined in the 1988 Federal Constitution. In this sense, the research seeks to contribute to the academic and legal debate on the constitutional limits of algorithmic surveillance in contemporary Brazil, highlighting the urgent need for regulatory frameworks capable of ensuring the protection of fundamental rights in the face of the expansion of security technologies.

Keywords: Constitutional principles. Facial recognition. Fundamental rights. Public security. Structural racism.

SUMÁRIO

LISTA DE TABELAS

1 INTRODUÇÃO

A difusão de tecnologias de vigilância baseadas na análise de dados biométricos, especialmente o reconhecimento facial, inaugurou um novo patamar de intervenção estatal no espaço público. Embora prometa ganhos de eficiência na segurança urbana, esse mecanismo submete todas as pessoas que transitam em espaços públicos à coleta involuntária de dados sensíveis, gerando tensões constitucionais relevantes, sobretudo em sociedades marcadas por desigualdades históricas e racismo estrutural.

No Brasil, o uso dessas tecnologias de vigilância tem se intensificado, particularmente por meio de iniciativas estatais, como o Programa Smart Sampa, promovido pela Prefeitura de São Paulo, durante a gestão de Ricardo Nunes. O projeto prevê a instalação de câmeras com sistemas de reconhecimento facial em diversas regiões da cidade, com a justificativa de aumentar a segurança e eficiência pública. Contudo, a ausência de legislação específica, a opacidade na gestão dos dados coletados e a possibilidade de viés algorítmico racista colocam em xeque sua legitimidade constitucional e sua compatibilidade com os direitos fundamentais previstos na Constituição Federal de 1988.

Neste cenário, a presente pesquisa tem como objeto de estudo a análise crítica da implementação do reconhecimento facial no Programa Smart Sampa, à luz dos princípios constitucionais da igualdade, dignidade da pessoa humana, não discriminação e da proteção contra práticas de criminalização seletiva. Interessa-nos compreender se tal política pública reproduz o racismo institucional sob a aparência de neutralidade tecnológica, ofendendo princípios constitucionais basilares.

Sob essa ótica, a pergunta que guia este trabalho é: a implementação do reconhecimento facial no Programa Smart Sampa, em São Paulo, reproduz práticas de racismo institucional em violação aos direitos fundamentais?

Parte-se da hipótese de que o sistema de reconhecimento facial adotado pelo Programa contribui para a criminalização seletiva de pessoas negras, em violação aos princípios constitucionais, e que, ao operar sem regulação específica, compromete garantias fundamentais, perpetuando desigualdades raciais no exercício do poder punitivo estatal.

O objetivo geral desta pesquisa é investigar a compatibilidade da tecnologia de reconhecimento facial, especialmente no Programa Smart Sampa, com os preceitos constitucionais da igualdade, da dignidade da pessoa humana e do devido processo legal. Como objetivos específicos: **a)** estudar os fundamentos teóricos do racismo estrutural, analisando a vigilância em sociedades contemporâneas a luz das ideias de Foucault e Deleuze; **b)** analisar o arcabouço normativo e legal referente ao Programa Smart Sampa, detalhando seus procedimentos internos e verificando possíveis risco de inconstitucionalidade; **c)** examinar os dados oficiais dos seis primeiros meses de funcionamento (21/11/2024–21/05/2025) do programa à luz dos dados empíricos e técnicos disponíveis avaliando principalmente seu impacto sobre a população negra.; e **d)** listar os vícios de constitucionalidade por meio dos dados teóricos e empíricos provenientes da análise.

A justificativa para o presente trabalho reside na urgência de se debater o impacto das tecnologias de vigilância sobre populações historicamente marginalizadas, principalmente no contexto brasileiro de racismo estrutural e seletividade penal. A análise do Programa Smart Sampa, nesse sentido, oferece uma oportunidade de reflexão crítica acerca da atuação do Estado e da compatibilidade da vigilância algorítmica, promovida pela prefeitura de São Paulo, com os postulados do Estado Democrático de Direito.

A metodologia empregada nesta pesquisa é qualitativa, com abordagem hipotético-dedutiva. Serão utilizados dados coletados por meio da Lei de Acesso à Informação (LAI), bem como relatórios institucionais, notícias jornalísticas, artigos científicos e jurisprudência do Supremo Tribunal Federal. O estudo de caso do Programa Smart Sampa será examinado à luz do marco teórico que articula os conceitos Sociedade de Controle, Racismo Institucional e Controle Constitucional.

O trabalho organiza-se em seis capítulos. O primeiro corresponde a esta introdução. O segundo apresenta o marco teórico, examinando os fundamentos do reconhecimento facial, a transição das sociedades disciplinares para as sociedades de controle e a persistência do racismo estrutural no Brasil e nas tecnologias. O terceiro dedica-se à análise dos normativos que instituem o Programa Smart Sampa e dos procedimentos operacionais que regulam o uso do reconhecimento facial. O quarto capítulo desenvolve a investigação empírica, a partir dos dados oficiais da amostragem de 6 meses de funcionamento do programa. O quinto capítulo discute os vícios de constitucionalidade identificados, tanto formais quanto materiais. Por fim, o sexto capítulo apresenta as considerações finais, retomando a pergunta de pesquisa, as hipóteses formuladas e os principais achados da pesquisa, bem como apontando limitações e perspectivas futuras.

Portanto, ao analisar criticamente o Programa Smart Sampa e a utilização de tecnologias de reconhecimento facial, pretende-se evidenciar não apenas os limites constitucionais dessa política pública, mas também os riscos que ela impõe à consolidação de um Estado Democrático de Direito fundado na igualdade, na dignidade da pessoa humana e na não discriminação. A investigação busca demonstrar que a promessa de eficiência e segurança não pode servir de justificativa para práticas que aprofundam desigualdades históricas, reproduzem o racismo institucional e enfraquecem garantias fundamentais. Assim, o estudo contribui para o debate acadêmico e jurídico sobre os impactos das tecnologias de vigilância no Brasil contemporâneo, ao mesmo tempo em que aponta para a urgência de uma reflexão crítica e da construção de marcos normativos capazes de assegurar a efetiva proteção dos direitos fundamentais diante da expansão da vigilância algorítmica

2 RACISMO ESTRUTURAL: UMA ANÁLISE CONSTITUCIONAL DA VIGILÂNCIA

2.1 APRESENTAÇÃO DO CAPÍTULO

O presente capítulo estabelece as bases teóricas e críticas para a análise do fenômeno de vigilância automatizada com reconhecimento facial em vias públicas na cidade de São Paulo, instituído por meio do Decreto Municipal nº 63.552, datado de 4 de julho de 2024, compreendendo-o como uma problemática eminentemente jurídico-política.

A investigação parte da premissa de que a Constituição da República Federativa do Brasil de 1988 representa um projeto de nação eminentemente fundamentado na dignidade da pessoa humana, na igualdade e na liberdade. Verifica-se, contudo, que a implementação crescente de tecnologias de vigilância pelo poder estatal tenciona diretamente esses objetivos fundantes, trazendo novos desafios à garantia dos direitos fundamentais estabelecidos no Pacto Social (Constituição Federal de 1988) que fundou o Estado brasileiro contemporâneo.

Demonstra-se, ao longo deste capítulo, como a adoção de tais aparatos, especialmente em uma sociedade historicamente marcada pelo racismo estrutural, arrisca converter-se em um vetor de aprofundamento das desigualdades e discriminação. A partir da articulação entre o direito constitucional, a teoria crítica e os estudos sobre tecnologia e sociedade, busca-se construir o alicerce analítico para a investigação empírica subsequente, que avaliará se a aplicação concreta de sistemas de reconhecimento facial pode gerar práticas discriminatórias e, assim, violar o núcleo axiológico do projeto constitucional brasileiro.

2.2 A CONSTITUIÇÃO DE 1988 COMO PROJETO EM TENSÃO

A promulgação da Constituição de 1988 representou a formalização de um pacto social que visava superar um passado autoritário e inaugurar um futuro democrático, pluralista e socialmente justo. A Constituição Federal, nesse sentido, "representa o esforço de reconstrução do país, o pacto de civilização celebrado pela sociedade brasileira para superar o autoritarismo" (BARROSO, 2020, p. 87), inaugurando uma nova ordem jurídica e social. Seus objetivos fundamentais, inscritos no artigo 3º, conferem ao texto um caráter inegavelmente emancipatório.

> Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil:

> I - Construir uma sociedade livre, justa e solidária;
> II - Garantir o desenvolvimento nacional;
> III - Erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais;
> IV - Promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.
> (BRASIL, Constituição Federal de 1988, artigo 3°)

Trata-se de um documento que não apenas organiza o Estado, mas projeta um ideal de sociedade a ser ativamente construído. Nesse sentido, a CF/88 pode ser compreendida como uma Constituição dirigente, que estabelece tarefas e programas a serem cumpridos pelos poderes públicos.

Contudo, uma análise crítica adverte contra uma leitura puramente idealista. A Constituição é também um campo de disputas, refletindo as contradições sociais e dificuldades na implementação destes ideais norteadores no mundo material. Isto é, ao mesmo tempo em que direciona a ação estatal para a promoção da ordem pública, ela cumpre o papel de proteção dos direitos e liberdades fundamentais contra abusos de entes públicos.

De forma que a Constituição "não é apenas um ordenamento jurídico orientador da ação estatal para a consecução de determinados fins, mas também um sistema que protege os direitos fundamentais contra a atuação arbitrária do poder público" (Canotilho, 2001, p. 117).

Esse duplo caráter da Constituição ganha relevo na era digital. A proteção de dados pessoais foi reconhecida como direito fundamental pela Emenda Constitucional nº 115/2022, que inseriu no art. 5º, inciso LXXIX, o direito à proteção de dados pessoais, inclusive nos meios digitais.

> "Art. 5º
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.
> (Emenda Constitucional nº 115/2022)

A doutrina tem ressaltado que a face humana, ao constituir elemento único e permanente de identificação, configura dado biométrico sensível, cuja tutela é reforçada pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que em seu art. 5º, II, define como dado sensível “informação biométrica, quando vinculada a uma pessoa natural”.

> Art. 5º Para os fins desta Lei, considera-se:

> I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> (Lei nº 13.709/2018)

Nesse sentido, Danilo Doneda (2019, p. 215) observa que "a biometria é o núcleo dos dados sensíveis, pois permite a identificação inequívoca do indivíduo e sua utilização exige restrições rígidas de finalidade e proporcionalidade".

A jurisprudência do Supremo Tribunal Federal também tem reconhecido a centralidade da proteção da identidade e da privacidade na era digital. No RE 1010606/SP (Tema 990 da repercussão geral), o STF fixou tese de que "o sigilo de dados pessoais é corolário do direito fundamental à intimidade e à vida privada". Mais recentemente, na ADPF 695, o Tribunal declarou que a coleta e o compartilhamento massivo de dados sem previsão legal específica viola a Constituição, justamente por afrontar os princípios da proporcionalidade e da reserva legal.

Sob esta ótica, a vigilância tecnológica implementada pelo Município de São Paulo, por meio do Programa Smart Sampa, evidencia a tensão intrínseca entre duas dimensões constitucionais: de um lado, seu papel de promoção da ordem pública e da segurança urbana; de outro, o risco de eventual violação de direitos fundamentais. A questão que se coloca, portanto, é como o projeto emancipatório da Constituição se mantém coerente quando os novos instrumentos de sua implementação podem, inadvertidamente, gerar uma afronta grave, aos seus objetivos essenciais

2.3 TECNOLOGIA, VIGILÂNCIA E O ESTADO

O programa Smart Sampa é exemplo de que o exercício do poder estatal encontra um novo paradigma que vai além de suas manifestações tradicionais, encontrando na coleta massiva de dados e na vigilância automatizada uma nova forma de controle social. Este fenômeno representa uma atualização das dinâmicas de poder que, segundo a genealogia de Foucault, sucederam o antigo poder soberano, para dar lugar ao poder disciplinar, e posteriormente, a uma Sociedade de Controle Difuso, (DELEUZE, 1992)

> Desaparece, pois, no início do século XIX, o grande espetáculo da punição física; o corpo supliciado é evitado; o ritual teatral da vingança pública não tem mais lugar. [...] O castigo deixou de ser o palco. Sua eficácia é medida a partir de sua fatalidade, não mais a sua intensidade visível. (FOUCAULT, 2014, p. 16).

> O poder disciplinar é um poder que, em vez de se apropriar e de retirar, tem como função maior ‘adestrar’; ou sem dúvida adestrar para retirar e se apropriar ainda mais e melhor. Ele não amarra as forças para reduzi-las; procura ligá-las para multiplicá-las e utilizá-las. [...] A disciplina ‘fabrica’ indivíduos; ela é a técnica específica de um poder que toma os indivíduos ao mesmo tempo como objetos e como instrumentos de seu exercício. (FOUCAULT, 2014, p. 177).

Este último, a sociedade disciplinar, de natureza produtiva, opera por meio de instituições como a prisão e a escola, visando otimizar as forças dos corpos através de uma vigilância hierarquizada e constante, simbolizada pela arquitetura panóptica. A disciplina funciona pela internalização da norma, induzida por uma visibilidade total do indivíduo, que se torna o principal agente de sua própria sujeição. A vigilância, nesse modelo, é uma "peça interna no aparelho de produção e uma engrenagem específica do poder disciplinar" (FOUCAULT, 2014, p. 175), garantindo a ordem através do controle minucioso dos comportamentos.

Com o aprimoramento das tecnologias de vigilância, contudo, evolui desse modelo para o que Deleuze (1992) conceitua como "sociedades de controle". Se a disciplina operava em espaços fechados e por meio de moldes fixos, o controle se caracteriza por sua natureza aberta, contínua e modulável, operando não mais por confinamento, mas por "controle contínuo e comunicação instantânea" (DELEUZE, 1992, p. 220).

> Nas sociedades de disciplina sempre se estava recomeçando (da escola para o quartel, do quartel para a fábrica), enquanto nas sociedades de controle nunca se termina nada [...]. A linguagem numérica do controle é feita de cifras, que marcam o acesso à informação, ou a recusa. Não se está mais diante do par massa-indivíduo. Os indivíduos se tornaram “dividuais”, e as massas se tornaram amostras, dados, mercados ou “bancos”. (DELEUZE, 1992, p. 224).

A transição do poder disciplinar para o poder de controle representa, portanto, uma intensificação e uma desterritorialização da vigilância. Ela se torna menos visível em sua arquitetura, porém mais onipresente e rápida no controle dos corpos, transformando o próprio espaço público em um elemento de constante vigilância digital e automatizada.

No contexto jurídico brasileiro, essa expansão do controle, contudo, não ocorre em um vácuo legal, mas em zonas cinzentas onde a inovação tecnológica avança mais rápido que a regulação. Essa anomia normativa, onde a tecnologia opera sem o devido processo de revisão legal e democrático de seus resultados, a vigilância deixa de ser uma ferramenta de investigação arriscando se tornar um mecanismo de controle seletivo, afetando desproporcionalmente corpos e territórios historicamente já posicionados nesse lugar de exceção.

2.4 RACISMO ESTRUTURAL E A AUTOMAÇÃO DA VIGILÂNCIA

O Pacto Constitucional de igualdade (art. 3º, IV) e o repúdio ao racismo (art. 5º, XLII) confrontam diretamente as bases escravocratas da história da nação brasileira.

> Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil:
> IV - Promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.
> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> XLII - a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei;
> (BRASIL, Constituição Federal de 1988, artigo 3°)

O racismo no Brasil, conforme define Silvio Almeida, é estrutural, sendo a "manifestação normal de uma sociedade, e não um fenômeno patológico" (ALMEIDA, 2019, p. 33). Essa estrutura se perpetua através das instituições, que são o "espaço de materialização" onde o racismo "se reproduz e ganha contornos de normalidade" (ALMEIDA, 2019, p. 52).

A tese de Silvio Almeida, de que o racismo se materializa nas instituições, encontra sua prova na seletividade penal, observável pelos dados do sistema de justiça criminal em

comparação com a proporção demográfica da população. Segundo o Anuário Brasileiro de Segurança Pública (2024), 68,2% da população carcerária brasileira é negra, uma super-representação massiva frente aos 56% (IBGE, 2024) que compõem a população geral de pessoas pretas e pardas somadas.

O perigo se agrava ao constatar que as ferramentas de Reconhecimento Facial são comprovadamente falhas, operando com vieses que penalizam grupos racializados. O estudo seminal "Gender Shades" expôs essa realidade ao revelar que, enquanto a taxa de erro de sistemas de reconhecimento facial para classificar o gênero de homens brancos era de apenas 0,8%, para mulheres negras essa taxa saltava para 34,7% (BUOLAMWINI; GEBRU, 2018).

O estudo seminal “Gender Shades” avaliou a acurácia de três APIs comerciais de classificação de gênero (Microsoft, IBM e Face++) e constatou uma disparidade expressiva: 0,8% de erro para homens de pele clara versus 34,7% para mulheres de pele escura. Para realizar a auditoria, as autoras criaram o Pilot Parliaments Benchmark (PPB), um conjunto de 1.270 imagens de parlamentares de três países africanos e três europeus, balanceado por gênero e por tom de pele segundo a escala de Fitzpatrick.

