



UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO ENGENHARIA DO CONHECIMENTO
CURSO DE PÓS-GRADUAÇÃO EM INTELIGÊNCIA E INOVAÇÃO NO
ENFRENTAMENTO AO CRIME ORGANIZADO

André Hiago de Amorim Santos
Denis Junio Rocha Rodrigues

Biometria Facial na Segurança Pública Brasileira: Análise Entre o Potencial Tecnológico e os Desafios Éticos e Legais para uma Implementação Democrática

Florianópolis
2026

André Hiago de Amorim Santos
Denis Junio Rocha Rodrigues

Biometria Facial na Segurança Pública Brasileira: Análise entre o potencial tecnológico e os desafios éticos e legais para uma implementação democrática

Trabalho de Conclusão de Curso submetido ao curso de Pós-Graduação em Inteligência e Inovação no Enfrentamento ao Crime Organizado do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de especialista em Inteligência e Inovação no Enfrentamento ao Crime Organizado

Orientador (a): Prof. Ronaldo David Viana Barbosa, Dr

Santos, André Hiago de Amorim
Biometria Facial na Segurança Pública Brasileira :
Análise entre o potencial tecnológico e os desafios éticos
e legais para uma implementação democrática / André Hiago
de Amorim Santos, Denis Junio Rocha Rodrigues ;
orientador, Ronaldo David Viana Barbosa, 2026.
36 p.

Monografia (especialização) - Universidade Federal de
Santa Catarina, Centro Tecnológico, Curso de
Especialização Lato Sensu em Inteligência e Inovação
aplicadas no Enfrentamento ao Crime Organizado,
Florianópolis, 2026.

Inclui referências.

1. Gestão do Conhecimento. 2. reconhecimento facial. 3.
segurança pública. 4. direitos fundamentais. 5. vieses
algorítmicos. I. Rodrigues, Denis Junio Rocha. II.
Barbosa, Ronaldo David Viana . III. Universidade Federal
de Santa Catarina. Especialização Lato Sensu em
Inteligência e Inovação aplicadas no Enfrentamento ao
Crime Organizado. IV. Título.

André Hiago de Amorim Santos
Denis Junio Rocha Rodrigues

Biometria Facial na Segurança Pública Brasileira: Análise entre o potencial tecnológico e os desafios éticos e legais para uma implementação democrática

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de Inteligência e Inovação no Enfrentamento ao Crime Organizado e aprovado em sua forma final pelo Curso Pós-Graduação em Inteligência e Inovação no Enfrentamento ao Crime Organizado

Florianópolis, 06 de março de 2026.

Coordenação do Curso

Banca examinadora

Prof. Ronaldo David Viana Barbosa, Dr.
Orientador(a)

Nadjanine Galindo de Freitas Farias, Msc.
Membro da banca

Daniel Rodrigues Kinchescki, Msc
Membro da banca

Florianópolis, 2026

"O corpo eletrônico, feito de dados e informações, torna-se cada vez mais a condição necessária para a existência no mundo contemporâneo. Proteger esse corpo é proteger a própria pessoa."

(Stefano Rodotà, 2008)

RESUMO

O presente trabalho examina a aplicação da tecnologia de reconhecimento facial na segurança pública brasileira, a partir do seguinte problema de pesquisa: como conciliar as exigências éticas, a exemplo dos vieses algorítmicos, das identificações incorretas e da proteção à privacidade, e os entraves legais, especialmente a ausência de regulamentação específica e os limites de incidência da Lei Geral de Proteção de Dados, com a necessidade de ampliar os meios tecnológicos na segurança pública para aperfeiçoar o desempenho operacional estatal no combate à criminalidade. Para tanto, adota-se uma abordagem qualitativa, de natureza aplicada, orientada por uma perspectiva interpretativista e operacionalizada por meio de revisão narrativa da literatura. A análise abrange o funcionamento técnico da biometria facial, sua evolução histórica, seus benefícios operacionais e os principais riscos éticos e jurídicos associados à sua utilização. Os resultados indicam que, embora a tecnologia apresente potencial para fortalecer ações de localização de foragidos, identificação de pessoas desaparecidas e otimização de recursos públicos, sua implementação desregulada pode intensificar discriminações algorítmicas, gerar falsos positivos, comprometer a presunção de inocência e ampliar práticas de vigilância incompatíveis com o Estado Democrático de Direito. No plano jurídico, verifica-se a persistência de um vácuo regulatório, uma vez que a LGPD não disciplina de forma suficiente o tratamento de dados biométricos no âmbito da segurança pública, inexistindo, até o momento, marco normativo específico capaz de assegurar transparência, controle e responsabilização. Conclui-se que a conciliação entre inovação tecnológica, proteção de direitos fundamentais e aprimoramento do desempenho operacional da segurança pública depende da instituição de regulação específica, com definição estrita de finalidades, controle humano obrigatório, protocolos transparentes e auditorias algorítmicas periódicas realizadas por instâncias independentes, com supervisão institucional da Autoridade Nacional de Proteção de Dados e fiscalização por órgãos de controle externo, como o Ministério Público e a Defensoria Pública.

Palavras-chave: reconhecimento facial; segurança pública; direitos fundamentais; proteção de dados; vieses algorítmicos.

ABSTRACT

This study examines the application of facial recognition technology in Brazilian public security, based on the following research problem: how to reconcile ethical requirements, such as algorithmic bias, misidentifications, and privacy protection, as well as legal obstacles, especially the absence of specific regulation and the limited scope of the General Data Protection Law, with the need to expand technological tools in public security in order to improve the State's operational performance in combating crime. To this end, a qualitative, applied approach is adopted, guided by an interpretivist perspective and carried out through a narrative literature review. The analysis covers the technical functioning of facial biometrics, its historical development, its operational benefits, and the main ethical and legal risks associated with its use. The results indicate that, although the technology has the potential to strengthen actions aimed at locating fugitives, identifying missing persons, and optimizing public resources, its unregulated implementation may intensify algorithmic discrimination, generate false positives, compromise the presumption of innocence, and expand surveillance practices that are incompatible with the Democratic Rule of Law. From a legal standpoint, the persistence of a regulatory gap is evident, since the General Data Protection Law does not sufficiently regulate the processing of biometric data in the field of public security, and, to date, there is no specific legal framework capable of ensuring transparency, oversight, and accountability. It is concluded that reconciling technological innovation, the protection of fundamental rights, and the improvement of the operational performance of public security depends on the establishment of specific regulation, with a strict definition of purposes, mandatory human oversight, transparent protocols, and periodic algorithmic audits conducted by independent bodies, under the institutional supervision of the National Data Protection Authority and oversight by external control bodies, such as the Public Prosecutor's Office and the Public Defender's Office.

Keywords: Facial Recognition; public security; fundamental rights; data protection; algorithmic biases.

LISTA DE ABREVIATURAS E SIGLAS

ACLU	American Civil Liberties Union
AI Act	Lei de Inteligência Artificial (União Europeia)
UFSC	Universidade Federal de Santa Catarina
ALERJ	Assembleia Legislativa do Estado do Rio de Janeiro
BNMP	Bancos Nacional de Mandados de Prisão
CESeC	Centro de Estudos de Segurança e Cidadania
DPU	Defensoria Pública da União
GDPR	General Data Protection Regulation (Regulamento Geral Sobre a Proteção de Dados).
IA	Inteligência Artificial
ITS Rio	Instituto de Tecnologia e Sociedade do Rio de Janeiro
LFW	Labeled Faces In the Wild
LGPD	Lei Geral de Proteção de Dados Pessoais
LPR	License Plate Recognition (Leitura Automática de Placas)
MIT	Massachusetts Institute of Technology
NIST	National Institute of Standards and Technology
PL	Projeto de Lei
POE	Plataforma de Observação Elevada
POPs	Procedimentos Operacionais Padrão
RF	Reconhecimento Facial
SSP-BA	Secretaria de Segurança Pública da Bahia
TRF	Tecnologias de Reconhecimento Facial