A discrepância nos resultados foi a principal evidência. A conclusão direta dos autores, no resumo do artigo:

> In our evaluation, we found that all classifiers performed better on male faces than female faces and on lighter faces than darker faces. The classifiers from IBM, Microsoft, and Face++ performed the worst on darker female subjects, with error rates of up to 34.7%. The maximum error rate for the lightest male subjects was 0.8%. This large disparity in accuracy for darker women demonstrates the need for substantially more inclusive training data and internal and external auditing of these systems to mitigate bias. (BUOLAMWINI; GEBRU, 2018, p. 1)1.

Essa evidência foi confirmada em larga escala pelo Instituto Nacional de Padrões e Tecnologia dos EUA (NIST), cujo relatório de 2019 concluiu que os algoritmos apresentaram

[1] Tradução livre: "Em nossa avaliação, descobrimos que todos os classificadores tiveram um desempenho melhor em rostos masculinos do que em rostos femininos e em rostos mais claros do que em rostos mais escuros. Os classificadores da IBM, Microsoft e Face++ tiveram o pior desempenho em indivíduos do sexo feminino com pele mais escura, com taxas de erro de até 34,7%. A taxa de erro máxima para os indivíduos do sexo masculino com pele mais clara foi de 0,8%. Essa grande disparidade na precisão para mulheres negras demonstra a necessidade de dados de treinamento substancialmente mais inclusivos e de auditoria interna e externa desses sistemas para mitigar o viés."[1]

taxas de falsos positivos, um erro que no contexto do Smart Sampa identifica um inocente como suspeito, de 10 a 100 vezes maiores para rostos de pessoas negras e asiáticas em comparação com rostos de brancos (NIST, 2019).

O estudo do Instituto Nacional de Padrões e Tecnologia dos EUA é a mais extensa auditoria do gênero, testando 189 algoritmos de 99 desenvolvedores. Ele focou nos erros de "falsos positivos", que ocorrem quando o sistema identifica incorretamente duas pessoas diferentes como sendo a mesma, um erro perigosíssimo em investigações criminais.

O relatório é categórico ao afirmar a existência de vieses demográficos. A citação direta do sumário executivo apresenta os dados mais alarmantes:

> For one-to-many matching, we found false positive rates often varied by large factors across demographics. For U.S. developed algorithms, there were high rates of false positives for Asian and African American faces relative to images of Caucasians. The differentials often ranged from a factor of 10 to beyond 100 times, depending on the algorithm. (NIST, 2019, p. iv).2

Este cenário, como define Tarcízio Silva, configura o racismo algorítmico, no qual "a reiteração de iniquidades raciais históricas por meio de sistemas computacionais" (SILVA, 2022, p. 27) transforma uma ferramenta pretensamente neutra em um mecanismo de perpetuação da discriminação.

Dessa forma, o viés de seletividade penal e o encarceramento em massa da população negra, já documentados por autores como Ana Flauzina, encontram nos algoritmos de vigilância uma forma de automatizar e legitimar, sob um manto de neutralidade técnica, as mesmas práticas discriminatórias que estruturam a sociedade.

É nesse maquinário já racialmente enviesado que as tecnologias de reconhecimento facial são inseridas. O problema central da vigilância por reconhecimento facial reside no acoplamento de uma tecnologia com vieses raciais comprovados a um aparato de segurança pública que já opera com base na seletividade penal. O sistema tecnológico não é implementado em um vácuo, mas sobre uma estrutura estatal historicamente discriminatória, resultando na amplificação mútua de ambos os vieses. Não apenas espelha o preconceito social, mas o

---

[2] Tradução livre: "Para a correspondência um-para-muitos, descobrimos que as taxas de falsos positivos frequentemente variavam por grandes fatores entre os grupos demográficos. Para os algoritmos desenvolvidos nos EUA, houve altas taxas de falsos positivos para rostos asiáticos e afro-americanos em relação a imagens de caucasianos. As diferenciações frequentemente variaram por um fator de 10 a mais de 100 vezes, dependendo do algoritmo."

operacionaliza em larga escala. Automatizando a suspeição, acelera a tomada de decisões e legitima práticas discriminatórias sob uma falsa aura de objetividade e neutralidade técnica, como alertam estudos de Buolamwini & Gebru (2018)

3 BASE IDEOLÓGICA E NORMATIVA DO PROGRAMA SMART SAMPA

3.1 APRESENTAÇÃO DO CAPÍTULO

O presente capítulo tem como objetivo científico analisar o Programa Smart Sampa em um estudo empírico e descritivo de tensão constitucional, aprofundando o conceito de Sociedade de Controle e a base normativa que trouxe o programa à luz. A análise examina de que modo a adoção de tecnologias de vigilância, em uma sociedade historicamente marcada pelo racismo estrutural, pode reproduzir desigualdades e fragilizar a concretização da promessa constitucional de dignidade e igualdade.

O capítulo anterior demonstrou que o racismo estrutural, longe de ser um desvio, configura-se como elemento das instituições brasileiras, reproduzindo a discriminação por meio do maquinário público. Nesse sentido, dados recentes evidenciam que sistemas de reconhecimento facial apresentam taxas de erro significativamente maiores em relação a pessoas negras, o que revela que a tecnologia não atua em um vácuo social, mas interage com estruturas de poder preexistentes, podendo amplificar suas distorções. Como adverte Silvio Almeida (2019, p. 47), "[...] o racismo não é um fenômeno periférico, mas um elemento constitutivo das instituições sociais e políticas brasileiras".

A análise constitucional crítica do Smart Sampa exige, portanto, situar o programa na racionalidade do biopoder, tal como formulada por Foucault. O autor demonstra, ao tratar do Panóptico, que a vigilância eficaz não se resume à coerção direta, mas induz um estado permanente de visibilidade, capaz de produzir disciplina interiorizada:

> "Fazer com que a vigilância seja permanente em seus efeitos, mesmo se é descontínua em sua ação; que a perfeição do poder tenda a tornar inútil a atualidade de seu exercício; que este aparelho arquitetural seja uma máquina de criar e sustentar uma relação de poder independente daquele que o exerce; enfim, que os detentos se encontrem presos numa situação de poder de que eles mesmos são os portadores" (FOUCAULT, 2014, p. 176-177).

Esse modelo disciplinar descrito pelo filósofo supracitado é ampliado por Deleuze, que identifica o surgimento das sociedades de controle, nas quais o poder não se restringe mais a instituições fechadas, mas opera de modo contínuo, difuso e capilar. Como adverte o autor:

> Nas sociedades de disciplina sempre se estava recomeçando (da escola para o quartel, do quartel para a fábrica), enquanto nas sociedades de controle nunca se termina nada [...]. A linguagem numérica do controle é feita de cifras, que marcam o acesso à informação, ou a recusa. Não se está mais diante do par massa-indivíduo. Os indivíduos se tornaram "dividuais", e as massas se tornaram amostras, dados, mercados ou "bancos". (DELEUZE, 1992, p. 224).

Quando Deleuze afirma que "os indivíduos se tornaram 'dividuais'", introduz uma noção fundamental para compreender a racionalidade que envolve o programa de reconhecimento facial do Município de São Paulo. O "dividual" é o sujeito observado sob o viés dos dados, reduzido a perfis de consumo, deslocamento e identificação biométrica.

No contexto do Smart Sampa, o cidadão deixa de ser concebido como indivíduo portador de direitos e garantias constitucionais, para tornar-se um conjunto de informações processáveis. A coleta massiva de dados dos indivíduos em espaços públicos para comparação com o Banco Nacional de Mandado de Prisão (BNMP), nesse sentido, apresenta-se como um processo de "dividuação" da pessoa humana.

Assim, o poder não se exerce mais sobre corpos situados em espaços delimitados, mas sobre fluxos de informações digitais, administrando probabilidades e projetando sobre cada rosto o potencial de corresponder a uma identidade "suspeita".

> "A solução deverá permitir a detecção de faces em tempo real a partir das imagens das câmeras, extrair as características biométricas de cada face detectada e compará-las com as faces cadastradas em um ou mais bancos de dados de referência (watchlists). Em caso de correspondência com um grau de confiança pré-estabelecido, o sistema deverá gerar um alarme em tempo real para o operador da central de monitoramento, que conterá a imagem da face, o vídeo do momento da detecção e os dados associados ao registro no banco de dados. "(Edital de Concorrência nº 01/SMIT/2023 – Contratação de Solução de

> Plataforma de Videomonitoramento Urbano Inteligente (Smart Sampa). Anexo I – Termo de Referência. São Paulo, 2023).

Sob essa ótica, o programa não apenas promete maior segurança e eficiência, mas também exemplifica a consolidação de uma sociedade de controle, marcada pela vigilância permanente e pela gestão algorítmica dos corpos e dos dados. Nesse contexto, o monitoramento constante dissolve as fronteiras entre o público e o privado, gerando novas tensões constitucionais quanto à proteção dos direitos fundamentais.

Diante disso, cabe examinar de forma detalhada a estrutura e o funcionamento do Programa Smart Sampa, identificando como suas tecnologias e procedimentos operacionais se articulam e de que modo impactam os princípios da legalidade, da igualdade e da dignidade da pessoa humana.

3.2 O FUNCIONAMENTO E BASE LEGAL DO PROGRAMA SMART SAMPA

O Programa Smart Sampa insere-se em um contexto nacional marcado pela expansão do uso de tecnologias de vigilância pela administração pública, legitimadas pelo discurso da modernização administrativa e da suposta eficiência no aprimoramento da segurança pública. “O programa Smart Sampa prevê a instalação de 20 mil novas câmeras na capital com tecnologia de reconhecimento facial. Elas se somarão a outras 20 mil já existentes de parceiros da Prefeitura [...].” (SÃO PAULO, Prefeitura Municipal. Secretaria Especial de Comunicação. 2023)

Concebido como o maior sistema de monitoramento da América Latina:

> “[...]Com isso, São Paulo terá o maior sistema de monitoramento de segurança da América Latina, que usa o reconhecimento facial de câmeras inteligentes para identificar casos de violência urbana e foragidos da polícia” (SÃO PAULO, Prefeitura Municipal. Secretaria Especial de Comunicação, Prefeitura lança o Smart Sampa, que vai instalar 20 mil câmeras com reconhecimento facial na cidade, 1 fev. 2023).

A etapa preliminar de concepção do Smart Sampa remonta ao Edital nº 01/SMIT/2023, Termo de Referência, publicado pela Secretaria Municipal de Inovação e Tecnologia (SMIT),

que estabeleceu as diretrizes técnicas e operacionais para o desenvolvimento de uma plataforma de integração de dados urbanos. Nesse documento, a Prefeitura determinou que;

> "[...]a plataforma deverá permitir integração com sistemas de diferentes secretarias municipais e órgãos públicos, incluindo segurança urbana, mobilidade e zeladoria" (SÃO PAULO, Edital nº 01/SMIT/2023 – Termo de Referência, 2023, Anexo I, item 3.2.1).

Assim, o edital funcionou como ato precursor e matriz tecnológica do programa, delineando a futura estrutura de interoperabilidade e análise algorítmica que seria posteriormente formalizada por meio do Decreto Municipal nº 63.552, de 4 de julho de 2024, que o instituiu sob a gestão da Secretaria Municipal de Segurança Urbana (SMSU).

> "Art. 2º Constituem diretrizes essenciais do Programa Smart Sampa:
> I - A implantação de plataforma integrada de serviços multiagências, objetivando a melhoria da qualidade dos serviços públicos prestados à população;
> II – A implantação de rede de câmeras de vigilância inteligente em locais estratégicos da cidade, com integração aos órgãos de segurança pública e serviços de urgência e emergência;
> III - a promoção da integração de dados e sistemas de informação entre os órgãos públicos, otimizando os serviços municipais de atendimento aos cidadãos;" (Decreto Municipal nº 63.552, de 4 de julho de 2024)

O Decreto Municipal nº 63.552/2024 estabelece como metas do Programa Smart Sampa o aprimoramento da segurança e da gestão pública, por meio de um sistema integrado de videomonitoramento.

O programa combina reconhecimento facial e leitura automática de placas veiculares, permitindo o cruzamento algorítmico de dados entre diferentes órgãos municipais.

No que se refere ao reconhecimento facial, reportagens internacionais indicam que o sistema utiliza tecnologia russa desenvolvida pela empresa NtechLab, responsável pelo software FindFace Multi, capaz de gerar alertas automáticos quando a similaridade facial ultrapassa 92%. Segundo o jornal El País:

> "El sistema está gestionado por el software impulsado por inteligencia artificial FindFace, desarrollado por la empresa rusa NtechLab. Los algoritmos comparan los rostros captados con las imágenes almacenadas en bases de datos de personas buscadas. Las coincidencias se activan únicamente cuando la similitud supera el 92%, para evitar errores de identificación" (EL PAÍS, São Paulo, un gran hermano de 25.000 cámaras y reconocimiento facial contra el crimen, 04/ 2025)[3]

Além do reconhecimento facial, o sistema também realiza a leitura automática de placas de veículos (LPR/ALPR) e emprega drones em situações de monitoramento aéreo. Segundo reportagem da CNN Brasil (2025):

> "A Prefeitura de São Paulo anunciou a integração de 5,3 mil câmeras de monitoramento privadas ao programa Smart Sampa, que já utiliza câmeras inteligentes com reconhecimento facial e leitura de placas de veículos para identificar foragidos da polícia, detectar atos de vandalismo e localizar pessoas desaparecidas. O sistema também prevê o uso de drones para o acompanhamento aéreo em tempo real." (CNN BRASIL. Prefeitura de SP integra 5,3 mil câmeras privadas ao Smart Sampa. São Paulo: CNN Brasil, 2025.)

A expansão e a integração institucional do programa foram destacadas pela Agência Brasil, que noticiou a inauguração da central de monitoramento:

> "A Prefeitura de São Paulo inaugurou nesta quinta-feira (4) a central do programa Smart Sampa, que já conta com mais de 13 mil câmeras instaladas e prevê alcançar 40 mil até 2025. O sistema cruza imagens captadas com bases de dados de pessoas desaparecidas e foragidas, e os alertas gerados automaticamente

[3] "O sistema é gerido pelo software FindFace, impulsionado por inteligência artificial e desenvolvido pela empresa russa NtechLab. Os algoritmos comparam os rostos captados com as imagens armazenadas em bases de dados de pessoas procuradas. As coincidências só são acionadas quando a similaridade supera 92%, a fim de evitar erros de identificação" (tradução nossa de: "El sistema está gestionado por el software impulsado por inteligencia artificial FindFace, desarrollado por la empresa rusa NtechLab. Los algoritmos comparan los rostros captados con las imágenes almacenadas en bases de datos de personas buscadas. Las coincidencias se activan únicamente cuando la similitud supera el 92%, para evitar errores de identificación" – EL PAÍS, São Paulo, un gran hermano de 25.000 cámaras y reconocimiento facial contra el crimen, abr. 2025).

> são verificados por agentes humanos antes do envio das equipes de campo" (AGÊNCIA BRASIL. SP abre central de vigilância de câmeras com reconhecimento facial. Brasília: Empresa Brasil de Comunicação – EBC, 4 jul. 2024.).

De acordo com o item 3.2.1 do mesmo Termo de Referência, além das capacidades descritas, o sistema é constituído por:

> "câmeras inteligentes IP com recursos de análise embarcada, capazes de realizar a detecção automática de eventos, como aglomerações, movimentações atípicas e objetos abandonados, gerando alertas automáticos para a central de monitoramento" (SÃO PAULO, Edital nº 01/SMIT/2023 – Termo de Referência, 2023, Anexo I, item 3.2.1).

O mesmo documento acrescenta a existência de;

> "módulos de análise preditiva baseados em inferência algorítmica, destinados à identificação de padrões de comportamento e à geração de alertas preventivos" (SÃO PAULO, Edital nº 01/SMIT/2023 – Termo de Referência, 2023, Anexo I, itens 3.4.2 e 3.6.1).

A documentação oficial da NtechLab para o FindFace Multi indica que esse software vai além do reconhecimento facial: ele é capaz de detectar e analisar rostos, corpos e veículos, associando a atributos como gênero, idade, óculos, barba e até máscaras faciais. Conforme consta na documentação:

> "FindFace multi can detect, identify, and analyze the following objects in the video: human faces, along with recognition of such facial attributes as gender, age, emotions, glasses, face mask, beard, and many others. The integrated 2D anti-spoofing system ensures that it is a live person in front of a camera and eliminates the possibility of fraud using images on paper or mobile device

> screens." (NTECHLAB, 2024, FindFace Multi Documentation, seção What's New / Object detection)[4]

Além disso, o sistema reconhece elementos específicos de carros, com identificação de atributos como marca, modelo, estilo de carroceria, cor, bem como o número da placa veicular:

> "Cars, with recognition of such car attributes as makes, model, body style, color, license plate number, and others." (NTECHLAB, 2024, FindFace Multi Documentation, seção What's New / Object detection)[5]

O software também utiliza um mecanismo anti-spoofing 2D embutido, que analisa várias imagens sequenciais para distinguir uma pessoa real de possíveis simulações de faces, como fotos ou telas:

> "The integrated 2D anti-spoofing system ensures that it is a live person in front of a camera and eliminates the possibility of fraud using images on paper or mobile device screens." (NTECHLAB, 2024, FindFace Multi Documentation) [6]

No âmbito da cooperação público-privada, o Edital de Chamamento Público da Secretaria Municipal de Segurança Urbana, de 5 de julho de 2024, estabelece que

> "pessoas jurídicas poderão disponibilizar imagens captadas por câmeras privadas para integração ao sistema do Programa Smart Sampa, sem ônus para o Poder Público", ampliando a cobertura territorial e a capilaridade da vigilância" (SÃO PAULO, Edital de Chamamento Público – SMSU, 2024, cláusula 2.1).