SUMÁRIO

1 INTRODUÇÃO	10
2 METODOLOGIA	11
3 DESENVOLVIMENTO	13
3.1 O FUNCIONAMENTO DA TECNOLOGIA: CONCEITOS, EVOLUÇÃO E ARQUITETURA	13
3.1.1 Definições e Processos da Biometria Facial	13
3.1.2 Marcos Evolutivos: Do Processamento Semiautomatizado ao Deep Learning.....	14
3.1.3 Arquitetura Técnica e Dinâmica Algorítmica Contemporânea	16
3.2 POTENCIAIS BENEFÍCIOS E RESULTADOS OPERACIONAIS NA SEGURANÇA PÚBLICA	17
3.3 DILEMAS ÉTICOS NA APLICAÇÃO DA BIOMETRIA FACIAL NA SEGURANÇA PÚBLICA.....	19
3.3.1 A Falibilidade Algorítmica e a Erosão da Presunção de Inocência	19
3.3.2 Discriminação Algorítmica: Vieses Raciais, Sociais e de Gênero	20
3.3.3 Vigilância em Massa vs. Segurança Coletiva	21
3.3.4 Assimetria de Poder e a Opacidade da 'Caixa-Preta' Algorítmica	22
3.4 ENTRAVES JURÍDICOS E O VÁCUO REGULATÓRIO NO ORDENAMENTO NACIONAL.....	23
3.4.1 Desafios do Ordenamento Brasileiro: Entre a Fragmentação e a Anomia	24
3.4.2 A 'Zona Cinzenta' da LGPD: O Artigo 4º e a Exceção da Segurança Pública	24
3.4.3 Ausência de Transparência, Responsabilização e Controle Externo	25
3.4.4 Dados Biométricos Sensíveis: Consentimento, Proporcionalidade e Finalidade	26
3.4.5 O Contraste com Marcos Regulatórios Internacionais	27
3.5 PROPOSTAS PARA UMA REGULAMENTAÇÃO DEMOCRÁTICA	27
4 CONCLUSÃO	29
REFERÊNCIAS.....	32

1 INTRODUÇÃO

A sociedade contemporânea atravessa um processo acelerado de transformação impulsionado pelo avanço das tecnologias digitais. Neste cenário, a Inteligência Artificial (IA) deixou de ser um conceito restrito ao campo teórico para promover uma verdadeira revolução tecnológica, industrial e sociológica, consolidando-se como ferramenta prática aplicada à tomada de decisões estatais (Gabello, 2024). No contexto da segurança pública, a adoção dessas tecnologias potencializa a capacidade do Estado de monitorar e atuar sobre dinâmicas sociais, ao mesmo tempo que levanta discussões relevantes sobre o exercício do poder e a proteção das garantias individuais.

Dentre as diversas aplicações da IA, o reconhecimento facial destaca-se como uma das tecnologias de identificação biométrica mais promissoras e, simultaneamente, controversas. Tecnicamente, consiste na extração automatizada, digitalização e comparação de características faciais para a identificação de indivíduos (Smith; Miller, 2022). Embora o reconhecimento facial tenha avançado com o desenvolvimento da inteligência artificial e da capacidade de processamento de dados, governos vêm ampliando seu uso em contextos de segurança pública, inclusive para identificação de foragidos e monitoramento de espaços públicos (UNINQ, 2025).

No Brasil, a adoção do reconhecimento facial pela segurança pública tem sido justificada pela expectativa de aumento da eficiência operacional. Experiências implementadas em estados como Bahia, São Paulo e Espírito Santo demonstram o avanço considerável desses sistemas em larga escala (Lima; Bueno; Maldonado, 2023). Contudo, esses programas são frequentemente alvos de debates públicos acerca de sua transparência, eficácia e dos riscos que representam aos direitos básicos, como a privacidade e a liberdade de reunião (Carvalho; Silva, 2024).

A implementação massiva de sistemas de biometria facial em uma sociedade democrática impõe relevantes dilemas éticos. A literatura aponta para riscos técnicos e sociais, como o racismo algorítmico, onde erros de identificação afetam desproporcionalmente grupos específicos, notadamente pessoas negras (DPU; CESEC, 2025). Tais falhas podem resultar em prisões arbitrárias que violam a presunção de inocência e o devido processo legal (Galícia Educação, 2025). Além disso, o armazenamento de dados biométricos gera questionamentos profundos sobre

a violação do direito à privacidade e à proteção de dados na chamada "sociedade da vigilância" (Rodotà, 2017).

No plano jurídico, o cenário brasileiro revela a existência de um vácuo regulatório. Embora a Lei Geral de Proteção de Dados Pessoais (LGPD) estabeleça diretrizes gerais, há uma carência de regulamentação específica que monitore a implementação dessa solução técnica na segurança pública. Essa lacuna normativa permite a aplicação da tecnologia sem o devido controle democrático, auditorias externas ou garantias legais robustas, gerando insegurança jurídica (Galícia Educação, 2025).

Diante desse panorama, observa-se um verdadeiro paradoxo: a necessidade urgente de novas estratégias para combater o crime versus a indispensabilidade de discutir as possíveis violações de direitos. Assim, o presente trabalho busca responder à seguinte questão de pesquisa: Como conciliar a efetivação de temáticas éticas (por exemplo, vieses algorítmicos, identificações incorretas e o direito à privacidade) e legais (a ausência de regulamentação específica e a aplicação da LGPD) com a necessidade de ampliar os meios tecnológicos junto à segurança pública para ter um maior desempenho operacional no combate à criminalidade?

A análise perpassa o funcionamento da tecnologia, seus potenciais benefícios operacionais, os dilemas éticos associados, bem como os entraves jurídicos no ordenamento nacional, visando contribuir para o debate acerca de uma implementação democrática e transparente dessas tecnologias no Brasil.

2 METODOLOGIA

O presente trabalho foi desenvolvido com base em uma abordagem qualitativa, de natureza aplicada, com objetivos exploratórios, descritivos e propositivos. A concepção filosófica que norteia a pesquisa é a interpretativista, na medida em que busca compreender e interpretar os fenômenos sociais, jurídicos e tecnológicos a partir dos significados, implicações e disputas que os envolvem (Creswell, 2014).

No que se refere ao procedimento lógico, a pesquisa adota, de forma predominante, o método indutivo. Parte-se da análise de contribuições doutrinárias, normativas e empíricas acerca do uso do reconhecimento facial na segurança pública, bem como de experiências concretas observadas no contexto nacional e

internacional, para, a partir desses elementos particulares, construir uma compreensão mais ampla sobre seus impactos e formular proposições voltadas à sua utilização compatível com os direitos fundamentais e com os objetivos da segurança pública. Esse percurso metodológico mostra-se adequado porque permite extrair, da observação crítica de casos, dados e debates especializados, inferências gerais sobre os limites, riscos e possibilidades de regulação da tecnologia.

Quanto aos objetivos, a pesquisa classifica-se como exploratória, pois busca proporcionar maior familiaridade com o problema, tornando-o mais explícito e permitindo melhor delimitação de suas variáveis analíticas. Assume também caráter descritivo, na medida em que expõe as características técnicas, operacionais, éticas e jurídicas relacionadas ao reconhecimento facial na segurança pública. Além disso, possui dimensão propositiva, uma vez que não se limita à descrição do paradoxo entre inovação tecnológica e proteção de direitos, mas avança na construção de parâmetros e diretrizes para sua conciliação no contexto brasileiro.

No que tange aos procedimentos técnicos, o estudo foi conduzido por meio de uma pesquisa bibliográfica, materializada na forma de uma revisão narrativa da literatura. Este método é apropriado para descrever e discutir o desenvolvimento ou o "estado da arte" de um determinado assunto, a partir de uma perspectiva teórica ou contextual (Rother, 2007). A revisão narrativa permite a análise de um amplo espectro de publicações e fontes, sendo particularmente útil para a fundamentação teórica de artigos, dissertações e teses, ao sintetizar e interpretar o conhecimento acumulado sobre um tema complexo e multifacetado.