---

[4] Tradução livre: "O FindFace Multi pode detectar, identificar e analisar os seguintes objetos no vídeo: rostos humanos, juntamente com o reconhecimento de atributos faciais como gênero, idade, emoções, óculos, máscara facial, barba e muitos outros. O sistema integrado de anti-spoofing 2D garante que haja uma pessoa real diante da câmera e elimina a possibilidade de fraude usando imagens em papel ou telas de dispositivos móveis"

[5] Tradução livre: "Carros, com reconhecimento de atributos como marca, modelo, estilo de carroceria, cor, número da placa e outros"

[6] Tradução livre: "O sistema integrado de anti-spoofing 2D garante que haja uma pessoa real diante da câmera e elimina a possibilidade de fraude usando imagens em papel ou telas de dispositivos móveis"

Já no campo legislativo, o Projeto de Lei nº 01-00166/2025, em tramitação na Câmara Municipal, propõe

> "à regulamentação da instalação de câmeras de monitoramento em logradouros públicos, com compartilhamento de dados e imagens para o sistema Smart Sampa, observados os princípios da proteção de dados pessoais e da transparência pública" (SÃO PAULO, Projeto de Lei nº 01-00166/2025, 2025, art. 3º).

Desse modo, o Smart Sampa ultrapassa a lógica da segurança pública tradicional, consolidando-se como uma infraestrutura algorítmica de vigilância urbana, na qual sistemas automatizados operam sobre extensas bases de dados. Essa integração transforma o espaço urbano em um ambiente de monitoramento permanente, no qual a eficiência tecnológica convive com desafios significativos à privacidade, à legalidade e aos direitos fundamentais.

3.2.1. Estrutura operacional e procedimentos

A execução do Programa Smart Sampa é disciplinada pelo Procedimento Operacional Padrão (POP) nº 16/2025, emitido pela Secretaria Municipal de Segurança Urbana (SMSU) em 20 de maio de 2025. Classificado como de "Nível de Padronização Setorial", o documento define a sequência técnica de ações que regula a operação dos algoritmos de vigilância, desde a captura e o processamento automatizado de imagens até a emissão e validação dos alertas para abordagem. Essa cadeia procedimental é executada no âmbito do Centro Integrado Operacional (CIOP), estrutura administrativa e tecnológica, responsável por coordenar, em tempo real, a integração entre sistemas de monitoramento e agentes públicos. A análise de seu conteúdo, com base em transcrições diretas, é essencial para compreender como a arquitetura normativa transforma o funcionamento algorítmico em decisões e intervenções concretas no espaço público.

A conexão entre o algoritmo e o Procedimento Operacional Padrão representa o momento em que a incerteza técnica é convertida em certeza administrativa. O processo é acionado não por um fato, mas por uma saída probabilística em formato de alerta acionado por operadores de telecomunicação: um índice de similaridade gerado pelo algoritmo, cuja margem de erro e vieses são inerentes à sua programação conforme demonstrado no capítulo anterior.

O POP, então, atua como o dispositivo normativo que absorve e formaliza essa probabilidade, conferindo-lhe o status de um evento administrativo.

3.2.1.1 O Papel do Operador de Telecomunicações (Atividade 1)

O Operador de Telecomunicações atua na linha de frente do fluxo decisório, com atribuições descritas no POP 16/2025 (35 itens), que vão da verificação de estações e sistemas ao despacho e acompanhamento de ocorrências em tempo real. O documento prevê monitoramento reativo e proativo, despacho célere e registro padronizado das ações.

3.2.1.2 Monitoramento e Despacho Geral

O Procedimento Operacional Padrão (POP) nº 16/2025 determina que o Operador de Telecomunicações deve "efetuar o monitoramento de imagens por câmeras, de forma proativa, com a finalidade de identificar possíveis fatos que venham comprometer a ordem pública". Diante da constatação de "fato crime em andamento ou na iminência de ocorrer", o fluxo operacional estabelece uma sequência obrigatória de ações:

> "9.1. Acionar imediatamente o Adjunto de Operações, transmitindo-lhe o identificador da câmera e um breve relato do fato, passando a acompanhar o andamento;
> 9.2. Transferir imagem para Videowall;
> 9.3. Cadastrar Protocolo de Ocorrência no Sentinel X, com o máximo de informações sobre o fato;
> 9.4. Acompanhar a ocorrência até finalizar e, após, adotar etapas do item 5
> Item 23.A diretriz de desempenho é igualmente objetiva: "minimizar ao máximo o tempo para despacho de ocorrências em tela". (SÃO PAULO, 2025, POP 16, PROCEDIMENTO OPERACIONAL PADRÃO DESPACHO DE OCORRÊNCIAS E MONITORAMENTO POR CÂMERAS)

Em síntese, a POP estrutura um modelo de resposta em tempo real, em que a atuação do operador é guiada por protocolos rígidos e automatizados, traduzindo a lógica de eficiência operacional em decisões imediatas de intervenção no espaço público.

3.2.1.3 Procedimentos específicos para tecnologias de reconhecimento (TRF- Tecnologia De Reconhecimento Facial e LPR – Leitura de Placas Veiculares)

O item 13 do Procedimento Operacional Padrão (POP) nº 16/2025 atribui ao Operador de Telecomunicações a execução direta das soluções de Tecnologia de Reconhecimento Facial (TRF) e Leitura de Placas Veiculares (LPR), determinando expressamente: “operar software com TRF e LPR”, 2025, POP 16, Ativ. 1, item 13).

Essas diretrizes configuram uma centralização técnica da vigilância algorítmica, na qual o operador atua como elo entre o sistema automatizado de detecção e as instâncias superiores de comando. Os fluxos operacionais variam conforme a natureza do alerta, definindo procedimentos distintos para correspondências faciais, identificação veicular ou outros eventos gerados pelas plataformas inteligentes.

a) Alerta de pessoa desaparecida (TRF – Tecnologia De Reconhecimento Facial)

Nesse caso, o gatilho operacional é o sinal gerado com índice de semelhança igual ou superior a 80% (item 14). A partir desse ponto, o POP determina que o operador deve “fazer uma segunda verificação dos dados nos sistemas inteligentes” (SÃO PAULO, 2025, POP 16, Ativ. 1, item 14.1). Confirmada a plausibilidade da correspondência, o fluxo impõe as seguintes ações sequenciais: “informar o Adjunto de Operações” (item 14.5) e “despachar a Equipe de Campo mais próxima do local” (SÃO PAULO, 2025, POP 16, Ativ. 1, item 14.6). O encerramento do protocolo é obrigatório quando “a pessoa encontrada não corresponda àquela fornecida pelo sistema” (SÃO PAULO, 2025, POP 16, Ativ. 1 item 14.8).

Em síntese, o procedimento revela uma lógica de dupla checagem com resposta imediata, em que a validação humana atua como etapa intermediária entre o reconhecimento algorítmico e a abordagem policial.

b) Alerta de pessoa procurada/foragida (TRF – Tecnologia De Reconhecimento Facial)

Este é o protocolo mais sensível do sistema, por envolver diretamente a privação de liberdade e a intervenção policial imediata. O gatilho ocorre diante de um alerta facial “com ≥ 90% de semelhança” (SÃO PAULO, 2025, POP 16, Ativ. 1, item 15). Nessa hipótese, o POP

determina uma sequência de validações sucessivas, iniciada pela etapa de checagem cruzada nos bancos de dados oficiais:

> "15.1. Fazer uma segunda verificação dos dados nos sistemas inteligentes (banco de dados de pessoas procurados e foragidos);
> 15.2. Caso não tenha mandado expedido/válido ou dados distintos ao do alerta, relatar observação no histórico do Sentinel X e finalizar o Protocolo de Ocorrência;
> 15.3. Caso o mandado seja válido, prosseguir." (SÃO PAULO, 2025, POP 16, Ativ. 1, itens 15.1–15.3).

Confirmada a validade do mandado, o operador deve "informar o Adjunto de Operações" (item 15.4), "despachar a Equipe de Campo mais próxima do local" (SÃO PAULO, 2025, POP 16, Ativ. 1, item 15.5) e "acompanhar a ação por todas as câmeras disponíveis" (SÃO PAULO, 2025, POP 16, Ativ. 1, item 15.6). Em caso de captura positiva, o protocolo impõe "confirmar os dados do PROCURADO/FORAGIDO com a Equipe de Campo" (item 15.10) (SÃO PAULO, 2025, POP 16, Ativ. 1, itens 15.4–15.6, 15.10).

> "Informar o Adjunto de Operações; despachar a Equipe de Campo […]; acompanhar todas as câmeras disponíveis […]; confirmar os dados […]."
> (SÃO PAULO, 2025, POP 16, Ativ. 1, itens 15.4–15.6, 15.10).

Em termos operacionais, esse fluxo expressa uma lógica de resposta automatizada com validação humana residual, na qual o operador desempenha um papel quase executório dentro da cadeia decisória.

c) Alerta de veículo (LPR - Leitura de Placas Veiculares)

O fluxo operacional referente à Leitura de Placas Veiculares (LPR) apresenta estrutura semelhante à dos protocolos de reconhecimento facial. O processo inicia-se com a etapa de validação automatizada, na qual o operador deve "fazer uma segunda verificação no banco de dados dos sistemas inteligentes" (SÃO PAULO, 2025, POP 16, Ativ. 1, item 16.1). Caso o alerta se revele um falso positivo, o procedimento determina o encerramento imediato do protocolo (SÃO PAULO, 2025, POP 16, Ativ. 1, item 16.2).

> "Fazer uma segunda verificação […]; no caso de veículo, seja um falso/positivo, […] finalizar o Protocolo de Ocorrência." (SÃO PAULO, 2025, POP 16, Ativ. 1, itens 16.1–16.2).

Confirmada a correspondência entre a placa detectada e o registro de interesse, o operador deve comunicar o Adjunto de Operações, despachar a Equipe de Campo e realizar o acompanhamento contínuo das imagens, com registro final no sistema Sentinel X (SÃO PAULO, 2025, POP 16, Ativ. 1, itens 16.1–16.13).

3.2.1.4 Ocorrências prioritárias e disciplina operacional

O Procedimento Operacional Padrão (POP) nº 16/2025 estabelece uma categoria específica de ocorrências prioritárias, classificadas como "Alerta Vermelho", destinadas a situações de extrema urgência. Entre os casos previstos estão "GCM em perigo, agentes de segurança pública, Guardiã Maria da Penha, Alerta Escolar e risco iminente à vida" (SÃO PAULO, 2025, POP 16, Ativ. 1, item 17).

Nessas hipóteses, o Operador de Telecomunicações adquire prerrogativa decisória imediata, podendo "liberar equipes em protocolos com prioridade baixa e/ou média" a fim de assegurar uma resposta rápida e efetiva (SÃO PAULO, 2025, POP 16, Ativ. 1, item 17.2). Essa diretriz confere ao operador um papel discricionário, deslocando momentaneamente o controle hierárquico em nome da urgência operacional.

Do ponto de vista normativo, o "Alerta Vermelho" representa a formalização de um estado de exceção procedimental, em que a eficiência e a celeridade justificam a suspensão temporária da hierarquia decisória ordinária. Esse arranjo revela a tensão entre celeridade administrativa e controle institucional, tema central para a análise constitucional da vigilância e do exercício do poder de polícia no espaço urbano.

3.2.1.5 O Papel da Supervisão Hierárquica (Atividades 2, 3 e 4)

O POP 16/2025 estrutura a supervisão do sistema Smart Sampa em três níveis hierárquicos, Adjunto de Operações, Gerente de Operações e Gestor Operacional, responsáveis por garantir o controle, a fiscalização e a coordenação das ações de monitoramento. Essa

arquitetura cria uma cadeia decisória verticalizada, na qual a supervisão atua como mediadora entre a análise algorítmica e a execução policial.

3.2.1.6 Adjunto de Operações

O Adjunto de Operações representa o primeiro nível de supervisão e atua diretamente sobre os operadores. Cabe-lhe “monitorar as estações de trabalho”, “fiscalizar a conduta dos operadores de telecomunicações” e “corrigir atitudes durante o serviço” (SÃO PAULO, 2025, POP 16, Ativ. 2, itens 1, 18 e 24). É também o ponto de contato para alertas de reconhecimento facial e leitura de placas (itens 31.6 e 31.7) e deve “solicitar imediatamente ao STI a reserva das imagens gravadas, para uso como prova nos autos da persecução penal” (item 42).

Assim, sua função combina supervisão operacional e preservação da cadeia de custódia digital.

3.2.1.7 Gerente de Operações

O Gerente de Operações supervisiona os Adjuntos e zela pela aplicação dos protocolos internos. Entre suas funções estão “fiscalizar o cumprimento das Normas Orientadoras e Procedimentos Operacionais Padrão” e “documentar incidentes e ações tomadas, inclusive os divulgados em mídias e redes sociais” (SÃO PAULO, 2025, POP 16, Ativ. 3, itens 5 e 12).

Sua atuação consolida a dimensão normativa e gerencial do sistema, garantindo conformidade procedimental e registro institucional das ocorrências.

3.2.1.8 Gestor Operacional

No topo da hierarquia, o Gestor Operacional coordena as atividades do CIOP e mantém comunicação direta com o Comando Geral e a SMSU. Compete-lhe “acompanhar ocorrências com potencial de repercussão” e “reportar-se à alta gestão em situações de gravidade” (SÃO PAULO, 2025, POP 16, Ativ. 4, itens 6 e 8).

Sua função consolida o elo entre o plano técnico e o político, transformando a supervisão operacional em instrumento de governança da vigilância urbana.

3.2.2 Resultados esperados e possibilidades de erro

O Procedimento Operacional Padrão (POP) nº 16/2025 encerra cada bloco de atividade com uma dupla dimensão normativa: de um lado, fixa metas de desempenho sob o título "Resultado Esperado"; de outro, reconhece formalmente as falhas potenciais na seção "Possibilidade de Erro". Essa estrutura revela a falibilidade do procedimento humano que envolve a operação dentro do sistema de vigilância.

No caso do Operador de Telecomunicações, o primeiro resultado esperado é o "Despacho de todas as ocorrências no menor tempo possível" (SÃO PAULO, 2025, POP 16/2025, Ativ. 1, item 1). Já a seção "Possibilidade de Erro" é particularmente reveladora, por explicitar os riscos estruturais embutidos no processo decisório. Entre os dez erros elencados, o documento destaca:

> "1. Morosidade no despacho de ocorrência, principalmente as de prioridade ALERTA VERMELHO e ALTA.
> 2. Não se atentar quanto à porcentagem exata de semelhança de ≥ 90% para PROCURADO/FORAGIDO e ≥ 80% para DESAPARECIDO."
> (SÃO PAULO, 2025, POP 16/2025, p. 5).

A admissão institucional dessas falhas é significativa. Ao reconhecer que o erro pode advir tanto da morosidade operacional quanto da interpretação incorreta de parâmetros algorítmicos, o próprio POP evidencia a tensão entre a rigidez procedimental e a incerteza da execução humana e o viés racial do algoritmo. Embora concebida para garantir padronização e rastreabilidade, a estrutura normativa demonstra que a adesão estrita a métricas quantitativas como os limiares de 80% e 90% de similaridade não elimina o risco de falsos positivos, cujas consequências recaem sobre direitos fundamentais, especialmente a liberdade e a integridade física dos sujeitos submetidos a lógica de vigilância do Programa Sampa.

3.2.3 A Arquitetura Operacional do Smart Sampa: Síntese POP 16/2025

A estrutura operacional do Smart Sampa, tal como descrita no POP 16/2025, revela um modelo de vigilância que combina automação algorítmica, supervisão humana e ação policial direta. Esse arranjo, embora composto por regras mínimas, expõe um conjunto de problemas estruturais relacionados à responsabilização, à confiabilidade técnica e aos limites

constitucionais do uso de inteligência artificial na segurança pública. A análise do procedimento permite identificar três zonas críticas de tensão, que agravam os impactos do viés racial presentes em algoritmos de reconhecimento facial em tecnologias de vigilância urbana:

(i) o gatilho algorítmico, em que decisões probabilísticas produzem alertas com potencial de erro estrutural;

(ii) a validação humana, que deveria funcionar como contrapeso ao automatismo, mas pode reproduzir o viés da máquina sob o disfarce de neutralidade técnica; e

(iii) a ação do estado em campo, momento em que a probabilidade se transforma em coerção, materializando o risco constitucional de restrição de liberdade com base em dados incertos.