O levantamento do material bibliográfico foi realizado entre os meses de setembro de 2025 e fevereiro de 2026, abrangendo um recorte temporal que se estende de publicações seminais sobre a temática da vigilância e direitos, até as mais recentes produções sobre tecnologia e segurança pública, publicadas até o ano de 2026. A coleta de dados envolveu a consulta a diversas fontes, incluindo:

- Bases de dados científicas: *SciELO (Scientific Electronic Library Online)* e *Google Scholar*;
- Repositórios de teses e dissertações: Biblioteca Digital Brasileira de Teses e Dissertações (BDTD);
- Livros e capítulos de livros de autores de referência nas áreas de Direito, Tecnologia, Sociologia e Segurança Pública;
- Legislação nacional e internacional pertinente ao tema;

- Relatórios e publicações de órgãos governamentais (como o *National Institute of Standards and Technology - NIST*), organizações não governamentais (como a *American Civil Liberties Union - ACLU* e o Fórum Brasileiro de Segurança Pública), e instituições de pesquisa (como o Centro de Estudos de Segurança e Cidadania - CESeC e o Instituto de Tecnologia e Sociedade do Rio - ITS Rio);

- Artigos e reportagens de veículos de comunicação de circulação nacional e internacional.

As buscas foram orientadas pelos seguintes descritores e suas combinações, nos idiomas português e inglês: "reconhecimento facial" (*facial recognition*), "segurança pública" (*public security*), "direitos fundamentais" (*fundamental rights*), "proteção de dados" (*data protection*), "vieses algorítmicos" (*algorithmic bias*), "vigilância" (*surveillance*) e "inteligência artificial" (*artificial intelligence*).

A análise do material coletado seguiu os preceitos da análise de conteúdo, envolvendo a leitura crítica e a interpretação dos documentos. As informações foram sistematicamente organizadas, fichadas e categorizadas em eixos temáticos que estruturam o desenvolvimento deste trabalho: (i) funcionamento e evolução da tecnologia; (ii) benefícios operacionais; (iii) dilemas éticos; (iv) entraves jurídicos e o vácuo regulatório; e (v) propostas para uma regulamentação democrática. Essa organização permitiu a construção de uma argumentação coesa e a síntese dos conhecimentos teóricos, legais e práticos, visando responder à questão de pesquisa proposta (Lakatos; Marconi, 1992).

3 DESENVOLVIMENTO

3.1 O FUNCIONAMENTO DA TECNOLOGIA: CONCEITOS, EVOLUÇÃO E ARQUITETURA

3.1.1 Definições e Processos da Biometria Facial

Para compreender a aplicação dessas tecnologias na segurança pública, é fundamental, primeiramente, definir o conceito de biometria. Nesse sentido:

Biometria é a ciência de reconhecer a identidade de uma pessoa com base em características físicas ou comportamentais. As tecnologias disponíveis para a biometria incluem: impressões digitais, face, voz, íris, veias das mãos,

forma de caminhar, e vincos palmares (Jain; Flynn; Ross, 2008 *apud* Oliveira *et al.*, 2022).

No contexto da identificação civil e criminal, esses sistemas mapeiam características específicas de cada indivíduo e as comparam com bancos de dados preexistentes para estabelecer correspondências e confirmar identidades.

Do ponto de vista técnico, a operação desses sistemas não é uniforme. A literatura especializada (Oliveira *et al.*, 2022) distingue três processos principais na análise de imagens: Detecção facial (ou extração): Limita-se a identificar a presença de um rosto em uma imagem ou vídeo, sem estabelecer vínculo com dados pessoais. Correspondência facial: Utiliza algoritmos para localizar rostos visualmente semelhantes, mas sem necessariamente identificar o sujeito. Reconhecimento facial: Configura-se como a modalidade biométrica propriamente dita, pois associa efetivamente a imagem a dados pessoais (nome, RG, histórico criminal), permitindo a individualização do sujeito.

Operacionalmente, os sistemas de reconhecimento facial funcionam, em geral, seguindo um fluxo de três etapas: (i) captura da imagem por meio de sensores ou câmeras; (ii) extração das características faciais por algoritmos, gerando um vetor numérico representativo (o *template* biométrico); e (iii) comparação desse vetor com os arquivos armazenados no banco de dados. O sistema então calcula o grau de similaridade e emite alertas aos operadores caso o índice de correspondência ultrapasse um limiar previamente definido (Nina da Hora, 2021).

A grande particularidade dessa tecnologia, e onde residem seus maiores desafios éticos, é o fato de que a captura do dado pode ocorrer à distância e em ambientes cotidianos, como ruas e estações de transporte, muitas vezes sem a ciência do indivíduo. Essa característica, ao transformar o rosto em uma chave permanente de rastreamento, amplia o potencial de vigilância estatal, mas intensifica as preocupações com a privacidade e o consentimento, temas centrais desta pesquisa.

3.1.2 Marcos Evolutivos: Do Processamento Semiautomatizado ao Deep Learning

A trajetória do reconhecimento facial não é linear; ela reflete a transição de experimentos acadêmicos isolados para uma infraestrutura global de monitoramento. Segundo Oliveira *et al.* (2022), a história dessa tecnologia remonta à década de 1960, com os experimentos pioneiros de Woodrow Wilson Bledsoe. Naquela época, o sistema era semiautomatizado, um operador humano precisava inserir manualmente em uma mesa digitalizadora as coordenadas das características faciais (olhos, nariz, boca). As limitações eram severas, pois o computador apenas calculava distâncias, falhando diante de qualquer variação de iluminação, pose ou envelhecimento.

Conforme Nora, Freitas e Sousa (2025), na década de 1970, pesquisadores como Takeo Kanade avançaram para sistemas de extração de características automatizadas, mas a precisão ainda era insatisfatória para uso civil. Um salto qualitativo ocorreu apenas entre o final dos anos 1980 e início dos 1990, com o desenvolvimento de métodos estatísticos como *Eigenfaces* (expandido por Turk e Pentland em 1991, utiliza a Análise de Componentes Principais (PCA) para converter imagens faciais complexas em um conjunto reduzido de vetores matemáticos essenciais, simplificando os dados para tornar a comparação e a identificação de rostos mais veloz e eficiente) e *Fisherfaces* (considerado uma evolução do Eigenface por apresentar maior robustez e menor sensibilidade a variações de iluminação e expressões faciais, otimizando a precisão do reconhecimento em condições ambientais diversas). Essas técnicas simplificaram a análise matemática, permitindo que o rosto fosse processado como uma "soma de imagens fantasmas" (redução de dimensionalidade). Contudo, foi somente em 2001, com o algoritmo de Viola-Jones, que a tecnologia se tornou leve o suficiente para detecção de rostos em tempo real em câmeras digitais comuns.

A verdadeira ruptura de paradigma, e o início das preocupações jurídicas contemporâneas ocorreu a partir de 2014, com a aplicação das Redes Neurais Profundas (*Deep Learning*). Exemplificado pelo sistema *DeepFace*, esse modelo elevou a precisão dos algoritmos a níveis próximos ou superiores à capacidade humana, impulsionado pela disponibilidade massiva de dados para treinamento em bancos de dados como o *Labeled Faces in the Wild* (LFW) (Nora, Freitas e Sousa, 2025). Zuboff (2019) alerta que esse aprimoramento técnico coincidiu com a ascensão do "Capitalismo de Vigilância", transformando traços biológicos em matéria-prima preditiva e permitindo que o reconhecimento facial deixasse de ser uma ferramenta passiva para se tornar uma fonte primária de inteligência de segurança pública.

3.1.3 Arquitetura Técnica e Dinâmica Algorítmica Contemporânea

Do ponto de vista da ciência da computação, o reconhecimento facial contemporâneo transcende a simples sobreposição de imagens, inserindo-se no campo do aprendizado de máquina (*machine learning*) e das Redes Neurais Profundas (*Deep Learning*). Diferente dos sistemas antigos, que operavam baseados em regras fixas de geometria (como a distância exata entre os olhos), os modelos atuais são "treinados" a partir de milhões de imagens para identificar padrões abstratos e complexos de textura e forma, simulando o processamento visual humano (Oliveira *et al.*, 2022).