3.3. O GATILHO ALGORÍTMICO

O ponto de partida do fluxo operacional é o gatilho técnico, isto é, uma decisão puramente automatizada. Conforme o Procedimento Operacional Padrão (POP) nº 16/2025, o sistema de Tecnologia de Reconhecimento Facial (TRF) opera com limiares distintos de similaridade. Para pessoas classificadas como "PROCURADA/FORAGIDA", o sistema gera um alerta quando a correspondência entre a imagem capturada e a constante no banco de dados atinge percentual igual ou superior a 90% (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025a, p. 4, item 15). Já nos casos de "DESAPARECIDA", o limiar é reduzido para 80% (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025a, p. 4, item 14).

Essa diferenciação revela uma camada estrutural de risco, pois a fixação desses limiares não é um dado técnico neutro, mas uma decisão administrativa que define quem está mais sujeito ao erro. Como demonstram Buolamwini e Gebru (2018), os sistemas de reconhecimento facial apresentam desempenho significativamente inferior para rostos de pessoas negras, com taxas de erro até 34,7% superiores às de indivíduos brancos. Do mesmo modo, o relatório do National Institute of Standards and Technology (NIST, 2019) confirmou que os algoritmos testados apresentavam de 10 a 100 vezes mais falsos positivos para rostos de pessoas negras e asiáticas em comparação com rostos de pessoas brancas.

Dessa forma, a calibragem do limiar de similaridade, 80% para desaparecidos e 90% para foragidos, produz efeitos racialmente assimétricos, ao operar sobre uma base tecnológica cuja acurácia é diferencial entre grupos raciais. Como aponta Silvio Almeida (2019, p. 33), o racismo no Brasil é estrutural, isto é, "a manifestação normal de uma sociedade, e não um

fenômeno patológico". A tecnologia, portanto, não elimina o racismo: ela o reproduz em escala algorítmica, ao propagar desigualdades históricas por meio de probabilidades matemáticas que geram suspeição com maior índice de erro para pessoas negras.

A própria administração municipal, em seu Relatório de Impacto à Proteção de Dados, reconhece formalmente a existência desse risco. O documento lista, entre as ameaças, a "possibilidade de discriminação ou preconceito no reconhecimento facial" e as "falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos" (Relatório de Impacto à Proteção de Dados. São Paulo: SMSU, 2025). Como medida de mitigação para tais falhas, o relatório aponta a "obrigatoriedade de dupla verificação de checagem com aprovação de validação de pessoal autorizado e com devido treinamento para tomada de decisão" (Relatório de Impacto à Proteção de Dados. São Paulo: SMSU, 2025).

A fragilidade desse modelo foi admitida na prática quando, em fevereiro de 2025, o limiar para pessoas procuradas foi elevado de 90% para 92%, com o objetivo declarado de "redução de falsos positivos" após a constatação de "inconsistências" (SÃO PAULO, 2025, p. 20). Essa revisão, embora necessária, teve caráter reativo e corretivo, evidenciando que o sistema operou, por um período, com uma taxa de erro considerada inaceitável pela própria gestão. O RIPD, ao tratar o risco de "falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos" como "Médio" e confiar na validação humana como principal salvaguarda, subestima a natureza sistêmica do viés algorítmico e a conhecida propensão ao viés de automação, no qual o operador humano tende a confirmar a decisão da máquina.

Em termos constitucionais, tal constatação revela que a decisão algorítmica probabilística não é apenas um problema técnico, mas um fator de violação potencial do princípio da igualdade (CF/88, art. 5º, caput). Ao automatizar vieses raciais já presentes nas estruturas sociais, o TRF (Tecnologia de Reconhecimento Facial) reconfigura o racismo estrutural como racismo algorítmico, deslocando a discriminação do campo das práticas humanas para o da governança tecnológica, sob a aparência de neutralidade e eficiência.

3.4. A VALIDAÇÃO HUMANA

Uma vez gerado o alerta, o POP 16/2025 determina que a decisão não é final. Inicia-se a fase de validação, conduzida por um Operador de Telecomunicações da Guarda Civil

Metropolitana (GCM). Este agente deve realizar uma "segunda verificação" (item 15.1), que consiste em:

Confirmar a validade do mandado de prisão no Banco Nacional de Mandados de Prisão (BNMP) ou em outros "sistemas inteligentes".

Avaliar a compatibilidade facial entre a imagem do alerta e a do registro oficial.

O procedimento estabelece que, caso o mandado não seja válido ou os dados sejam distintos, o operador deve finalizar o protocolo (item 15.2). Somente após a confirmação humana, o alerta é repassado a um superior (Adjunto de Operações) e uma viatura é despachada (item 15.5). A administração utiliza essa etapa para argumentar que "não há atuação autônoma do algoritmo" (PREFEITURA DE SÃO PAULO, 2025, p. 4).

Contudo, a intervenção humana, neste contexto, está sujeita ao que a literatura denomina viés de automação: a tendência de confiar excessivamente na sugestão de um sistema automatizado, tratando a "compatibilidade de 90%" não como uma probabilidade, mas como uma verdade. O operador, pressionado pelo tempo ("Minimizar ao máximo o tempo para despacho", item 23) e pela aparente objetividade da máquina, pode realizar uma verificação meramente protocolar. Como adverte Luigi Ferrajoli, as garantias penais e processuais existem precisamente para criar obstáculos à eficiência punitiva do Estado, protegendo o cidadão contra o erro.

> "O garantismo penal se opõe a qualquer modelo de direito penal máximo, que se caracteriza pela excessiva severidade das penas, pela sua aplicação indiscriminada e pela ausência de limites e controles sobre o poder punitivo do Estado." (FERRAJOLI, Luigi. Direito e Razão: Teoria do Garantismo Penal. 3. ed. São Paulo: Revista dos Tribunais, 2002, p. 85).

A validação humana, em vez de um filtro robusto, pode se tornar um elo frágil que apenas legitima a falha algorítmica, pavimentando o caminho para a abordagem física.

3.5. A AÇÃO EM CAMPO: A CONVERSÃO DA PROBABILIDADE EM COERÇÃO

A fase final é a abordagem e confirmação, que materializa a vigilância no espaço físico. A equipe da GCM, despachada para o local, realiza a "verificação visual direta da pessoa abordada" (PREFEITURA DE SÃO PAULO, 2025, p. 4). É neste momento que o risco

constitucional atinge seu maior ponto de tensão com os direitos fundamentais. Um cidadão, cuja única infração pode ter sido a semelhança estatística com uma imagem em um banco de dados, é submetido a uma intervenção estatal coercitiva.

O próprio relatório oficial admite a gravidade da situação ao prever que, "se a identificação não puder ser concluída com segurança, a pessoa é conduzida à Delegacia de Polícia" (PREFEITURA DE SÃO PAULO, 2025, p. 4). Isso significa que uma falha do sistema pode resultar na restrição da liberdade de um inocente, ainda que temporariamente. Entre 21 de novembro de 2024 e 21 de maio de 2025, foram registradas 1.246 abordagens sob esse regime, um número que dimensiona o alcance prático do programa.

Essa condução à delegacia, baseada em uma dúvida gerada por um sistema probabilístico, tenciona diretamente o direito fundamental à liberdade de locomoção (CF/88, art. 5º, XV e LXI). A ausência de uma lei formal que discipline tal procedimento agrava a situação, configurando uma potencial violação ao princípio da legalidade estrita. A estrutura operacional do Smart Sampa, portanto, cria um funil onde a probabilidade algorítmica é progressivamente convertida em certeza administrativa e, por fim, em coerção física, com insuficientes salvaguardas para proteger o cidadão contra o erro estatal automatizado.

3.6 CONCLUSÕES E PROPOSIÇÕES JURÍDICAS

A análise empreendida evidencia que o Programa Smart Sampa apresenta vícios de inconstitucionalidade formal e material. No plano formal, foi instituído por decreto municipal, em violação ao princípio da reserva legal (CF/88, art. 5º, II). No plano material, compromete direitos fundamentais à privacidade (CF/88, art. 5º, X e LXXIX), à igualdade (CF/88, art. 3º, IV e art. 5º, caput) e à proporcionalidade, ao implementar vigilância algorítmica sem comprovação empírica de eficácia e sem mecanismos robustos de controle democrático.

Como observa Barroso (2020, p. 219), “o princípio da proporcionalidade exige que medidas restritivas a direitos fundamentais passem por um escrutínio rigoroso de adequação e necessidade” A experiência concreta do Smart Sampa demonstra que tal escrutínio não foi realizado, prevalecendo uma lógica tecnocrática de eficiência em detrimento das garantias constitucionais.

Conclui-se, portanto, que a compatibilização entre inovação tecnológica e o Estado Constitucional de 1988 somente será possível mediante reformas normativas e institucionais que assegurem transparência, participação e limites claros ao uso da vigilância algorítmica.

Assim, reafirma-se que a dignidade da pessoa humana, fundamento da República (CF/88, art. 1º, III), não pode ser sacrificada em nome de uma eficiência aparente, sob pena de esvaziamento do projeto emancipatório constitucional.

4 A EFICÁCIA DA SUSPEITA: UMA ANÁLISE DOS DADOS DE TRANSPARÊNCIA DO PROGRAMA SMART SAMPA

4.1 APRESENTAÇÃO DA FONTE DE DADOS E DELIMITAÇÃO METODOLÓGICA

O presente capítulo estabelece a análise empírica dos dados estatísticos oficiais do Programa Smart Sampa. A investigação fundamenta-se no *Relatório de Transparência – Programa Smart Sampa*, documento técnico emitido pela Secretaria Municipal de Segurança Urbana (SMSU), que abrange o período de 21 de novembro de 2024 a 21 de maio de 2025, correspondente aos seis primeiros meses de funcionamento do sistema.

A metodologia adotada estrutura-se em dois eixos analíticos complementares. O primeiro corresponde à análise interna dos dados do relatório, destinada a identificar padrões, inconsistências, omissões e contradições. O segundo consiste no cruzamento dos dados apresentados com fontes externas, especialmente de indicadores demográficos e socioeconômicos da cidade, a fim de contextualizar empiricamente os resultados e revelar eventuais padrões de seletividade territorial e social.

Dessa forma, a análise pretende verificar se as evidências apresentadas confirmam, tensionam ou contradizem as hipóteses teóricas sobre racismo estrutural e ofensa ao direito fundamental de não discriminação que sustentam a presente investigação. A leitura dos dados estatísticos do programa ultrapassa o mero exercício técnico, pois traduz a atuação estatal em indicadores de política pública, permitindo avaliar sua efetividade à luz da Constituição.

4.2 APRESENTAÇÃO DE DADOS

O núcleo de análise é o universo de dados disponíveis sobre abordagens e prisões decorrentes do programa de reconhecimento facial do município de São Paulo, referentes ao período compreendido entre 21 de novembro de 2024 e 21 de maio de 2025. O documento oficial explicita que:

> "O presente Relatório de Transparência tem como objetivo apresentar os dados consolidados do Programa Smart Sampa no período compreendido entre 21 de novembro de 2024 e 21 de maio de 2025, intervalo que marca os primeiros seis meses de operação do sistema de reconhecimento facial implementado na cidade de

> São Paulo. Os dados aqui apresentados abrangem a utilização do reconhecimento facial para a identificação de procurados e foragidos da Justiça, com base nos seguintes indicadores:
>
> - Número de pessoas presas por inconsistência do reconhecimento facial;
> - Número de pessoas abordadas, conduzidas à delegacia de polícia e presas;
> - Número de pessoas abordadas e liberadas no local (sem condução à delegacia);
> - Número de pessoas abordadas, conduzidas à delegacia e liberadas
>
> "(Secretaria Municipal de Segurança Urbana de São Paulo, 2025).

4.3 PERÍODO E QUANTIDADE TOTAL DE ABORDAGENS

Durante os primeiros seis meses de operação, o Programa Smart Sampa registrou um volume operacional significativo. O relatório apresenta os seguintes dados consolidados sobre o número total de abordagens:

"[...] foram registradas 1.246 (mil duzentos e quarenta e seis) pessoas abordadas [...]"

(Secretaria Municipal de Segurança Urbana de São Paulo, 2025, p. 5).

Esse número, embora apresentado como indicador de eficiência, revela a dimensão do risco constitucional de submissão massiva da população a procedimentos coercitivos. A ausência de lei formal que discipline tais abordagens torna a prática incompatível com o princípio da reserva legal e afronta a presunção de inocência prevista no art. 5º, LVII, da CF/88.

Tabela 1 – Distribuição por cor nas abordagens do Programa Smart Sampa (21/11/2024 – 21/05/2025)

Categoria	Branca (%)	Parda (%)	Preta (%)
Total de abordagens (mandado)	38,95	44,99	16,06

Fonte de dados: SECRETARIA MUNICIPAL DE SEGURANÇA URBANA DE SÃO PAULO. Relatório de Transparência do Programa Smart Sampa. São Paulo: SMSU, 2025, p. 5, 7, 13-16.[7]

A distribuição por cor evidencia a seletividade racial da política de segurança: pessoas negras aparecem sobrerrepresentadas em relação à sua participação demográfica na cidade. Esse descompasso não é neutro estatisticamente, mas sim a expressão do racismo estrutural que atravessa o sistema penal, em afronta direta ao princípio da igualdade material previsto no art. 5º da Constituição.

No que se refere à distribuição por cor declarada no mandado, os dados revelam a seguinte composição:

> "16,01% Branca;
> 18,49% Parda;
> 6,60% Preta;
> 58,90% N/C (Nada Consta)"
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA DE SÃO PAULO, 2025, p. 7).

A expressiva presença da categoria "Nada Consta" limita a precisão do mapeamento racial, mas os percentuais identificados já indicam a presença da seletividade racial no exame do programa.

Entre os casos de pessoas conduzidas ao distrito policial e posteriormente liberadas por inconsistência cadastral no Banco Nacional de Mandados de Prisão, com um total de 53 pessoas, o relatório aponta:

> "Branca – 10 pessoas;
> Parda – 6 pessoas;
> Preta – 2 pessoas;
> N/C – 35 pessoas"
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA DE SÃO PAULO, 2025, p. 13).

[7] Para fins analíticos, optou-se por excluir a categoria "Nada Consta (N/C)", recalculando as proporções do total de abordagens entre as categorias raciais Branca, Parda e Preta. Essa escolha visa evidenciar a distribuição real entre os grupos raciais identificados, evitando que a elevada presença da categoria "N/C" distorça a análise comparativa.

De forma semelhante, entre as pessoas liberadas por Erro no Reconhecimento facial, os dados registram:

> "Branca – 4 pessoas;
> Parda – 8 pessoas;
> Preta – 2 pessoas;
> N/C – 9 pessoas"
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA DE SÃO PAULO, 2025, p. 14).

Tais informações quantitativas, ainda que limitadas pela alta incidência da categoria "N/C", permitem identificar tendências de seletividade racial nos erros do sistema. A recorrência de abordagens indevidas contra pessoas pardas e pretas, reforça a necessidade de investigação crítica da tecnologia à luz do racismo estrutural e dos princípios constitucionais de igualdade e não discriminação. Os dados serão melhor apresentados adiante

Esses erros não podem ser tratados como meras falhas operacionais. Quando transformam probabilidades algorítmicas em constrangimentos físicos, configuram violação ao devido processo legal e ao direito fundamental à liberdade de locomoção (art. 5º, XV, CF/88). O erro estatal automatizado adquire, portanto, gravidade constitucional.

4.4 NARRATIVA OFICIAL

A narrativa oficial do programa aponta a suposta alta taxa de confiabilidade do sistema de reconhecimento facial com base na ausência de prisões decorrentes de inconsistências no reconhecimento facial. Conforme podemos observar adiante.

> "Do número total de pessoas abordadas, nenhuma pessoa foi presa em decorrência de inconsistência no reconhecimento facial no âmbito do Programa Smart Sampa. Isto ocorreu em virtude dos procedimentos, bem como dos aprimoramentos adotados que serão apresentados mais adiante neste relatório. "(Secretaria Municipal de Segurança Urbana de São Paulo, 2025, p. 5).

Essa afirmação, contudo, demanda leitura crítica. De fato, nenhuma pessoa poderia ser presa em decorrência de inconsistência algorítmica, uma vez que o próprio Procedimento

Operacional Padrão (POP 2025/16) do Programa Smart Sampa estabelece que, havendo qualquer dúvida quanto à identidade, a pessoa abordada deve ser conduzida obrigatoriamente à Delegacia de Polícia para verificação presencial pela autoridade competente.