O ciclo de vida operacional dessa tecnologia inicia-se muito antes da captura da imagem na rua, ele começa na fase de treinamento. Nessa etapa, o algoritmo é exposto a vastos bancos de dados de faces rotuladas para que "aprenda" a distinguir características distintivas. A literatura técnica adverte que a qualidade e a diversidade desse conjunto de dados de treinamento são determinantes para a eficácia do sistema, se o banco de dados for homogêneo, composto majoritariamente por indivíduos de determinada etnia ou gênero, a "assinatura facial" gerada para grupos sub-representados terá menor precisão, ampliando a margem de erro. Após o treinamento, o funcionamento em tempo real segue um fluxo lógico de quatro etapas quais sejam: Aquisição: A captura da imagem (foto ou frame de vídeo); o pré-processamento: A normalização da imagem (ajustes de luz, rotação e recorte da face); a extração de características: A conversão da imagem em um vetor numérico único (*faceprint* ou *template*); e a classificação: A comparação matemática desse vetor com o banco de dados (Fernandes, 2022).

É na etapa de classificação que reside uma das maiores complexidades técnicas com repercussão jurídica, o limiar de confiança (*threshold*). Ao comparar a face capturada com o banco de dados, o sistema não entrega uma resposta binária absoluta (sim/não), mas sim uma pontuação de probabilidade (score) de que aquelas duas imagens pertençam à mesma pessoa (ex: "92% de similaridade"). Cabe ao operador do sistema, no caso, a autoridade de segurança pública, definir o "ponto de corte". Se o limiar for ajustado muito baixo, o sistema gera muitos "falsos positivos" (pessoas inocentes identificadas como criminosos); se muito alto, gera "falsos negativos", criminosos não são detectados.

Além disso, a aplicação na segurança pública enfrenta o desafio do "ambiente não controlado". Enquanto a biometria para desbloqueio de celular ocorre com boa iluminação e pose frontal, a vigilância policial lida com variações extremas de luz, ângulos oblíquos, baixa resolução de câmeras e oclusões parciais (uso de bonés, máscaras ou óculos). Esses ruídos ambientais degradam a qualidade da imagem de busca (*probe image*) em comparação à imagem de arquivo (*gallery image*), comprometendo a confiabilidade da correspondência (Oliveira *et al.*, 2022).

Por fim, avanços recentes têm tentado mitigar essas limitações e expandir o uso da ferramenta, por meio do Reconhecimento Facial Comportamental. Diferente da biometria estática, essa abordagem utiliza a neurociência para mapear microexpressões faciais e contrações musculares involuntárias, visando inferir estados emocionais (como nervosismo ou agressividade) ou intenções. Tal evolução sugere uma transição de uma tecnologia puramente identificatória para uma tecnologia preditiva, o que eleva substancialmente o grau de intrusão na esfera psíquica do indivíduo (Alves; Conceição, 2025).

3.2 POTENCIAIS BENEFÍCIOS E RESULTADOS OPERACIONAIS NA SEGURANÇA PÚBLICA

A implementação de tecnologias de reconhecimento facial (RF) na segurança pública inaugura um novo paradigma nas táticas de policiamento ostensivo e investigativo, atuando como um multiplicador de força que converte o monitoramento passivo de vídeo em inteligência policial acionável em tempo real (Vieira; Herdman, 2024). Ao automatizar a identificação de indivíduos, as forças de segurança mitigam as falhas inerentes à memória e à atenção humana, e a integração dessa ferramenta aos bancos de dados oficiais não apenas agiliza a captura de alvos, mas redefine a gestão do espaço público. Conforme destacam Nora, Freitas e Sousa (2025, p. 575):

Os benefícios advindos do uso dessa tecnologia em conjunto com bases de dados governamentais e sistemas de monitoramento incluem a identificação ágil de pessoas de interesse, como indivíduos com mandados de prisão ou desaparecidos, sem aumentar a necessidade de forças policiais. Além disso, permite uma gestão mais eficaz e humanizada dos espaços públicos, possibilitando abordagens menos invasivas e mais respeitosas aos direitos dos cidadãos, ao mesmo tempo em que otimiza recursos e minimiza o risco de confrontos diretos.

Sob essa ótica, o policiamento guiado por reconhecimento facial permite uma atuação cirúrgica, direcionando o efetivo para alvos específicos apenas quando há um alerta positivo confirmado pelo sistema. Essa triagem automatizada, viabilizada pela interconexão com bases de dados como o Banco Nacional de Mandados de Prisão (BNMP), demonstra um impacto mensurável e afasta a discussão do campo meramente teórico. Os resultados operacionais em diversos estados brasileiros confirmam esse potencial. Na Bahia, o sistema implementado pela Secretaria da Segurança Pública (SSP) já possibilitou a prisão de mais de 3.200 criminosos desde 2019 (CNN Brasil, 2025), alcançando em 2023 a marca de mil foragidos capturados exclusivamente por meio do alerta biométrico (Silva; Vieira; Barbuda, 2024). Em São Paulo, o programa Smart Sampa foi responsável pela captura de mais de 2.000 foragidos em menos de dois anos, com uma média de cinco prisões por dia (Moraes 2025). No Espírito Santo, a marca de 600 prisões foi alcançada no início de 2026, com o sistema se mostrando vital também na localização de pessoas desaparecidas (Governo do Estado do Espírito Santo, 2026).

A eficácia dessa "vigilância de precisão" torna-se ainda mais evidente em cenários de grande aglomeração, onde o policiamento tradicional enfrenta severas limitações. Durante o Carnaval de Salvador, por exemplo, a tecnologia foi decisiva para a identificação de dezenas de foragidos em meio à multidão (Silva; Vieira; Barbuda, 2024), uma vitória para a segurança pública dificilmente alcançável por métodos convencionais. Ademais, o potencial da biometria facial é maximizado quando integrado a um "cerco digital" mais amplo, que combina dados de diferentes sensores, como os sistemas de leitura automática de placas de veículos (LPR), a exemplo do sistema Detecta, em São Paulo (Lima; Bueno; Maldonado, 2023). Essa abordagem não apenas otimiza o emprego do efetivo policial, mas também fortalece a fase investigativa e o processo penal, fornecendo elementos probatórios de alta robustez que conferem maior objetividade à instrução criminal.

Entretanto, a celebração desses índices de produtividade não deve ofuscar os complexos desafios que acompanham a expansão massiva dessa tecnologia. Conforme apontam Lima, Bueno e Maldonado (2023), a implementação desses sistemas é frequentemente alvo de debates públicos justamente pela opacidade de seus algoritmos e pela ausência de auditorias independentes sobre seus erros. Surge, assim, a necessidade imperativa de examinar o custo democrático dessa vigilância, temática que impõe limites éticos e técnicos à sua aplicação.

3.3 DILEMAS ÉTICOS NA APLICAÇÃO DA BIOMETRIA FACIAL NA SEGURANÇA PÚBLICA

A incorporação de tecnologias de reconhecimento facial (TRF) nas rotinas de segurança pública tem sido apresentada como um marco de modernização e eficiência no combate à criminalidade. No entanto, a sua adoção acelerada e, por vezes, acrítica, suscita profundos dilemas éticos que demandam uma análise rigorosa. A promessa de uma sociedade mais segura, viabilizada por sistemas automatizados de vigilância, aparenta colidir diretamente com direitos fundamentais e expõe vieses estruturais que podem ser amplificados pela tecnologia.

3.3.1 A Falibilidade Algorítmica e a Erosão da Presunção de Inocência

Um dos argumentos centrais contra a adoção indiscriminada do reconhecimento facial reside em sua natureza probabilística, e não determinística. O sistema não oferece uma certeza de identidade, mas sim um índice de probabilidade de correspondência entre duas imagens. Essa característica intrínseca da tecnologia, aliada a falhas algorítmicas, resulta em um número significativo de "falsos positivos", que são conceituados como identificações incorretas que podem levar a consequências devastadoras para cidadãos inocentes. A literatura acadêmica e relatórios técnicos demonstram consistentemente que a acurácia desses sistemas varia drasticamente conforme o grupo demográfico analisado.

O estudo *Gender Shades*, conduzido por Joy Buolamwini e Timnit Gebru no Massachusetts *Institute of Technology* (MIT), revelou disparidades alarmantes: enquanto a taxa de erro para classificar o gênero de homens de pele clara era de apenas 0,8%, para mulheres de pele escura o índice saltava para 34,7% (Buolamwini; Gebru, 2018). Da mesma forma, estudos do *National Institute of Standards and Technology* (NIST) dos Estados Unidos apontam que os algoritmos de reconhecimento facial são de 10 a 100 vezes mais propensos a identificar erroneamente rostos de pessoas negras e asiáticas em comparação com rostos de pessoas brancas (Grother; Ngan; Hanaoka, 2019).

No Brasil, esses riscos se materializam em violações concretas de direitos. Um relatório conjunto da Defensoria Pública da União (DPU) e do Centro de Estudos

de Segurança e Cidadania (CESeC), intitulado Mapeando a Vigilância Biométrica, aponta que, em 2019, 90% das pessoas presas em decorrência do uso de tecnologias de reconhecimento facial eram negras, majoritariamente acusadas de crimes sem violência (DPU; CESeC, 2025). A própria Polícia Militar do Rio de Janeiro já admitiu, em audiência pública na Assembleia Legislativa do Estado do Rio de Janeiro (ALERJ), uma taxa de 10% de falsos positivos em abordagens geradas por seus sistemas (ALERJ, 2024). Esses erros não são meras falhas técnicas; eles se traduzem em abordagens policiais indevidas, prisões arbitrárias e a instauração de processos criminais sem fundamento, violando frontalmente a presunção de inocência e o devido processo legal, garantias consagradas no artigo 5º, inciso LVII, da Constituição Federal (Brasil, 1988).

Contudo, como aponta a pesquisa de Nora, Freitas e Sousa (2025), o "problema algorítmico" não é uma característica inerente à tecnologia, mas uma consequência de seu treinamento com dados enviesados. A solução, portanto, não é abandonar a ferramenta, mas sim exigir dos fornecedores e do Estado a construção de bancos de dados mais diversos e representativos da população brasileira. Além disso, é fundamental estabelecer que a tecnologia deve ser sempre uma ferramenta de apoio à decisão humana, e nunca a decisão final. O alerta gerado pelo sistema deve ser o ponto de partida para uma verificação por um policial treinado, que seguirá protocolos claros antes de qualquer abordagem. Conforme estabelece a *International Network of Civil Liberties Organizations* (INCLO), um resultado de reconhecimento facial, por si só, jamais deve ser base suficiente para uma interpelação, detenção ou prisão (Inclo, 2024). A criação de Procedimentos Operacionais Padrão (POPs) é, portanto, um caminho essencial para garantir que a tecnologia seja usada como um filtro inicial de inteligência, e não como um mandado de prisão automatizado.

3.3.2 Discriminação Algorítmica: Vieses Raciais, Sociais e de Gênero

A questão dos falsos positivos está intrinsecamente ligada ao problema da discriminação algorítmica. Os sistemas de inteligência artificial são treinados a partir de vastos conjuntos de dados (datasets) que, muitas vezes podem refletir os preconceitos e as desigualdades existentes na sociedade. Se um banco de dados de treinamento é composto majoritariamente por rostos de pessoas brancas, como demonstrado no estudo Gender Shades, onde os datasets IJB-A e Adience eram

compostos por 79,6% e 86,2% de pessoas de pele clara, respectivamente (Buolamwini; Gebru, 2018), o algoritmo desenvolverá uma capacidade menor para identificar com precisão rostos de outros grupos étnico-raciais. O resultado é a perpetuação e a amplificação de vieses históricos sob um manto de suposta neutralidade tecnológica.

Toda essa dinâmica é reforçada pela falta de diversidade nos próprios processos de desenvolvimento tecnológico. Pesquisadores como Perkowitz (2021), em estudo publicado pelo MIT, destacam que a sub-representação de minorias nos conjuntos de dados de treinamento e nas equipes de desenvolvimento é uma das causas estruturais do viés algorítmico. A discriminação, portanto, não é um efeito colateral accidental, mas uma consequência previsível de escolhas técnicas e políticas que negligenciam a equidade.

3.3.3 Vigilância em Massa vs. Segurança Coletiva

O debate sobre a vigilância em massa e a erosão da privacidade é, talvez, o mais complexo, e sua correta compreensão exige um diálogo com pensadores que se debruçaram sobre as relações de poder e controle. A metáfora do “Panóptico”, concebida por Jeremy Bentham e analisada por Michel Foucault em “Vigiar e Punir”, é o ponto de partida clássico: uma arquitetura de poder onde a possibilidade de ser vigiado a qualquer momento induz ao comportamento disciplinado (Foucault, 1999). A preocupação é que as tecnologias de reconhecimento facial criem um “panóptico digital” (Freitas; Sousa; Nora, 2025), uma estrutura de vigilância onipresente e invisível.

Autores contemporâneos, no entanto, argumentam que o modelo foucaultiano foi superado. Zygmunt Bauman e David Lyon (2013) falam em uma “vigilância líquida”, que flui por redes digitais e não depende mais de torres e muros. Já Byung-Chul Han (2017) vai além, afirmando que o panóptico digital atual não opera pela coerção, mas pela sedução: a vigilância se torna palatável através da autoexposição voluntária em redes sociais, em uma “sociedade da transparência” onde a própria privacidade é mercantilizada. Nesse contexto, Shoshana Zuboff (2019) cunha o termo “capitalismo de vigilância” para descrever um novo modelo econômico que transforma a experiência humana em dados comportamentais para fins de predição e controle. Nossos rostos, nesse modelo, tornam-se ativos valiosos.

Diante desse arcabouço teórico, a preocupação com a vigilância estatal ganha novas camadas. Não se trata apenas da violação do "direito de ser deixado em paz", mas da proteção do que o jurista italiano Stefano Rodotà (2017) chamou de "corpo eletrônico": o conjunto de nossos dados que forma nossa identidade digital e cuja proteção é uma extensão dos direitos da personalidade. A vigilância constante pode gerar o que se conhece como *chilling effect* (efeito inibidor), um desincentivo à participação em protestos, à livre associação e à expressão de opiniões dissidentes, minando as bases da própria democracia (Article 19, 2023).

Contudo, é preciso ponderar que a vida em sociedade impõe uma constante negociação entre direitos individuais e a segurança coletiva. O contrato social pressupõe a cessão de uma parcela da liberdade individual ao Estado em troca de proteção. O policiamento ostensivo, a revista pessoal em grandes eventos ou o uso de detectores de metais em aeroportos são exemplos de medidas que, de alguma forma, mitigam a privacidade individual em nome de um bem maior. O uso de câmeras de segurança em espaços públicos já é uma realidade amplamente aceita pela população, que, em sua maioria, aprova as iniciativas de monitoramento (Moraes, 2025). O reconhecimento facial é uma camada de inteligência sobre essa infraestrutura já existente.

A chave para o equilíbrio democrático, portanto, não está na proibição da tecnologia, mas na aplicação rigorosa dos princípios da finalidade, necessidade e proporcionalidade, (Almeida, Shmarko e Lomas 2022). A tecnologia não deve ser usada para monitorar o comportamento de cidadãos comuns ou para a "classificação social" (Lyon, 2003), mas para fins específicos e legalmente previstos: a identificação de indivíduos com mandado de prisão em aberto e a localização de pessoas desaparecidas. A regulamentação deve proibir expressamente o uso da tecnologia para controle social, monitoramento político ou qualquer outra finalidade que extrapole a persecução penal estrita, garantindo que o poder de vigilância do Estado permaneça sob o controle da lei e da sociedade.