> "Se confirmada a correspondência com um procurado ou foragido, ou se a identificação não puder ser concluída com segurança, a pessoa é conduzida à Delegacia de Polícia, onde passará por verificação da autoridade policial competente, utilizando sistemas oficiais de identificação" (Secretaria Municipal de Segurança Urbana de São Paulo, 2025, p. 4)

Assim, o erro reconhecimento facial não constitui o ato final que culminaria na prisão indevida, mas sim o gatilho técnico que desencadeia o processo de abordagem e verificação, deslocando a decisão para a esfera policial.

Sob essa perspectiva, o verdadeiro ponto de risco crítico não reside na "prisão por inconsistência", mas na abordagem indevida, isto é, nas intervenções estatais que se originam de falsos positivos produzidos pelo sistema.

4.5 TAXA DE ERRO

Durante o período analisado, o sistema registrou "1.246 pessoas abordadas", das quais "1.153" foram formalmente presas após confirmação de identidade e existência de mandado ativo (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, Relatório de Transparência p. 5). As outras 93 pessoas, isto é, 7,47% em dos casos, foram abordadas em decorrência de erros do sistema.

De maneira que, somando-se as 11 pessoas abordadas liberadas no local com as 82 conduzidas e liberadas, obtém-se um total de 93 erros que resultaram em intervenção estatal direta sobre o cidadão. Considerando o universo de 1.246 abordagens realizadas no período de seis meses, resulta em uma taxa real de erro de 7,47%, o que significa que aproximadamente uma em cada treze abordagens geradas pelo sistema resultou em constrangimento indevido.

Sobre os casos de liberação imediata, o documento detalha:

> "Durante o período de 21 de novembro de 2024 a 21 de maio de 2025, foram registrados 11 (onze) eventos em que, após a abordagem in loco, a pessoa apresentou documentação válida que

> justificou sua liberação imediata, sem a necessidade de condução à Delegacia de Polícia. Entre os documentos apresentados que embasaram as liberações, destacam-se: documento original com foto que comprovava a divergência da identificação; alvará de soltura vigente; contramandado judicial ou outro documento oficial que demonstrasse a inexistência de pendências judiciais ativas" (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 9).

No que se refere às 82 pessoas conduzidas e liberadas no DP, o Relatório complementa:

> "[...] foram registrados 82 (oitenta e dois) eventos em que, embora a pessoa tenha sido abordada e conduzida ao Distrito Policial (DP) com base em alerta emitido pelo sistema de reconhecimento facial do Programa Smart Sampa, a autoridade policial, após análise das circunstâncias e da documentação apresentada, decidiu pela liberação do conduzido. Deste total, 53 pessoas foram liberadas em razão da ausência de baixa de mandado no BNMP; 6 pessoas foram liberadas por inconsistência cadastral; e 23 pessoas foram liberadas por inconsistência no reconhecimento facial" (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 10).

A narrativa oficial do programa concentra-se exclusivamente no resultado da prisão, omitindo os impactos das abordagens e conduções indevidas sobre os direitos fundamentais dos cidadãos. Contudo, a análise dos dados demonstra que aproximadamente uma em cada treze abordagens iniciadas pelo sistema resultou em erro, expondo indivíduos a constrangimento indevido e violação direta ao princípio da presunção de inocência.

Esse volume, embora aparentemente modesto quando comparado ao total de abordagens presenciais realizadas na cidade, cerca de 30 mil por mês, segundo o Boletim de Segurança Pública da SSP-SP 2025, merece atenção especial, pois decorre de decisões automatizadas, cuja legitimidade repousa na precisão dos algoritmos e na eficácia da supervisão humana. Em outros termos, mesmo um número reduzido de erros adquire relevância constitucional, na medida em que evidencia o risco de arbitrariedade tecnológica no exercício do poder de polícia.

4.6 Tipos de erros operacionais decorrentes do sistema automatizado de vigilância

Além das abordagens com liberação no local foram listadas três categorias de erro identificadas no relatório: Erro no reconhecimento facial com a liberação da pessoa no local da abordagem, pessoas conduzidas à delegacia e posteriormente liberadas por falta de baixa no BNMP, por inconsistência cadastral e por inconsistência no reconhecimento facial.

A classificação dos erros revela mais do que falhas técnicas: cada ocorrência representa a materialização de um constrangimento ilegal imposto a cidadãos inocentes. A repetição desses equívocos compromete o devido processo legal e fragiliza a presunção de inocência (art. 5º, LVII, CF/88), demonstrando que a margem de falibilidade do sistema não pode ser naturalizada como mero acidente operacional.

4.7.1 liberações no local da abordagem

A primeira categoria de erro operacional refere-se às pessoas que foram abordadas com base em alertas do sistema de reconhecimento facial, mas liberadas no próprio local da abordagem, sem necessidade de condução à delegacia. O relatório oficial detalha que:

Durante o período de 21 de novembro de 2024 a 21 de maio de 2025, foram registrados 11 (onze) eventos em que, após a abordagem in loco, a pessoa apresentou documentação válida que justificou sua liberação imediata, sem a necessidade de condução à Delegacia de Polícia. (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 9).

Esses 11 casos representam falsos positivos que geram intervenção estatal coercitiva baseada em erro do sistema. Embora não tenham resultado em condução à delegacia, essas abordagens constituem uma forma de constrangimento e violação da presunção de inocência, especialmente quando motivadas por identificação algorítmica incorreta. A abordagem policial, mesmo quando não resulta em condução, representa uma forma de exercício do poder punitivo do Estado que submete o cidadão a uma situação de suspeição e potencial humilhação pública.

4.7.2 Pessoas conduzidas e liberadas

A segunda e mais significativa categoria de erro refere-se às pessoas que foram não apenas abordadas, mas efetivamente conduzidas à delegacia e posteriormente liberadas. O relatório oficial apresenta os seguintes dados consolidados:

> “Durante o período analisado, compreendido entre 21 de novembro de 2024 e 21 de maio de 2025, foram registrados 82 (oitenta e dois) eventos em que, embora a pessoa tenha sido abordada e conduzida ao Distrito Policial (DP) com base em alerta emitido pelo sistema de reconhecimento facial do Programa Smart Sampa, a autoridade policial, após análise das circunstâncias e da documentação apresentada, decidiu pela liberação do conduzi-lo”. (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 10).

Esses 82 casos representam o núcleo concreto dos erros operacionais do sistema, pois envolveram não apenas a abordagem, mas também a condução coercitiva e o processo de verificação formal na delegacia. O relatório esclarece que:

> “A verificação e eventual liberação, em todos os casos, foram realizadas exclusivamente pela autoridade policial competente, conforme previsto nos protocolos legais e operacionais vigentes. “(SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 11).

4.7.2.1 Pessoas conduzidas e liberadas: por falta de baixa no BNMP

A primeira subcategoria de pessoas conduzidas a delegacia e liberadas refere-se àquelas cujas liberações decorreu da falta de atualização no Banco Nacional de Mandados de Prisão (BNMP).

Durante o período analisado, 53 pessoas foram vítimas desse tipo de erro, representando 64,6% do total de conduções indevidas.

> “Dentre o período analisado, 53 (cinquenta e três) pessoas foram abordadas e conduzidas com base em mandado de prisão que, no momento da abordagem, constava como ativo no Banco Nacional de Mandados de Prisão (BNMP)”
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 12).

4.7.2.2 Pessoas conduzidas e liberadas: Inconsistência cadastral

A segunda subcategoria refere-se às liberações motivadas por inconsistências nos dados cadastrais. O relatório explica que:

> "Casos de inconsistência cadastral ocorreram quando os dados provenientes dos bancos de dados integrados ao Smart Sampa apresentaram incoerências que comprometeram a qualidade do alerta gerado. Essas inconsistências incluem: dados pessoais divergentes entre o cadastro e a realidade da pessoa abordada; presença de duas imagens distintas associadas ao mesmo cadastro; imagem de má qualidade vinculada ao cadastro; erros no próprio mandado de prisão, como nomes trocados ou dados incompletos" (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 14).

Dentre o período analisado, 6 (seis) pessoas foram abordadas, conduzidas e liberadas por motivo de inconsistência cadastral (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 14).

Embora numericamente menor, essa categoria é particularmente reveladora das fragilidades estruturais do sistema. Os erros cadastrais demonstram problemas na qualidade e na integração das bases de dados, comprometendo a confiabilidade do sistema como um todo. A presença de "duas imagens distintas associadas ao mesmo cadastro" ou "imagem de má qualidade vinculada ao cadastro" revela falhas básicas na curadoria dos dados que alimentam o algoritmo.

O perfil demográfico dos 6 liberados por inconsistência cadastral mostra:

Em relação ao gênero:

> "05 pessoas (9,43%);
> Masculino: 48 pessoas (90,57%) "
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 13).

Em relação à cor:

> "Branca: 03 pessoas;
> Parda: 01 pessoas;

> Preta: 01 pessoas;
> N/C*: 01 pessoas “
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 14).

4.7.2.3 Pessoas conduzidas e liberadas: inconsistência no reconhecimento facial

A terceira e mais crítica subcategoria corresponde às abordagens, conduções e liberações decorrentes de inconsistências diretas no reconhecimento facial, constituindo o núcleo empírico mais relevante para a análise do viés racial algorítmico e de suas implicações constitucionais. Essa categoria representa os falsos positivos em sua forma mais direta, nos quais o algoritmo identifica incorretamente uma pessoa como “procurada”, desencadeando toda a cadeia de intervenção estatal até que a autoridade policial, somente após a condução à delegacia e a realização de procedimentos presenciais de identificação é que a autoridade policial constata o erro.

> “Mesmo seguindo o protocolo de verificação, há situações em que a semelhança facial detectada pelo sistema gera dúvidas no momento da abordagem, como por exemplo: a pessoa abordada não portava documento de identidade ou o documento não era válido; o documento apresentado era cópia simples ou não autenticada; a imagem de referência era de baixa qualidade, dificultando a verificação manual[...]” (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 15)

Do universo de 1.246 vezes que o sistema acionou a atuação estatal, 23 pessoas foram abordadas, conduzidas à delegacia e, posteriormente, liberadas em razão de inconsistências no reconhecimento facial, o que representa aproximadamente 1,85% do total de acionamentos. De maneira que 1 em cada 54 acionamentos ocorreram de maneira indevida por erro do sistema.

Essa perspectiva se mostra mais crítica quando observamos que 71,43% dos casos com dados de cor disponíveis ocorreram com pessoas negras. Em termos práticos, isso significa que por aproximação 1 em cada 78 acionamentos resultou em uma abordagem indevida de uma pessoa negra.

O perfil demográfico desses casos apresenta características específicas.

Quanto ao Gênero:

> “Feminino – 1 pessoa (4,35%);
> Masculino – 22 pessoas (95,65%)”
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 15).

Distribuição territorial:

> “24º DP Ponte Rasa – 5 pessoas;
> 8º DP Brás/Belém – 5 pessoas;
> 73º DP Jaçanã – 2 pessoas. “
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 15).

Quanto a cor:

> “Branca – 4 pessoas;
> Parda – 8 pessoas;
> Preta – 2 pessoas;
> N/C – 9 pessoas “
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 15).

A leitura quantitativa desses dados, quando comparada com indicadores demográficos oficiais (IBGE, Censo 2022), revela correlações que contradizem a narrativa institucional de neutralidade tecnológica. O cruzamento demonstra que as pessoas negras, pretas e pardas, concentram 71,43% dos erros por inconsistência facial, percentual significativamente superior à sua representatividade na população paulistana (43,5%).

Tabela 2 – Comparativo do perfil racial: População de SP vs. dados do Smart Sampa.

Grupo	População de São Paulo (Censo 2022)	Presos pelo Smart Sampa (dados válidos)	Erros do Smart Sampa (Inconsistência Facial)

Pessoas Negras (Pretas + Pardas)	43,5%	60,97%	71,43%
Pessoas Brancas	54,3%	38,82%	28,57%

Fonte: Elaboração própria a partir do Relatório de Transparência (p. 8, 16) e dados do IBGE/O Globo [1]. Os percentuais do Smart Sampa excluem os registros "N/C (Não consta a informação de raça na base de dados)" para permitir a comparação.

> "*Observação Sobre 'N/C – Nada Consta': Algumas categorias de informação apresentadas neste relatório podem conter registros classificados como N/C (Nada Consta). Isso significa que o dado correspondente não foi informado no mandado de prisão do Banco Nacional de Mandados de Prisão (BNMP). É importante esclarecer que o BNMP é gerenciado pelo Conselho Nacional de Justiça (CNJ) e alimentado diretamente pelos tribunais de justiça estaduais. Dessa forma, caso o mandado não contenha todas as informações necessárias, esses dados não estarão disponíveis para consulta. Como a Secretaria Municipal de Segurança Urbana não possui ingerência sobre o conteúdo inserido nesse banco de dados, essa ausência reflete neste relatório com a indicação 'Nada Consta'." (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 7).

Os dados analisados reforçam, de forma inequívoca, as teses e evidências apresentadas nas seções anteriores, demonstrando que o Programa Smart Sampa reproduz padrões estruturais de seletividade racial e territorial historicamente observados nas práticas de policiamento urbano brasileiro. A concentração de erros em regiões periféricas e a desproporcionalidade racial, em que 71,43% das vítimas de inconsistência facial são pessoas negras (pretas e pardas), embora representem 43,5% da população paulistana, evidenciam que o sistema de reconhecimento facial não é neutro, mas atua como extensão digital das assimetrias sociais e raciais. Esse fenômeno converge com os resultados do estudo *Gender Shades* de Buolamwini e Gebru (2018), que identificou taxas de erro de até 34,7% em mulheres negras, frente a apenas 0,8% em homens brancos, e com os relatórios do NIST (2019), que demonstraram que

algoritmos de reconhecimento facial apresentam até cem vezes mais falsos positivos para rostos de pessoas negras e asiáticas.

4.8 SUBNOTIFICAÇÃO RACIAL

O *Relatório de Transparência* revela uma lacuna significativa na coleta de dados raciais, apontando que 58,90% dos registros de pessoas presas não possuem informação sobre cor ou raça, omissão atribuída a falhas no *Banco Nacional de Mandados de Prisão (BNMP)*. Essa ausência de dados, no entanto, transcende uma limitação técnica, pois na prática funciona como um mecanismo de opacidade institucional, que impossibilita a realização de uma auditoria precisa sobre o viés racial do sistema de reconhecimento facial.

Conforme consta no próprio relatório:

> “Branca: 16,01%;
> Parda: 18,49%;
> Preta: 06,60%;
> N/C*: 58,90%.”
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 8).

O relatório esclarece que a sigla "N/C" significa "Nada Consta", explicando que:

> “Algumas categorias de informação apresentadas neste relatório podem conter registros classificados como N/C (Nada Consta). Isso significa que o dado correspondente não foi informado no mandado de prisão do Banco Nacional de Mandados de Prisão (BNMP). É importante esclarecer que o BNMP é gerenciado pelo Conselho Nacional de Justiça (CNJ) e alimentado diretamente pelos tribunais de justiça estaduais. Dessa forma, caso o mandado não contenha todas as informações necessárias, esses dados não estarão disponíveis para consulta. Como a Secretaria Municipal de Segurança Urbana não possui ingerência sobre o conteúdo inserido nesse banco de dados, essa ausência reflete neste relatório com a indicação "Nada Consta" (BRASIL, 2025, p. 8).

Sob esta ótica, em um país estruturalmente racista, a ausência de dados raciais em um sistema de vigilância em massa não é uma mera omissão burocrática, mas uma barreira que protege o sistema de um escrutínio mais rigoroso. A subnotificação racial torna impossível a plena fiscalização da conformidade do sistema com o princípio constitucional da igualdade, criando uma zona de imunidade que permite a perpetuação de práticas discriminatórias sob o manto da suposta neutralidade técnica.

4.9 LOCALIZAÇÃO TERRITORIAL DOS ERROS

A análise da distribuição territorial dos erros de reconhecimento facial evidencia padrões estatisticamente relevantes. Observa-se concentração de falhas em delegacias específicas, com destaque para:

> "- 24º *DP Ponte Rasa*: 5 casos (21,7% dos erros faciais);
> - 8º *DP Brás/Belém*: 5 casos (21,7% dos erros faciais). [...]"
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 8).

De forma particularmente significativa, o 8º DP Brás/Belém aparece simultaneamente como a unidade com o maior número de prisões (238 pessoas) e como uma das líderes em erros de reconhecimento facial (5 casos). Essa sobreposição revela que a intensidade da vigilância em determinadas regiões urbanas não apenas eleva o número de capturas, mas também amplia a probabilidade de erros, expondo os moradores e transeuntes desses territórios a um duplo risco: o de serem corretamente identificados e o de serem indevidamente reconhecidos pelo sistema.

Essa correlação reforça a hipótese de seletividade territorial da vigilância tecnológica, na qual o aparato algorítmico reproduz, sob forma digital, as mesmas lógicas históricas de concentração policial em áreas de maior vulnerabilidade socioeconômica, intensificando a desigualdade no exercício do poder de polícia.