3.3.4 Assimetria de Poder e a Opacidade da 'Caixa-Preta' Algorítmica

A expansão do reconhecimento facial aprofunda a já existente assimetria de poder entre o Estado e o cidadão. O monopólio da força e da vigilância, quando potencializado por tecnologias opacas e de difícil escrutínio, cria um desequilíbrio

perigoso para a democracia. Empresas como a Clearview AI, que constroem seus bancos de dados a partir de bilhões de imagens coletadas da internet sem consentimento e os vendem para agências de segurança, exemplificam a falta de controle e a vulnerabilidade a que os cidadãos estão expostos. Segundo Nunes e Lima (2025), o valor total contratado apenas com a representante da Clearview no Brasil ultrapassa R\$ 14 milhões, e todos os contratos identificados foram firmados por inexigibilidade de licitação, sob o argumento de singularidade técnica.

O uso de contratos firmados sem licitação, a ausência de auditorias independentes e a falta de transparência sobre os algoritmos e suas taxas de erro consolidam um ecossistema onde a responsabilização é praticamente inexistente. A tecnologia é apresentada como uma "caixa-preta", cujas decisões devem ser aceitas sem questionamento, normalizando o monitoramento constante como um preço a ser pago pela segurança. Essa normalização representa um risco não apenas para os direitos individuais, mas para a própria vitalidade do debate democrático e da fiscalização do poder estatal. Como advertem Almeida, Shmarko e Lomas (2022), é necessário que haja responsabilização por meio de maior transparência, regulação, auditoria e explicação do uso e da aplicação dessas tecnologias em contextos individuais.

Em suma, os dilemas éticos que circundam o uso do reconhecimento facial na segurança pública são complexos e multifacetados. Eles revelam que a busca por eficiência não pode se sobrepor aos princípios fundamentais que sustentam uma sociedade livre e justa. A tecnologia, em vez de ser uma solução definitiva, pode se tornar um vetor de injustiça e opressão se não for submetida a um rigoroso controle ético, social e democrático.

3.4 ENTRAVES JURÍDICOS E O VÁCUO REGULATÓRIO NO ORDENAMENTO NACIONAL

A expansão das tecnologias de reconhecimento facial na segurança pública brasileira ocorre em um cenário de notável vácuo regulatório. A ausência de uma legislação federal específica que estabeleça limites, procedimentos e mecanismos de controle para o uso de dados biométricos pelo Estado cria um ambiente de insegurança jurídica e abre margem para a violação sistemática de direitos fundamentais.

3.4.1 Desafios do Ordenamento Brasileiro: Entre a Fragmentação e a Anomia

O ordenamento jurídico brasileiro carece de uma norma que discipline de forma abrangente o uso do reconhecimento facial para fins de segurança pública e persecução penal. Embora a Constituição Federal estabeleça um robusto arcabouço de proteção aos direitos fundamentais, como a privacidade, a imagem, a liberdade e, mais recentemente, a proteção de dados pessoais (Art. 5º, incisos X, XV e LXXIX) (Brasil, 1988), a tradução desses princípios em regras concretas para a atividade policial ainda é incipiente no que tange às novas tecnologias.

Essa lacuna permite que estados e municípios implementem projetos de vigilância biométrica de forma fragmentada, cada qual com seus próprios protocolos (ou a ausência deles), critérios de aquisição e políticas de uso. Conforme aponta o relatório do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio), essa descentralização sem uma diretriz nacional impede a criação de um padrão mínimo de garantias, deixando o cidadão sujeito a diferentes níveis de proteção a depender da localidade (ITS RIO, s.d.). A situação é agravada pela utilização de contratos por inexigibilidade de licitação para aquisição de softwares de empresas como a Clearview AI, o que reduz a transparência e o escrutínio público sobre as ferramentas empregadas (Nunes; Lima, 2025).

3.4.2 A 'Zona Cinzenta' da LGPD: O Artigo 4º e a Exceção da Segurança Pública

A Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), representou um avanço civilizatório ao estabelecer um marco para o tratamento de dados pessoais no Brasil. A lei classifica expressamente os dados biométricos como "dados pessoais sensíveis" (Art. 5º, II), cujo tratamento exige um nível de proteção ainda mais elevado e só pode ocorrer em hipóteses taxativas, como o consentimento explícito do titular ou o cumprimento de obrigação legal (Art. 11) (Brasil, 2018). No entanto, a eficácia da LGPD para regular o uso do reconhecimento facial pela segurança pública é severamente limitada por uma de suas próprias disposições.

O Artigo 4º, inciso III, da LGPD exclui de seu escopo de aplicação o tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa

nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (Brasil, 2018). Embora o mesmo artigo preveja que esse tratamento deve ser regido por legislação específica, essa lei ainda não existe. Cria-se, assim, uma zona cinzenta: a principal norma de proteção de dados do país não se aplica plenamente à atividade estatal que mais potencialmente ameaça esses mesmos dados. Consequentemente, princípios basilares da LGPD, como a necessidade, a finalidade, a transparência e a não discriminação, não são juridicamente vinculantes para os projetos de vigilância biométrica em curso, deixando a proteção dos direitos dos cidadãos em um estado de vulnerabilidade.

Essa lacuna foi identificada pelo próprio legislador, que reconheceu a necessidade de um anteprojeto de lei de proteção de dados para a segurança pública, a chamada "LGPD Penal". Conforme analisa o ITS Rio, o anteprojeto traz em seu conteúdo duas proibições ao uso de tecnologias de monitoramento, reacendendo o debate sobre as aplicações da tecnologia de reconhecimento facial, que se complexifica entre os benefícios à segurança pública e as ameaças ao direito à privacidade (ITS Rio, s.d.). Contudo, até o momento, esse anteprojeto não foi convertido em lei, perpetuando o vácuo normativo.

3.4.3 Ausência de Transparência, Responsabilização e Controle Externo

A falta de um marco legal específico resulta na ausência de critérios claros para a transparência, a responsabilização (*accountability*) e a auditoria dos sistemas de reconhecimento facial. Atualmente, não há obrigação legal para que os órgãos de segurança pública divulguem informações essenciais sobre a origem e a composição dos bancos de dados utilizados para comparação, os algoritmos empregados e suas respectivas taxas de erro para diferentes grupos demográficos, os protocolos de abordagem em caso de correspondência positiva, ou as políticas de armazenamento e descarte dos dados biométricos coletados de milhões de pessoas não investigadas.

Essa opacidade impede o controle social e a fiscalização por parte de órgãos como o Ministério Público e a Defensoria Pública. A auditoria algorítmica, um mecanismo fundamental para verificar se os sistemas operam de forma justa e precisa, não é uma prática exigida ou padronizada no Brasil. Sem ela, é impossível aferir a real extensão dos vieses discriminatórios e responsabilizar o Estado e as empresas fornecedoras por erros que resultem em prisões indevidas e outras

violações de direitos (Nunes; Lima, 2025). Das 81 solicitações de informação enviadas pelo CESeC a órgãos estaduais, em mais da metade dos casos não houve resposta, e quando houve retorno, as informações eram frequentemente genéricas ou incompletas (Nunes; Lima, 2025).

O debate sobre o Projeto de Lei 2.338/2023, que busca criar um Marco Legal da Inteligência Artificial, tangencia essa questão ao classificar o reconhecimento facial como de "risco excessivo" (Brasil, 2023). Todavia, o texto ainda falha em propor mecanismos robustos e concretos de governança e auditoria para seu uso na segurança pública. A Portaria do Ministério da Justiça e Segurança Pública nº 961/2025 estabeleceu diretrizes sobre o uso de inteligência artificial em investigações, mas não criou instrumentos concretos de fiscalização no que se refere ao reconhecimento facial (Nunes; Lima, 2025).

3.4.4 Dados Biométricos Sensíveis: Consentimento, Proporcionalidade e Finalidade

O tratamento de dados biométricos pelo Estado na segurança pública levanta questões jurídicas específicas relacionadas ao consentimento, à proporcionalidade e à finalidade. Os dados biométricos faciais são, por natureza, irrevogáveis: diferentemente de uma senha ou de um número de documento, o rosto de uma pessoa não pode ser alterado. Uma vez que esses dados são coletados, armazenados e eventualmente comprometidos em um vazamento, o dano é permanente e irreversível.