4.10 PRISÕES EFETIVADAS: PERFIL QUANTITATIVO E TIPOLÓGICO

Do total de 1.246 pessoas abordadas, o sistema resultou em 1.153 prisões efetivadas. O relatório detalha que:

> “Durante o período compreendido, o Programa Smart Sampa registrou 1.153 (mil cento e cinquenta e três) casos de pessoas conduzidas ao Distrito Policial (DP) e formalmente presas após a confirmação de identidade e existência de mandado de prisão ativo. Essas prisões decorreram de abordagens realizadas conforme o Procedimento Operacional Padrão (POP), após validação manual da similaridade facial superior a 90% entre a imagem captada pelas câmeras e os registros dos bancos de dados integrados ao sistema “ (BRASIL, 2025, p. 6).

A análise da natureza dos crimes que motivaram as prisões revela uma concentração significativa em delitos patrimoniais e relacionados ao tráfico de drogas. Conforme os dados da página 6 do relatório, os três tipos criminais mais frequentes foram: Art. 157 (Roubo) com 153 pessoas (13,3%), Art. 33 da Lei 11.343/06 (Tráfico de Drogas) com 137 pessoas (11,9%) e Art. 155 (Furto) com 82 pessoas (7,1%). Essa distribuição não é neutra; ela reflete a seletividade penal já documentada na literatura criminológica brasileira, que historicamente concentra a repressão estatal sobre crimes patrimoniais e de drogas, frequentemente associados a populações em situação de vulnerabilidade socioeconômica.

4.11 PERFIL DEMOGRÁFICO DOS PRESOS: GÊNERO

O perfil demográfico das pessoas detidas em decorrência da operação do programa apresenta características que refletem problemas estruturais da sociedade brasileira. Em relação ao gênero, 93,58% são homens e 6,42% mulheres, reproduzindo o padrão histórico do sistema prisional brasileiro.

> “A análise do perfil da população prisional brasileira, no que tange à variável sexo, demonstra a manutenção de um padrão acentuadamente masculino. Do total de 644.794 pessoas privadas de liberdade em celas físicas, 94,18% são homens e 5,82% são mulheres. Essa sobrerrepresentação masculina é uma característica persistente ao longo de toda a série histórica do levantamento, indicando a seletividade de gênero que opera no sistema de justiça criminal. “(Ministério da Justiça e Segurança Pública. Secretaria Nacional de Políticas Penais, 2023).

O relatório apresenta dados demográficos das pessoas presas, revelando características específicas do público-alvo do sistema. Em relação ao gênero, observa-se uma concentração extrema na população masculina:

> “Feminino: 74 pessoas (6,42%);
> Masculino: 1.079 pessoas (93,58%) “
> (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 8).

A desproporção de gênero confirma a persistência do padrão histórico do sistema penal brasileiro, majoritariamente voltado ao encarceramento de jovens negros e homens pobres. Esses números reiteram que o programa não apenas identifica indivíduos, mas legitima estruturalmente um modelo de seletividade penal em desacordo com a igualdade material garantida pela Constituição.

4.12 DISTRIBUIÇÃO TERRITORIAL DAS PRISÕES

A análise da distribuição geográfica das prisões demonstra uma concentração territorial que materializa a tese da seletividade espacial da vigilância. As cinco delegacias com maior número de ocorrências respondem por 46,8% de todas as prisões, com destaque para o 8º DP Brás/Belém, que sozinho concentra 20,6% do total.

Tabela 3 – Concentração Territorial das Prisões

Distrito Policial (DP)	Nº de Presos	% do Total
8º DP Brás/Belém	238	20,6%
2º DP Bom Retiro	95	8,2%
49º DP São Mateus	78	6,8%

24º DP Ponte Rasa	69	6,0%
47º DP Capão Redondo	60	5,2%
Total Top 5	540	46,8%

Fonte: SECRETARIA MUNICIPAL DE SEGURANÇA URBANA DE SÃO PAULO. Relatório de Transparência do Programa Smart Sampa. São Paulo: SMSU, 2025, p. 7.

A análise da distribuição geográfica das prisões (p. 7) demonstra uma concentração significativa, um indicativo de policiamento seletivo. Essas cinco delegacias concentram 540 prisões, equivalentes a 46,8% do total, evidenciando uma seletividade territorial na operação do sistema.

Essas áreas correspondem a duas categorias: territórios centrais de intenso comércio popular e grande circulação de trabalhadores (Brás, Bom Retiro) e distritos periféricos nas Zonas Leste e Sul (São Mateus, Ponte Rasa, Capão Redondo), historicamente marcados por maiores índices de vulnerabilidade social. Segundo o Mapa da Desigualdade de São Paulo 2024, produzido pela Rede Nossa São Paulo, esses territórios apresentam indicadores socioeconômicos significativamente inferiores aos das áreas centrais e nobres da cidade.

4.13 CONSIDERAÇÕES PARCIAIS

A partir dos dados apresentados, constata-se que o Smart Sampa realizou 1.246 abordagens em seis meses, alcançando índice de efetividade de 92,5%. Apesar dos resultados operacionais expressivos, 82 abordagens resultaram em liberações, evidenciando 6,5% de inconsistências sendo a maioria decorrente de falhas administrativas e uma parcela menor de erros algorítmicos.

O relatório afirma, em sua página 5, que "nenhuma pessoa foi presa em decorrência de inconsistência no reconhecimento facial". Essa asserção constrói uma narrativa de precisão irreal. Contudo, uma análise agregada dos próprios dados do relatório revela uma realidade distinta. O sistema produziu um total de 93 erros operacionais que resultaram em intervenção estatal direta sobre o cidadão, conforme detalhado na Tabela 4.

Tabela 4 – Consolidação dos Erros Operacionais

Categoria do Erro	Quantidade
Pessoas abordadas e liberadas no local	11
Pessoas conduzidas ao DP e liberadas	82
Total de Erros Operacionais	93

Fonte: PREFEITURA DE SÃO PAULO. *Relatório de Transparência – Programa Smart Sampa*. São Paulo: Secretaria Municipal de Segurança Urbana, 2025, p. 9-10.

Considerando o universo de 1.246 pessoas abordadas, a taxa de erro operacional real do sistema é de 7,47%. Isso significa que, na prática, aproximadamente 1 em cada 13 abordagens iniciadas pelo sistema de reconhecimento facial foi um erro, submetendo um cidadão a uma abordagem ou condução indevida. A narrativa de "zero prisões por inconsistência" oculta os erros que ocorrem nas etapas anteriores do funil de abordagem, esvaziando o conceito de transparência ao focar apenas no resultado (a prisão) e não no processo e em seus impactos.

A análise da natureza dos crimes que motivaram as prisões revela uma concentração significativa em delitos patrimoniais e relacionados ao tráfico de drogas. Conforme os dados da página 6 do relatório, os três tipos criminais mais frequentes foram: Art. 157 (Roubo) com 153 pessoas (13,3%), Art. 33 da Lei 11.343/06 (Tráfico de Drogas) com 137 pessoas (11,9%) e Art. 155 (Furto) com 82 pessoas (7,1%). Essa distribuição não é neutra; ela reflete a seletividade penal já documentada na literatura criminológica brasileira, que historicamente concentra a repressão estatal sobre crimes patrimoniais e de drogas, frequentemente associados a populações em situação de vulnerabilidade socioeconômica.

Quanto à cor, podemos observar a tabela a seguir que correlaciona dados demográficos de raça da população de São Paulo com os dados relacionados ao Programa Smart Sampa.

Tabela 5 – Consolidação dos erros operacionais (revisão detalhada)

Grupo	População de São Paulo (Censo 2022)	Presos pelo Smart Sampa (dados válidos)	Erros do Smart Sampa (Inconsistência Facial)
Pessoas Negras (Pretas + Pardas)	43,5%	60,97%	71,43%
Pessoas Brancas	54,3%	38,82%	28,57%

Fonte: Elaboração própria a partir do Relatório de Transparência (p. 8, 16) e dados do IBGE/O Globo [1]. Os percentuais do Smart Sampa excluem os registros "N/C (Não consta a informação de raça na base de dados)" para permitir a comparação.

A análise dos dados válidos supracitados revela três fenômenos críticos:

1 **Seletividade racial nas prisões:**
Pessoas negras representam 43,5% da população da cidade, mas constituem 60,97% dos presos pelo sistema de vigilância, indicando uma sobrerrepresentação de 40% em relação à sua parcela na população. (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 16; IBGE, 2022)

2 **Viés racial de erro:**
A desproporcionalidade é ainda mais acentuada nos casos de erro. Pessoas negras compõem 71,43% das vítimas de inconsistência no reconhecimento facial. (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 15) Isso sugere que o algoritmo não apenas opera de forma seletiva, mas também erra mais frequentemente contra pessoas negras, corroborando as teses de racismo algorítmico apresentadas anteriormente.

3 **Subnotificação dados raciais:**
Os dados disponíveis, considerando os 58,90% de registros classificados como "Nada Consta", indicam a seguinte distribuição: 18,49% pardos, 16,01% brancos e 6,60%

> pretos. Essa aparente predominância de pessoas brancas, ainda que menos que a quantidade de pessoas negras, contudo, deve ser interpretada com extrema cautela, considerando a altíssima taxa de subnotificação racial. (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 14)

Em síntese, o relatório descreve um sistema que alia eficiência operacional e complexidade normativa, cuja compreensão exige análise jurídica cuidadosa nos capítulos seguintes.

A análise crítica dos dados oficiais do Programa Smart Sampa revela um conjunto de correlações que desafiam frontalmente a narrativa de eficácia, neutralidade e transparência construída pelo poder público. Os achados empíricos corroboram as hipóteses teóricas desenvolvidas no capítulo anterior, demonstrando como a vigilância tecnológica, quando implementada em uma sociedade estruturalmente desigual, tende a reproduzir e amplificar essas desigualdades sob uma nova forma.

A taxa de erro operacional de 7,47%, ocultada pela narrativa oficial, evidencia que o sistema submete regularmente cidadãos inocentes a constrangimentos desnecessários, violando o princípio da presunção de inocência. O viés racial, manifesto tanto na seletividade da captura quanto na desproporcionalidade dos erros, demonstra como o racismo estrutural se atualiza em práticas algorítmicas automatizadas. A opacidade racial sistêmica funciona como um mecanismo de imunidade que impede o pleno controle democrático sobre o sistema. Por fim, a seletividade territorial revela como a vigilância se concentra sobre espaços e populações específicas, materializando uma geografia do controle que reforça desigualdades preexistentes.

Esses achados não são meras falhas técnicas ou operacionais passíveis de correção por meio de ajustes procedimentais. Eles revelam contradições estruturais entre a promessa constitucional de igualdade e a realidade da vigilância tecnológica em uma sociedade racista.

A conjunção desses fatores sugere que o Programa Smart Sampa, tal como implementado, desafia na prática o núcleo igualitário e garantista da Constituição de 1988, convertendo-se em um vetor de aprofundamento das desigualdades que deveriam contribuir para superar.

A análise empírica, portanto, confirma as teses críticas sobre a tecnologia e o racismo algorítmico, demonstrando a necessidade urgente de uma revisão profunda não apenas dos procedimentos operacionais, mas dos próprios fundamentos que orientam a implementação de tecnologias de vigilância em massa no Brasil. O próximo capítulo sintetiza essas conclusões e suas implicações para o direito constitucional brasileiro.

5 VÍCIOS DE CONSTITUCIONALIDADE DO PROGRAMA SMART SAMPA

5.1 INTRODUÇÃO: DA PROMESSA DE SEGURANÇA AO RISCO DE INCONSTITUCIONALIDADE

O presente capítulo marca uma transição fundamental na análise do Programa Smart Sampa. Após examinar seus dados estatísticos de abordagens e funcionamento técnico e normativo nos capítulos anteriores, volta-se agora o olhar para uma análise crítica constitucional que revela a tensão entre a promessa de segurança pública e os riscos de violação às garantias fundamentais. Se o programa se apresenta como uma solução tecnológica moderna para problemas urbanos complexos, sua implementação suscita questionamentos profundos sobre sua compatibilidade com os pilares do Estado Democrático de Direito.

A centralidade do problema reside precisamente no fato de que o Smart Sampa afronta garantias constitucionais tanto formais quanto materiais. Não se trata apenas de uma questão técnica ou administrativa, mas de um conflito estrutural entre a lógica da vigilância algorítmica e os fundamentos da ordem constitucional brasileira. A pergunta que guia esta análise é: até que ponto a implementação do programa se sustenta diante dos limites constitucionais estabelecidos pela Carta de 1988?

A resposta a essa indagação exige um exame sistemático dos vícios de constitucionalidade que permeiam o programa, desde sua criação por instrumento normativo inadequado até suas implicações materiais sobre direitos fundamentais. Conforme se demonstrará, o Smart Sampa não apenas falha em observar as formas constitucionais, mas também compromete substancialmente o núcleo essencial de direitos que a Constituição visa proteger.

5.2.1 Violação ao princípio da reserva legal

O primeiro e mais evidente vício formal do Programa Smart Sampa reside na sua própria origem normativa. Instituído por meio do Decreto Municipal nº 63.552, de 4 de julho de 2024, um ato do Poder Executivo, o programa incorre em vício de inconstitucionalidade formal por violar o princípio da reserva legal, um dos pilares do Estado de Direito. Este princípio, consagrado no artigo 5º, inciso II, da Constituição Federal, "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei", estabelece que qualquer medida que restrinja direitos e garantias fundamentais deve, necessariamente, emanar de lei em sentido

estrito, ou seja, de um ato normativo aprovado pelo Poder Legislativo, órgão de representação popular.

A implementação de um sistema de vigilância biométrica em massa, que submete todos os cidadãos à coleta e ao tratamento contínuo de dados sensíveis, representa uma severa restrição aos direitos à privacidade, à intimidade e à proteção de dados. Tal medida, portanto, não poderia ser veiculada por um decreto, que é um ato normativo secundário e infralegal, mas demandaria um amplo e transparente debate democrático no âmbito do parlamento, culminando na edição de uma lei formal.

A submissão à lei, de que fala o art. 5º, II, da Constituição, não pode ser a submissão a qualquer ato do Poder Público. Há de ser um ato revestido de todas as características da lei em sentido formal, isto é, um ato normativo emanado do Poder Legislativo, segundo o processo de formação das leis previsto na Constituição. É que somente a lei formal pode inovar originariamente a ordem jurídica, criando direitos e obrigações para as pessoas. Atos normativos secundários, como decretos, regulamentos, portarias, não podem criar deveres ou proibições que a lei não estabeleceu, nem impor restrições a direitos que a lei não restringiu, sob pena de violarem o princípio da legalidade.

O vício decorre do fato de que o Programa Smart Sampa foi instituído diretamente pelo Decreto Municipal nº 63.552/2024, ato normativo do Executivo local. Ora, como observa José Afonso da Silva, "o regulamento não pode inovar na ordem jurídica, pois sua função é apenas explicitar o comando normativo da lei que regulamenta" (SILVA, 2019, p. 425).

Nesse sentido, ao criar um sistema de vigilância massiva e coleta de dados biométricos de todos os cidadãos que circulam em espaços públicos, o decreto não regulamentou lei anterior: ele inovou no ordenamento, instituindo um regime restritivo de direitos sem base em lei formal.

A distinção entre decreto e lei é clara na doutrina constitucional. Como lembra Canotilho,

> "a reserva de lei significa que determinadas matérias, especialmente as relativas aos direitos, liberdades e garantias, só podem ser reguladas por lei da Assembleia ou por decreto-lei autorizado, excluindo-se, portanto, regulamentos ou atos normativos secundários" (CANOTILHO, 2003, p. 263).

Assim, ao disciplinar diretamente a vigilância por reconhecimento facial e a integração de dados pessoais sensíveis, o município extrapolou sua competência regulamentar e violou a reserva legal.

A jurisprudência do Supremo Tribunal Federal reforça essa limitação. No Mandado de Segurança nº 24.268, o Ministro Gilmar Mendes afirmou expressamente que

> "[...]a reserva de lei formal traduz limitação ao exercício das atividades administrativas e jurisdicionais do Estado" (BRASIL, Supremo Tribunal Federal, MS 24.268/DF, Rel. Min. Gilmar Mendes, j. 13 maio 2004, DJ 10 ago. 2004).

A distinção entre decreto e lei, fundamental para a proteção dos direitos, é clara na doutrina constitucional. Corroborando essa tese, o princípio da legalidade estrita impede que atos do Poder Executivo inovem na ordem jurídica para restringir garantias fundamentais. O mestre José Afonso da Silva leciona:

> A submissão à lei, de que fala o art. 5º, II, da Constituição, não pode ser a submissão a qualquer ato do Poder Público. Há de ser um ato revestido de todas as características da lei em sentido formal, isto é, um ato normativo emanado do Poder Legislativo, segundo o processo de formação das leis previsto na Constituição. É que somente a lei formal pode inovar originariamente a ordem jurídica, criando direitos e obrigações para as pessoas. Atos normativos secundários, como decretos, regulamentos, portarias, não podem criar deveres ou proibições que a lei não estabeleceu, nem impor restrições a direitos que a lei não restringiu, sob pena de violarem o princípio da legalidade. (SILVA, 2020, p. 425).