No modelo atual de vigilância biométrica em espaços públicos, o consentimento do titular é simplesmente inexistente. Cidadãos têm seus dados faciais capturados e processados sem qualquer ciência ou autorização, o que contraria o princípio da autodeterminação informativa, fundamento da proteção de dados pessoais. A finalidade do tratamento, outro pilar da proteção de dados, também é frequentemente descumprida, uma vez que os dados coletados podem ser compartilhados entre diferentes órgãos sem critérios claros para acesso, revisão ou contestação (DPU; CESeC, 2025).

3.4.5 O Contraste com Marcos Regulatórios Internacionais

A situação de vácuo normativo no Brasil contrasta fortemente com os desenvolvimentos regulatórios em outras partes do mundo, notadamente na União Europeia. O Regulamento Geral sobre a Proteção de Dados (GDPR), que inspirou a LGPD, classifica dados biométricos como uma categoria especial de dados pessoais (Art. 9) e proíbe seu processamento como regra geral, admitindo exceções apenas em hipóteses estritamente definidas (União Europeia, 2016).

Mais recentemente, a União Europeia aprovou o AI Act (Lei de Inteligência Artificial), o primeiro marco regulatório abrangente para inteligência artificial do mundo. O AI Act adota uma abordagem baseada em risco e proíbe certas aplicações de IA consideradas de "risco inaceitável", incluindo a utilização de sistemas de identificação biométrica remota "em tempo real" em espaços de acesso público para fins de aplicação da lei, salvo em casos excepcionais e estritamente definidos, como a busca por vítimas de crimes graves ou a prevenção de ameaças terroristas (União Europeia, 2024). A legislação europeia estabelece, portanto, uma presunção contra a vigilância biométrica em massa, exigindo autorização judicial e uma justificativa robusta para seu uso pontual.

Nos Estados Unidos, embora não exista uma legislação federal unificada, ao menos 20 cidades e 15 estados adotaram proibições ou restrições significativas ao uso de reconhecimento facial por agências governamentais, refletindo uma crescente preocupação com os riscos dessa tecnologia para os direitos civis (ACLU, 2026). Essa abordagem descentralizada, ainda que imperfeita, demonstra uma sensibilidade regulatória que o Brasil ainda não desenvolveu de forma consistente.

A comparação com esses marcos internacionais evidencia que é possível e desejável impor limites legais estritos à tecnologia em nome da salvaguarda da democracia e da liberdade. O Brasil, ao manter-se em um estado de anomia regulatória, não apenas falha em proteger seus cidadãos, mas também se distancia das melhores práticas internacionais em matéria de direitos humanos e governança tecnológica.

3.5 PROPOSTAS PARA UMA REGULAMENTAÇÃO DEMOCRÁTICA

O enfrentamento do vácuo normativo detalhado anteriormente não implica a proibição da tecnologia, mas exige a construção de um marco legal robusto que concilie a inovação na segurança pública com a salvaguarda dos direitos fundamentais. A superação dos dilemas jurídicos passa pela adoção de um conjunto de medidas que garantam o uso do reconhecimento facial de forma ética, transparente e proporcional. Nesse sentido, uma futura legislação, como a chamada "LGPD Penal", deveria contemplar os seguintes eixos estruturantes:

1. Definição de Finalidade e Proporcionalidade: A lei deve estabelecer um rol taxativo e restrito de finalidades para as quais o reconhecimento facial pode ser empregado, como a identificação de indivíduos com mandado de prisão por crimes graves ou a busca por pessoas desaparecidas. A aplicação dos princípios da necessidade e da proporcionalidade é crucial para vedar o uso da tecnologia para fins de controle social, monitoramento político ou classificação de cidadãos, alinhando-se às melhores práticas internacionais, como as previstas no AI Act da União Europeia (União Europeia, 2024).

2. Transparência e Auditoria Algorítmica: É imperativo que a legislação torne obrigatória a realização de auditorias independentes e periódicas nos algoritmos, com a publicação de relatórios de impacto que detalhem as taxas de erro e a acurácia para diferentes grupos demográficos. Essa medida, defendida por autores como Almeida, Shmarko e Lomas (2022), é o principal instrumento para combater os vieses discriminatórios e permitir o controle social sobre a tecnologia. A transparência deve abranger também a origem e a composição dos bancos de dados utilizados.

3. Controle Humano e Responsabilização: A tecnologia deve ser regulada como uma ferramenta de apoio à decisão, e nunca como uma decisão final e automatizada. Para tanto, a lei deve exigir a criação de Procedimentos Operacionais Padrão (POPs) que determinem a verificação obrigatória de todo alerta positivo por um agente humano treinado antes de qualquer abordagem ou detenção (Inclo, 2024). Isso estabelece uma cadeia de responsabilidade clara e mitiga os riscos de prisões arbitrárias decorrentes de falsos positivos.

4. Governança e Controle Externo: A regulamentação deve fortalecer os mecanismos de governança e fiscalização, garantindo que órgãos de controle externo, como o Ministério Público e a Defensoria Pública, tenham acesso irrestrito às informações sobre o funcionamento dos sistemas para exercerem sua função fiscalizatória. A criação de um órgão supervisor ou a atribuição de competências

claras à Autoridade Nacional de Proteção de Dados (ANPD) para o setor de segurança pública seria um passo fundamental para assegurar a conformidade contínua com a lei e a proteção dos direitos dos cidadãos.

4 CONCLUSÃO

A sociedade contemporânea experimenta transformações inéditas nos mecanismos de coleta, processamento e utilização de informações pessoais (Rodotà, 2017). Nesse cenário, a biometria facial emerge como uma tecnologia de vanguarda e, simultaneamente, como um vetor de profundas inquietações para o Estado Democrático de Direito. A concepção tradicional de privacidade, fundamentada no direito de isolamento, demonstrou-se inadequada diante das transformações impostas pela era digital. Nesse novo contexto, a privacidade contemporânea passa a ser compreendida como o "direito a controlar o uso que os outros façam das informações que me digam respeito" (Rodotà, 2017, p. 74).

Nesse sentido, o autor aponta que a lógica da proteção de dados se deslocou. Se antes o paradigma se concentrava na relação "pessoa-informação-sigilo", hoje a dinâmica mais relevante é a de "pessoa-informação-circulação-controle". Isso significa que o titular dos dados não busca mais apenas impedir a divulgação de suas informações, mas sim exigir mecanismos que lhe permitam governar como elas circulam e são utilizadas por terceiros, o que o autor define como o direito a uma "circulação controlada" (Rodotà, 2017).

É sob essa perspectiva de "circulação controlada" que se insere o debate central deste trabalho. A presente pesquisa debruçou-se sobre o paradoxo que permeia a adoção do reconhecimento facial pela segurança pública brasileira: a busca legítima por maior eficiência operacional no combate à criminalidade em contraposição aos riscos concretos de violação de direitos fundamentais. A revisão narrativa da literatura permitiu examinar esse fenômeno a partir de suas dimensões técnica, ética e jurídica, revelando um cenário de avanços inegáveis, porém acompanhados de lacunas preocupantes.

No plano operacional, a análise dos programas implementados em estados como Bahia, São Paulo e Espírito Santo demonstrou que a tecnologia oferece benefícios tangíveis. A captura de milhares de foragidos, a localização de pessoas desaparecidas e a otimização do emprego do efetivo policial são resultados concretos

que atestam o valor estratégico da ferramenta. A integração da biometria facial com bancos de dados como o Banco Nacional de Mandados de Prisão confere às forças de segurança uma capacidade de atuação sem precedentes, convertendo o monitoramento passivo em inteligência policial acionável.

Contudo, a investigação aprofundou-se nos dilemas éticos que acompanham essa expansão. Os vieses algorítmicos, amplamente documentados por estudos como o Gender Shades e os relatórios do NIST, revelam que os erros de identificação não são distribuídos de forma equânime na sociedade, penalizando desproporcionalmente a população negra. No Brasil, os dados compilados pela Defensoria Pública da União e pelo CESeC confirmam essa tendência, apontando que a grande maioria das prisões decorrentes do reconhecimento facial recai sobre pessoas negras, muitas vezes por delitos sem violência. A ocorrência de falsos positivos, longe de ser uma mera falha técnica, configura uma violação direta da presunção de inocência e do devido processo legal. Ademais, a vigilância biométrica em massa, quando desprovida de controle, produz o chamado chilling effect, inibindo o exercício de liberdades civis como a manifestação e a livre associação, pilares de qualquer regime democrático.