Na mesma linha, o Ministro Alexandre de Moraes, ao delimitar o alcance do poder regulamentar, reforça que decretos não podem ser utilizados para a supressão de direitos:

> O Chefe do Poder Executivo, na edição de decretos e regulamentos, não poderá inovar na ordem jurídica, suprimindo ou alterando direitos e obrigações, legalmente previstos, pois sua função limita-se à fiel execução das leis existentes. O poder regulamentar do Presidente da República não é um poder legislativo, mas sim um poder estritamente administrativo, que lhe permite ditar normas

> com o fim de dar cumprimento às regras preexistentes na legislação. Consequentemente, o decreto não pode criar direitos ou impor obrigações que não estejam previamente estabelecidas em lei. (MORAES, 2023, p. 412).

A jurisprudência do Supremo Tribunal Federal (STF) tem sido firme em coibir excessos normativos municipais que restrinjam direitos fundamentais ou invadam a competência da União. Em casos análogos, como na Arguição de Descumprimento de Preceito Fundamental (ADPF) 449, o Tribunal declarou a inconstitucionalidade de leis municipais que proibiam serviços de transporte por aplicativo, por violação aos princípios da livre iniciativa e da competência federal para legislar sobre o tema. A lógica subjacente a essa decisão é perfeitamente aplicável ao caso do Smart Sampa: a regulação de uma atividade com impacto sistêmico sobre direitos fundamentais e que se insere em um domínio de competência federal não pode ser usurpada pelo poder local, especialmente por meio de um ato de natureza executiva.

A utilização de um ato do Executivo local para instituir uma política de vigilância tão invasiva serviu para contornar dois filtros democráticos essenciais. O primeiro é o debate público e plural que caracteriza o processo legislativo, espaço por excelência para a ponderação de interesses e a proteção de minorias. O segundo é a esfera de competência federativa adequada, que a Constituição designou à União para assegurar um tratamento uniforme e garantista a temas de relevância nacional, como a proteção de dados. Essa manobra, portanto, não apenas viola a forma, mas corrói a substância do pacto federativo e da separação de poderes, tornando a gênese do programa, por si só, um ato de afronta ao ordenamento constitucional.

5.2.2. Ausência de lei específica sobre vigilância algorítmica e uso de dados biométricos

A coleta massiva de dados biométricos, realizada sem o consentimento informado dos cidadãos, configura violação direta ao direito à privacidade (art. 5º, X, CF/88) e ao direito fundamental à proteção de dados pessoais (art. 5º, LXXIX, CF/88). O programa em questão promove uma vigilância indiscriminada sobre todos os transeuntes em espaços públicos, registrando e processando suas características faciais sem qualquer fundamentação individualizada que justifique tal medida. Essa prática transforma a exceção na busca por criminosos procurados em regra, submetendo a coletividade a um monitoramento constante e desproporcional.

A lacuna normativa em relação ao uso de dados biométricos para vigilância pública constitui um segundo vício formal significativo. Embora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e a Emenda Constitucional nº 115/2022, que elevou a proteção de dados a direito fundamental, tenham estabelecido marcos importantes, ainda não existe legislação específica que discipline o uso de reconhecimento facial pelo poder público para fins de segurança.

Essa ausência de regulamentação específica é particularmente problemática considerando-se a natureza sensível dos dados biométricos e o potencial discriminatório da Tecnologia De Reconhecimento Facial. A LGPD, embora aplicável, foi concebida primordialmente para regular o tratamento de dados por particulares, não contemplando adequadamente as especificidades e os riscos da vigilância algorítmica estatal.

A conexão com a Emenda Constitucional nº 115/2022 é fundamental, pois ela inseriu no artigo 5º da Constituição o inciso LXXIX, que garante a proteção de dados pessoais como direito fundamental. Essa elevação de status constitucional reforça a necessidade de lei específica para disciplinar o uso de tecnologias invasivas como o reconhecimento facial, especialmente quando empregadas pelo poder público.

5.3 VÍCIOS MATERIAIS: AFRONTA A DIREITOS FUNDAMENTAIS

5.3.1 Igualdade e não discriminação

Este é o argumento central que demonstra a mais grave inconstitucionalidade do Programa Smart Sampa. Longe de ser uma ferramenta neutra de segurança, o sistema opera como um potente mecanismo de discriminação racial, violando frontalmente o objetivo fundamental da República de "promover o bem de todos, sem preconceitos de origem, raça, [...] cor [...] e quaisquer outras formas de discriminação" (art. 3º, IV) e o princípio da isonomia (art. 5º, caput).

O princípio da igualdade (art. 5º, caput, CF/88) e o objetivo fundamental de promover o bem de todos, sem preconceitos de raça ou cor (art. 3º, IV, CF/88), são violados pelo racismo algorítmico inerente aos sistemas de reconhecimento facial. A Constituição também tipifica o racismo como crime inafiançável e imprescritível (art. 5º, XLII), o que torna ainda mais grave a adoção de uma tecnologia com viés discriminatório comprovado.

A ADPF 635 (Caso das Milícias do Rio de Janeiro) é particularmente relevante por abordar o racismo estrutural em políticas de segurança. O STF reconheceu que "práticas

discriminatórias em políticas de segurança pública violam o princípio da igualdade e perpetuam injustiças históricas" (STF, ADPF 635, Rel. Min. Edson Fachin).

Estudos técnicos demonstram que algoritmos de reconhecimento facial apresentam taxas de erro significativamente maiores para pessoas negras, especialmente mulheres. O estudo "Gender Shades", conduzido por Joy Buolamwini e Timnit Gebru, revelou que enquanto a taxa de erro para homens brancos era de 0,8%, para mulheres negras chegava a 34,7%. Em uma sociedade estruturalmente racista como a brasileira, essa disparidade técnica se traduz em discriminação institucionalizada.

O viés estrutural nos falsos positivos contra pessoas negras significa que essas pessoas têm maior probabilidade de serem erroneamente identificadas como procuradas, resultando em abordagens policiais indevidas. Isso perpetua e automatiza padrões de discriminação racial, contrariando frontalmente os mandamentos constitucionais de igualdade e não discriminação.

A materialização dessa violação é inequivocamente demonstrada pela análise empírica dos dados oficiais do próprio programa, apresentados no Capítulo 4. A articulação desses dados com o arcabouço teórico do racismo algorítmico revela um padrão sistêmico de tratamento desigual. Os indicadores mais alarmantes são:

1. **Viés Racial de Erro:** Pessoas negras (a soma de pretos e pardos) representam 71,43% das vítimas de erros de identificação por inconsistência facial, embora constituam apenas 43,5% da população da cidade de São Paulo (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 15; IBGE, 2022). Este dado é a evidência empírica de que a tecnologia não é neutra e falha desproporcionalmente em detrimento da população negra, confirmando no contexto local os achados de estudos internacionais como o *Gender Shades*.
2. **Viés Racial de Captura:** Mesmo nos casos de acerto, o sistema demonstra uma seletividade racial. Pessoas negras correspondem a 60,97% do total de presos identificados pelo programa, uma sobrerrepresentação de mais de 40% em relação à sua participação demográfica (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 16; IBGE, 2022). Isso indica que o sistema está sendo implementado de forma a amplificar os padrões de policiamento seletivo já existentes.
3. **Opacidade Institucional como Mecanismo de Discriminação:** A alarmante taxa de 58,90% de registros de prisão sem a informação de raça/cor não é uma mera falha burocrática. Na prática, essa subnotificação funciona como um véu de opacidade que

impede o controle social e a fiscalização rigorosa do impacto racial do programa, perpetuando a discriminação ao dificultar sua comprovação.

Para visualizar a magnitude dessa disparidade, a tabela 6 abaixo consolida a análise comparativa:

Tabela 6: Análise comparativa da seletividade racial no Programa Smart Sampa

Grupo Racial	% na População de SP (IBGE/Censo 2022)	% dos Presos pelo Programa (Dados Válidos)	% das Vítimas de Erro Facial (Dados Válidos)
Pessoas Negras (Pretas + Pardas)	43,5%	60,97%	71,43%
Pessoas Brancas	54,3%	38,82%	28,57%

Fonte: IBGE. Censo Demográfico 2022: População residente por cor ou raça – Município de São Paulo. Rio de Janeiro: IBGE, 2022. SECRETARIA MUNICIPAL DE SEGURANÇA URBANA DE SÃO PAULO. Relatório de Transparência do Programa Smart Sampa. São Paulo: SMSU, 2025, p. 13-16.

Essa realidade empírica convoca a aplicação da jurisprudência do STF em matéria de controle de políticas públicas com impacto racial desproporcional. A ADPF 635, conhecida como "ADPF das Favelas", tornou-se um marco ao reconhecer que o Poder Judiciário tem o dever de intervir em políticas de segurança pública quando estas violam sistematicamente direitos fundamentais da população negra e periférica. Como afirmou o Ministro Edson Fachin, relator da ação:

> "a Constituição Federal não autoriza políticas públicas de segurança baseadas na violação sistemática de direitos fundamentais" (BRASIL, STF, ADPF 635 MC/DF, Rel. Min. Edson Fachin, j. 05 jun. 2020, p. 17).

Na mesma decisão cautelar, Fachin determinou que o Estado do Rio de Janeiro elaborasse um plano de redução da arbitrariedade policial, destacando:

> "A proteção da vida e da dignidade da população, em especial da população negra residente em comunidades periféricas, deve orientar a atuação estatal em matéria de segurança pública" (BRASIL, STF, ADPF 635 MC/DF, Rel. Min. Edson Fachin, j. 05 jun. 2020, p. 23).

A mesma lógica se aplica ao Smart Sampa: se a Corte agiu para controlar os efeitos discriminatórios do policiamento ostensivo e físico, deve, com igual ou maior rigor, controlar uma política de policiamento tecnológico que automatiza e potencializa a mesma discriminação estrutural.

5.3.2 Privacidade e proteção de dados pessoais

O direito à privacidade (art. 5º, X, CF/88) e à proteção de dados pessoais (art. 5º, LXXIX, CF/88) são violados pela coleta massiva de dados biométricos sem consentimento informado. O programa opera uma vigilância indiscriminada de todos os transeuntes em espaços públicos, coletando e processando suas características faciais sem qualquer justificativa individualizada para que seja possível compará-las aos dados de criminosos procurados.

A face humana constitui um dado biométrico e, como tal, possui proteção legal classificada como um **dado pessoal sensível**. A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) é explícita ao definir essa categoria:

> Art. 5º, II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> (Lei nº 13.709/2018)

Na ADI 5874, o STF reconheceu a importância dos dados pessoais e direitos digitais no contexto constitucional contemporâneo. A Corte enfatizou que "a proteção de dados pessoais é corolário da dignidade da pessoa humana e da privacidade" (STF, ADI 5874, Rel. Min. Rosa Weber).

A razão para essa proteção legal rigorosa é detalhada pela doutrina, que aponta para o elevado potencial discriminatório e o profundo impacto que o tratamento de tais dados pode gerar na vida do indivíduo. Bruno Bioni, um dos maiores especialistas no tema, esclarece:

> A categoria ‘dados pessoais sensíveis’ designa um conjunto de informações que, por sua natureza, revela aspectos íntimos e mais profundos da personalidade de uma pessoa ou que pode ser utilizada como um critério de distinção e de discriminação, com potencial de causar a sua estigmatização, segregação ou exclusão social. A sua utilização, portanto, representa um risco mais elevado aos direitos e liberdades fundamentais do titular. (BIONI, 2020, p. 98).

Dessa forma, o simples trânsito em via pública não pode implicar renúncia tácita ao direito à privacidade e à proteção de dados. A vigilância biométrica contínua em espaços públicos elimina o anonimato prático, essencial ao exercício de liberdades como a de manifestação e associação, transformando a esfera pública num espaço de controle. Como observa Stefano Rodotà, "a proteção de dados não é apenas uma questão técnica, mas uma questão de poder e de democracia" (RODOTÀ, 2008, p. 69).

A jurisprudência do STF, na ADI 6387, estabeleceu que o tratamento de dados pessoais pelo poder público deve observar finalidades específicas, legítimas e informadas, limitando-se ao mínimo necessário. O Smart Sampa, com sua coleta massiva e prospectiva de dados sensíveis, contraria manifestamente esses parâmetros constitucionais e legais.

Além disso, o Programa Smart Sampa realiza tratamento de dados pessoais sensíveis (biométricos) em larga escala, sem respaldo legal adequado. A LGPD, em seu artigo 11, dispõe de forma categórica:

> “O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I – Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II – Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (...).” (LGPD, BRASIL, 2018, art. 11).

Do mesmo modo, o artigo 6º da LGPD estabelece o princípio da necessidade, também chamado de minimização, segundo o qual:

> “O tratamento de dados pessoais deverá observar a boa-fé e os seguintes princípios:
> (...) III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados” (BRASIL, 2018, art. 6º, III).

Quando um programa de vigilância biométrica capta indiscriminadamente todos os cidadãos que circulam por vias públicas para identificar uma minoria, no seu caso, cerca de 1.153 prisões em seis meses (SECRETARIA MUNICIPAL DE SEGURANÇA URBANA, 2025, p. 5), essa estratégia excede o que poderia ser considerado “estritamente necessário” e se aproxima de medida desproporcional, violando o princípio da minimização.

Portanto, o Smart Sampa, ao adotar a coleta massiva e prospectiva de dados sensíveis sem consentimento e sem delimitação de finalidade, reproduz exatamente os vícios que o STF já considerou inconstitucional, violando tanto a LGPD quanto a Constituição ao comprometer os direitos fundamentais à privacidade e à proteção de dados pessoais.

5.3.3 Devido processo legal e presunção de inocência

O devido processo legal (art. 5º, LIV, CF/88) e a presunção de inocência (art. 5º, LVII, CF/88) são comprometidos pela transformação de cidadãos em suspeitos a priori. A presunção de inocência estabelece que "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória", mas o programa inverte essa lógica ao tratar todos como potenciais procurados.

A vigilância algorítmica opera uma "suspeição generalizada" que contraria o devido processo legal. Em vez de investigações baseadas em indícios concretos e individualizados, o

sistema submete toda a população a um escrutínio constante, presumindo a necessidade de vigilância universal. Isso representa uma inversão do ônus da prova: em vez de o Estado demonstrar razões específicas para investigar alguém, todos devem provar continuamente sua inocência ao sistema algorítmico.

5.3.4 Proporcionalidade

O princípio da proporcionalidade, embora implícito na Constituição, é reconhecido pela jurisprudência do STF como limitador fundamental da atividade estatal restritiva de direitos. Segundo Robert Alexy, toda medida restritiva deve ser submetida aos testes de adequação, necessidade e proporcionalidade em sentido estrito. O Programa Smart Sampa falha em todos esses níveis.

Quanto à **adequação**, não existem evidências empíricas robustas que comprovem sua eficácia na redução da criminalidade. O estudo "Smart Sampa vigia, mas não protege", elaborado pelo Centro de Estudos de Segurança e Cidadania (CESeC), avaliou os principais indicadores criminais da capital paulista e concluiu que;

> "não há evidência de que o programa de reconhecimento facial tenha tido qualquer impacto significativo sobre os níveis desses crimes na cidade de São Paulo, comparado aos outros municípios do Estado" (PANTALEÃO; NUNES, 2025, p. 9)

Nessa lógica, observa-se que existem medidas alternativas menos invasivas e mais alinhadas às garantias fundamentais, como o fortalecimento do policiamento comunitário e o investimento em inteligência investigativa tradicional. Já sob a ótica da proporcionalidade em sentido estrito, os danos impostos à coletividade, a coleta massiva de dados biométricos, risco de erros de identificação e reforço da seletividade racial, superam largamente os benefícios, que se revelaram marginais. Como sintetizam os autores do estudo.

> "o programa Smart Sampa não produziu efeitos estatisticamente significativos nos indicadores de criminalidade analisados (...) sugerindo que o reconhecimento facial tem sido mais eficaz como instrumento de propaganda política do que como política pública baseada em evidências" (PANTALEÃO; NUNES, 2025, p. 11)

Dessa forma, o programa incorre em clara violação ao princípio da proporcionalidade, por impor restrições intensas a direitos fundamentais sem oferecer contrapartida real em termos de segurança pública.

5.4 VIGILÂNCIA ALGORÍTMICA E A BANALIZAÇÃO DA VIOLÊNCIA BUROCRÁTICA

A análise do Smart Sampa não pode se limitar aos aspectos técnicos ou jurídicos formais. É necessário compreender como a vigilância algorítmica opera não apenas como risco de erro técnico, mas como normalização de práticas autoritárias que se ocultam sob o verniz da eficiência burocrática.

Hannah Arendt, em sua obra "Eichmann em Jerusalém", desenvolveu o conceito de "banalidade do mal" para explicar como atrocidades podem ser cometidas por pessoas comuns que simplesmente cumprem ordens burocráticas, sem intenção explícita de maldade. Esse conceito é particularmente relevante para compreender como sistemas de vigilância algorítmica podem perpetuar violência estrutural através de rotinas administrativas aparentemente neutras.

A violência burocrática praticada "sem intenção de maldade, mas por cumprimento de ordens" encontra no Smart Sampa um exemplo paradigmático. Os operadores de telecomunicações do sistema seguem protocolos técnicos, os gestores implementam diretrizes administrativas, e os agentes de segurança executam procedimentos padronizados. Cada um cumpre sua função dentro de uma engrenagem maior, sem necessariamente questionar as implicações mais amplas de suas ações, correndo o risco de serem responsabilizadas como tais.

A conexão com o Procedimento Operacional Padrão (POP) 16/2025 é reveladora. O documento estabelece que operador e gestor devem seguir etapas automáticas de identificação e comunicação, enquanto a abordagem coercitiva surge como "mero protocolo" a ser executado pelos agentes de campo. Essa fragmentação de responsabilidades dilui a percepção da violência inerente ao processo, transformando cada etapa em uma rotina burocrática aparentemente inocente.

O Smart Sampa transforma a suspeição em rotina administrativa, ocultando o caráter violador de direitos sob a aparência de eficiência técnica. A identificação algorítmica se apresenta como "objetiva" e "neutra", quando na verdade reproduz e amplifica vieses discriminatórios. A abordagem policial decorrente é apresentada como "procedimento padrão", quando na verdade constitui constrangimento baseado em suspeita algorítmica infundada.

Essa banalização da violência é particularmente perigosa porque normaliza práticas autoritárias, tornando-as socialmente aceitáveis. A população gradualmente se acostuma à vigilância constante, internalizando a ideia de que é normal e necessário ser monitorado pelo Estado. A resistência diminui, e o espaço democrático se contrai sem que haja uma percepção clara do processo em curso.

5.5 CONSIDERAÇÕES PARCIAIS

A análise desenvolvida neste capítulo revela que o Programa Smart Sampa padece de vícios formais e materiais que o tornam incompatível com a Constituição Federal de 1988. Os vícios formais incluem a violação ao princípio da reserva legal e a ausência de lei específica sobre vigilância algorítmica. Os vícios materiais abrangem violações à dignidade da pessoa humana, à igualdade, à privacidade, ao devido processo legal e ao princípio da proporcionalidade.

O argumento central que emerge desta análise é que o Smart Sampa é incompatível com a Constituição por violar garantias estruturais do Estado Democrático de Direito. Não se trata de meros defeitos técnicos ou administrativos que possam ser corrigidos por ajustes pontuais. O problema é estrutural e reside na própria lógica da vigilância algorítmica massiva, que é incompatível com os fundamentos constitucionais da dignidade, da igualdade e da liberdade.

A jurisprudência do STF e a doutrina constitucional de referência oferecem fundamentos sólidos para questionar a constitucionalidade do programa. Mais do que isso, a análise inspirada no conceito de "banalidade do mal" de Hannah Arendt revela como a vigilância algorítmica pode normalizar práticas autoritárias através de rotinas burocráticas aparentemente neutras.

Essa constatação aponta para a necessidade de limites normativos rigorosos, participação democrática efetiva e controle constitucional rígido para evitar a consolidação de um modelo de vigilância autoritária. O próximo capítulo explorará essas alternativas e apresentará as considerações finais do trabalho, enfatizando a importância de preservar o espaço democrático diante dos desafios impostos pelas novas tecnologias de controle social.

6 CONCLUSÃO

A presente pesquisa analisou criticamente a implementação do Programa Smart Sampa, instituído pela Prefeitura de São Paulo, à luz dos princípios constitucionais da igualdade, da dignidade da pessoa humana e do devido processo legal. Partindo da hipótese de que o uso do reconhecimento facial no espaço público reforça práticas de racismo estrutural sob a aparência de neutralidade tecnológica, buscou-se verificar a compatibilidade dessa política com a Constituição de 1988.

Ao longo do trabalho, foi demonstrado que o reconhecimento facial opera em um ambiente já marcado pela seletividade penal e pelo racismo institucional, como revelam os dados da população carcerária e a sobrerrepresentação de pessoas negras nas abordagens do programa. A análise teórica, fundamentada em autores como Foucault, Deleuze e Silvio Almeida, evidenciou que a vigilância algorítmica se insere em uma lógica de sociedade de controle, na qual a suspeição é automatizada e potencializa a discriminação racial.

O exame dos dados oficiais obtidos por meio da Lei de Acesso à Informação confirmou a existência de inconsistências técnicas e de erros operacionais que recaíram majoritariamente sobre a população negra. Entre os resultados, destacam-se as elevadas taxas de falsos positivos, a subnotificação racial e a concentração territorial das prisões em regiões periféricas e vulneráveis da cidade. Esses achados reforçam a hipótese de que a tecnologia não atua em um vácuo, mas amplia seletividades já estruturais do sistema penal brasileiro.

Do ponto de vista jurídico-constitucional, a pesquisa apontou vícios formais e materiais do Programa Smart Sampa. No plano formal, a instituição por decreto municipal afronta o princípio da reserva legal. No plano material, a coleta massiva de dados biométricos sem consentimento informado, somada à reprodução de vieses algorítmicos discriminatórios, compromete direitos fundamentais de privacidade, igualdade e não discriminação.

Dessa forma, conclui-se que a implementação do reconhecimento facial no Programa Smart Sampa não se mostra compatível com o projeto emancipatório da Constituição de 1988. Em vez de promover segurança e eficiência, o programa reforça desigualdades raciais e fragiliza garantias fundamentais. A principal contribuição deste trabalho é demonstrar, a partir de análise teórica e empírica, que o uso de tecnologias de vigilância sem regulação específica e controle democrático aprofunda o racismo estrutural e coloca em risco a consolidação do Estado Democrático de Direito.

REFERENCIAS

AGAMBEN, Giorgio. *Estado de exceção*. São Paulo: Boitempo, 2004.

AGÊNCIA BRASIL. SP abre central de vigilância de câmeras com reconhecimento facial. Brasília: Empresa Brasil de Comunicação – EBC, 4 jul. 2024. Disponível em: https://agenciabrasil.ebc.com.br/. Acesso em: 6 out. 2025.

ALEXY, Robert. *Teoria dos direitos fundamentais*. 2. ed. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2011.

ALMEIDA, Silvio Luiz de. *Racismo estrutural*. São Paulo: Pólen, 2019.

ARENDT, Hannah. *Eichmann em Jerusalém: um relato sobre a banalidade do mal*. São Paulo: Companhia das Letras, 1999.

BARROSO, Luís Roberto. *Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo*. 9. ed. São Paulo: Saraiva, 2020.

BIONI, Bruno. *Proteção de dados pessoais: a função e os limites do consentimento*. 4. ed. Rio de Janeiro: Forense, 2020.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Senado Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais. *Diário Oficial da União*, Brasília, 2022.

BRASIL. Lei nº 12.288, de 20 de julho de 2010. Institui o Estatuto da Igualdade Racial. *Diário Oficial da União*, Brasília, 2010.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações (Lei de Acesso à Informação – LAI). *Diário Oficial da União*, Brasília, 2011.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Recomendação nº 20, de 14 de setembro de 2023. Dispõe sobre o uso de tecnologias analíticas de imagem no contexto do Programa Smart Sampa. *Participa + Brasil*, Brasília, 2023. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/30979. Acesso em: 6 out. 2025.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade 5.874/DF*. Rel. Min. Edson Fachin, julgado em 12 set. 2018. Disponível em: https://portal.stf.jus.br. Acesso em: 10 out. 2025.

BUOLAMWINI, Joy; **GEBRU**, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: *Conference on Fairness, Accountability, and Transparency*, 2018, New York. Proceedings... New York: PMLR, 2018. p. 77-91.

CANOTILHO, J. J. Gomes. *Direito constitucional e teoria da constituição*. 7. ed. Coimbra: Almedina, 2003.

CNN BRASIL. Reconhecimento facial em São Paulo levanta polêmica. *CNN Brasil*, São Paulo, 2025. Disponível em: https://www.cnnbrasil.com.br/. Acesso em: 6 out. 2025.

CNN BRASIL. Prefeitura de SP integra 5,3 mil câmeras privadas ao Smart Sampa. São Paulo: CNN Brasil, 2025. Disponível em: https://www.cnnbrasil.com.br/. Acesso em: 6 out. 2025

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. In: _____. *Conversações*. Rio de Janeiro: Ed. 34, 1992. p. 219-226.

EL PAÍS. São Paulo testa câmeras inteligentes do Smart Sampa. *El País*, São Paulo, 2025. Disponível em: https://brasil.elpais.com/. Acesso em: 6 out. 2025.

L PAÍS. São Paulo, un gran hermano de 25.000 cámaras y reconocimiento facial contra el crimen. El País, São Paulo, 2025. Disponível em: https://brasil.elpais.com/. Acesso em: 6 out. 2025

FERRAJOLI, Luigi. *Direito e razão: teoria do garantismo penal*. 2. ed. São Paulo: Revista dos Tribunais, 2002.

FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*. 42. ed. Petrópolis: Vozes, 2014.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA (FBSP). *Anuário brasileiro de segurança pública 2024*. São Paulo: FBSP, 2024. Disponível em: https://forumseguranca.org.br/. Acesso em: 6 out. 2025.

FRASER, Nancy. *Redistribuição ou reconhecimento?*. Rio de Janeiro: Record, 2006.

HABERMAS, Jürgen. *Direito e democracia: entre facticidade e validade*. Rio de Janeiro: Tempo Brasileiro, 1997.

MBEMBE, Achille. Necropolítica. *Arte & Ensaios*, Rio de Janeiro, n. 32, p. 123–151, dez. 2016.

NIST. *Face Recognition Vendor Test (FRVT) – Performance Reports*. Gaithersburg: National Institute of Standards and Technology, 2022. Disponível em: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt. Acesso em: 6 out. 2025.

NTECHLAB. *FindFace Multi – Documentation*. Moscou: NtechLab, 2024. Disponível em: https://ntechlab.com/press/ntechlab-launches-findface-multi-a-multi-object-recognition-platform-that-detects-faces-and-bodies-of-people-as-well-as-cars/. Acesso em: 6 out. 2025.

PREFEITURA DE SÃO PAULO. *Relatório de Transparência – Programa Smart Sampa*. São Paulo: Secretaria Municipal de Segurança Urbana, 2025. Disponível em: https://smartsampa.prefeitura.sp.gov.br/relatorio_transparencia_smart_sampa.pdf. Acesso em: 6 out. 2025.

PREFEITURA DE SÃO PAULO. *Smart Sampa – O maior sistema de monitoramento de segurança da América Latina*. São Paulo: Prefeitura de São Paulo, 2024. Disponível em: https://smartsampa.prefeitura.sp.gov.br/. Acesso em: 6 out. 2025.

REDE NOSSA SÃO PAULO. *Mapa da desigualdade de São Paulo 2024*. São Paulo: Rede Nossa São Paulo, 2024. Disponível em: https://www.nossasaopaulo.org.br/. Acesso em: 6 out. 2025.

RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*. 12. ed. Porto Alegre: Livraria do Advogado, 2015.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 13. ed. Porto Alegre: Livraria do Advogado, 2019.

SÃO PAULO (Município). Decreto nº 63.552, de 4 de julho de 2024. Institui o Programa Smart Sampa. *Diário Oficial da Cidade de São Paulo*, São Paulo, 5 jul. 2024. Disponível em: https://legislacao.prefeitura.sp.gov.br/leis/decreto-63552-de-4-de-julho-de-2024. Acesso em: 6 out. 2025.

SÃO PAULO (Município). Decreto Municipal nº 63.552, de 20 de maio de 2024. Institui o Programa Smart Sampa. Diário Oficial da Cidade de São Paulo, São Paulo, SP, 21 maio 2024.

SÃO PAULO (Município). Projeto de Lei nº 01-00166/2025. Dispõe sobre a instalação de câmeras de monitoramento em logradouros públicos sob o Programa Smart Sampa. Câmara Municipal de São Paulo, 2025. Disponível em: https://www.saopaulo.sp.leg.br/iah/fulltext/projeto/PL0166-2025.pdf. Acesso em: 6 out. 2025

SÃO PAULO (Município). Secretaria Municipal de Segurança Urbana. Relatório de Impacto à Proteção de Dados (RIPD). São Paulo: SMSU, 2025

SÃO PAULO (Município). Edital de Chamamento Público – Programa Smart Sampa. Secretaria Municipal de Segurança Urbana, 5 jul. 2024. Disponível em: https://www.sinesp.org.br/legislacao/saiu-no-doc-legislacao/19658-edital-de-chamamento-publico-secretaria-municipal-de-seguranca-urbana-programa-smart-sampa-05-07-2024. Acesso em: 6 out. 2025

SÃO PAULO (Município). Secretaria Municipal de Inovação e Tecnologia. Edital de Concorrência nº 01/SMIT/2023 – Contratação de Solução de Plataforma de Videomonitoramento Urbano Inteligente (Smart Sampa): Anexo I – Termo de Referência. São Paulo: SMIT, 2023. Disponível em:

https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/inovacao/Edital_VF__1.pdf. Acesso em: 6 out. 2025

SÃO PAULO (Município). Secretaria Municipal de Segurança Urbana. POP 16/2025: Procedimento Operacional Padrão – Despacho de Ocorrências e Monitoramento por Câmeras. Versão 1.0. São Paulo: SMSU/GCM, 2025

SÃO PAULO (Município). Edital de Chamamento Público – Programa Smart Sampa. Secretaria Municipal de Segurança Urbana, 5 jul. 2024. Disponível em: https://www.sinesp.org.br/legislacao/saiu-no-doc-legislacao/19658-edital-de-chamamento-publico-secretaria-municipal-de-seguranca-urbana-programa-smart-sampa-05-07-2024. Acesso em: 6 out. 2025.

SÃO PAULO (Município). Edital de Concorrência nº 01/SMIT/2023 – Contratação de Solução de Plataforma de Videomonitoramento Urbano Inteligente (Smart Sampa): Anexo I – Termo de Referência. São Paulo: Secretaria Municipal de Inovação e Tecnologia, 2023. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/inovacao/Edital_VF__1.pdf. Acesso em: 6 out. 2025.

SÃO PAULO (Município). Portaria Conjunta SME/SMSU nº 04, de 12 de dezembro de 2024. *SINESP*, São Paulo, 2024. Disponível em: https://www.sinesp.org.br/legislacao/saiu-no-doc-legislacao/20898-portaria-conjunta-sme-smsu-sp-n-04-de-12-12-2024. Acesso em: 6 out. 2025.

SÃO PAULO (Município). Portaria SGM nº 180, de 6 de setembro de 2024. *SINESP*, São Paulo, 2024. Disponível em: https://www.sinesp.org.br/legislacao/saiu-no-doc-legislacao/20150-portaria-sgm-n-180-de-06-09-2024-designa-representantes-para-compor-o-conselho-de-gestao-e-transparencia-do-programa-smart-sampa. Acesso em: 6 out. 2025.

SÃO PAULO (Município). Projeto de Lei nº 01-00166/2025. Dispõe sobre a instalação de câmeras de monitoramento em logradouros públicos sob o Programa Smart Sampa. *Câmara Municipal de São Paulo*, 2025. Disponível em: https://www.saopaulo.sp.leg.br/iah/fulltext/projeto/PL0166-2025.pdf. Acesso em: 6 out. 2025.

SÃO PAULO (Município). Secretaria Municipal de Segurança Urbana. *Relatório de Impacto à Proteção de Dados (RIPD)*. São Paulo: SMSU, 2025.

SECRETARIA MUNICIPAL DE SEGURANÇA URBANA. *POP 16/2025: Procedimento Operacional Padrão – Despacho de Ocorrências e Monitoramento por Câmeras*. Versão 1.0. São Paulo: SMSU/GCM, 2025.

SECRETARIA MUNICIPAL DE SEGURANÇA URBANA (São Paulo). *Procedimento Operacional Padrão nº 16/2025***.** Estabelece diretrizes de padronização setorial do Programa Smart Sampa. São Paulo: SMSU, 2025.

SEMANÁRIO ZONA NORTE. Relatório de transparência do Smart Sampa comprova eficácia do sistema de reconhecimento facial. *Semanário Zona Norte*, São Paulo, 28 jun. 2025. Disponível em: https://www.semanariozonanorte.com.br/noticia/relatorio-de-transparencia-do-smart-sampa-comprova-eficacia-do-sistema-de-reconhecimento-facial. Acesso em: 7 out. 2025.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 43. ed. São Paulo: Malheiros, 2020.

SILVA, Tarcízio. Racismo algorítmico em plataformas digitais: microagressões e discriminação em código. *Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação*, v. 22, n. 3, 2019.

SILVEIRA, Sergio Amadeu da. *Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais*. São Paulo: Edições Sesc, 2021.

TASSI, Gabriel. Smart Sampa: o polêmico projeto de IA para SP. *AgEMT*, 18 abr. 2023. Disponível em: https://agemt.pucsp.br/noticias/smart-sampa-o-polemico-projeto-de-ia-para-sp. Acesso em: 6 out. 2025.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Rio de Janeiro: Intrínseca, 2020.