No campo jurídico, o estudo evidenciou um vácuo regulatório que agrava os riscos descritos. A Lei Geral de Proteção de Dados, embora classifique dados biométricos como sensíveis, exclui de seu escopo o tratamento para fins de segurança pública, e a legislação específica prevista para suprir essa lacuna, a chamada "LGPD Penal", ainda não foi aprovada. Essa anomia normativa permite que estados e municípios implementem projetos de vigilância de forma fragmentada, sem padrões mínimos de transparência, auditoria ou responsabilização. A comparação com marcos regulatórios internacionais, notadamente o AI Act da União Europeia, demonstrou que é possível e desejável impor limites rigorosos ao uso dessa tecnologia, tratando-a como de alto risco e exigindo autorização judicial e justificativa robusta para seu emprego.

Diante do exposto, a resposta à questão de pesquisa que orientou este trabalho aponta para uma conciliação que não reside na proibição da ferramenta, mas em sua regulação criteriosa e democrática. É imperativo que o ordenamento jurídico brasileiro avance na criação de um marco legal específico que estabeleça, com clareza, as finalidades estritas para o uso do reconhecimento facial na segurança pública, os mecanismos de auditoria algorítmica independente, os protocolos de

verificação humana obrigatória antes de qualquer abordagem policial e as formas de responsabilização do Estado e dos fornecedores por erros e abusos. A tecnologia deve servir como instrumento de apoio à decisão humana, e jamais como um veredito automatizado. Somente por meio de um amplo debate público, de uma regulamentação transparente e do respeito irrestrito aos direitos fundamentais será possível garantir que a biometria facial cumpra sua promessa de segurança sem sacrificar a liberdade e a dignidade que constituem os alicerces do Estado Democrático de Direito.

REFERÊNCIAS

Abordagens por reconhecimento facial têm 10% de falsos positivos, afirma PM em audiência na Alerj. **ALERJ**, 2024. Disponível em: <https://www.alerj.rj.gov.br/Visualizar/Noticia/68952>. Acesso em: 01 dez. 2025.

AI and The Risk of Wrongful Convictions in the U.S. **Innocence Project**, 2024. Disponível em: <https://innocenceproject.org/news/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/>. Acesso em: 11 fev. 2026.

ALMEIDA, D.; SHMARKO, K.; LOMAS, E. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. **AI and Ethics**, v. 2, p. 377-387, 2022. Disponível em: <https://link.springer.com/article/10.1007/s43681-021-00077-w>. Acesso em: 15 jan. 2025.

ALVES, D. S.; CONCEIÇÃO, M. M. O impacto da inteligência artificial na automação de auditorias em conformidade com as leis de proteção de dados. **RECIMA21 - Revista Científica Multidisciplinar**, v. 6, n. 1, p. e616167, 2025. Disponível em: <https://recima21.com.br/recima21/article/view/6167>. Acesso em: 26 fev. 2026.

ALVES, D. S.; CONCEIÇÃO, M. M. O reconhecimento facial comportamental na segurança pública. **RECIMA21 - Revista Científica Multidisciplinar**, v. 6, n. 1, p. e616190, 2025. Disponível em: <https://recima21.com.br/recima21/article/view/6190>. Acesso em: 01 fev. 2026.

BAUMAN, Z.; LYON, D. **Vigilância líquida: diálogos**. Rio de Janeiro: Zahar, 2013.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 05 nov. 2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.338/2023**. Institui o Marco Legal da Inteligência Artificial. Brasília, DF: Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262>. Acesso em: 01 nov. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 01 nov. 2025.

BUOLAMWINI, J. **Gender shades**: intersectional phenotypic and demographic evaluation of face datasets and gender classifiers. 2017. 116 f. Tese (Doutorado) – Massachusetts Institute of Technology, Cambridge, 2017. Disponível em: <https://dspace.mit.edu/handle/1721.1/114068>. Acesso em: 15 fev. 2026.

BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. **Proceedings of Machine Learning Research**, v.

81, p. 1-15, 2018. Disponível em: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. Acesso em: 15 fev. 2026.

CARVALHO, L.; SILVA, R. Segurança pública, vigilantismo e novas tecnologias: o reconhecimento facial como ferramenta de garantia de direitos. **Revista F&T**, 2024. Disponível em: <https://revistaft.com.br/seguranca-publica-vigilantismo-e-novas-tecnologias-oreconhecimento-facial-como-ferramenta-de-garantia-de-direitos/>. Acesso em: 11 mar. 2026.

COMENTÁRIOS ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública: Tecnologia de Reconhecimento Facial. **ITS Rio**, [s.d.]. Disponível em: <https://itsrio.org/pt/publicacoes/comentarios-ao-anteprojeto-de-lei-de-protecao-de-dados-para-a-seguranca-publica/>. Acesso em: 05 jan. 2026.

CRESWELL, J. W. **Investigação Qualitativa e Projeto de Pesquisa: escolhendo entre cinco abordagens**. 3. ed. Porto Alegre: Penso, 2014.

ESPÍRITO Santo alcança marca de 600 presos com uso de reconhecimento facial. **Portal do Governo do estado do Espírito Santo**, 2026. Disponível em: <https://planejamento.es.gov.br/Not%C3%ADcia/espírito-santo-alcanca-marca-de-600-presos-com-uso-de-reconhecimento-facial>. Acesso em: 11 fev. 2026.

EYES on the Watchers: Challenging the Rise of Police Facial Recognition. **INCLO (International Network of Civil Liberties Organizations)**, 2024. Disponível em: <https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/>. Acesso em: 12 jan. 2025.

FERNANDES, F. A. C. **Reconhecimento facial, racismo e segurança pública**: um estudo sobre os riscos da tecnologia para a população negra no Brasil. 2022. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2022.

FERNANDES, M.; LIMA, T.; PIETRANI, J. Reconhecimento facial e os riscos da vigilância indiscriminada. **Consultor Jurídico**, 2025. Disponível em: <https://www.conjur.com.br/2025-nov-05/reconhecimento-facial-e-os-riscos-da-vigilancia-indiscriminada/>. Acesso em: 20 jan. 2026.

FOUCAULT, M. **Vigiar e punir: nascimento da prisão**. 39. ed. Petrópolis, RJ: Vozes, 1999. 291 p.

GABELLO, K. La IA es una quimera real: puede hacer el mundo radicalmente mejor. **El País**, 2024. Disponível em: <https://elpais.com/ideas/2024-12-07/la-ia-es-una-quimera-real-puede-hacer-el-mundo-radicalmente-mejor.html>. Acesso em: 02 jan. 2026.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008. GROTH, P.; NGAN, M.; HANAOKA, K. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. **Gaithersburg: National Institute of Standards and Technology (NIST)**, 2019. Disponível em: <https://www.nist.gov/news->

events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. Acesso em: 11 set. 2025.

HAN, B. **Sociedade da transparência**. Petrópolis: Vozes, 2017.

LAKATOS, E. M.; MARCONI, M. de A. **Metodologia do trabalho científico: procedimentos básicos, pesquisa bibliográfica, projeto e relatório, publicações e trabalhos científicos**. 4. ed. São Paulo: Atlas, 1992.

LIMA, R. S.; BUENO, S.; MALDONADO, D. (org.). **Anuário Brasileiro de Segurança Pública 2023**. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf>. Acesso em 11 mar. 2026

LYON, David. **Surveillance after September 11**. Cambridge: Polity Press, 2003.

MORAES, L. Smart Sampa chega a 2 mil prisões de foragidos e apreensões circulam na web; veja vídeos. **Exame**, 2025. Disponível em: <https://exame.com/brasil/smart-sampa-chega-a-2-mil-prisoas-de-foragidos-e-apreensoes-circulam-na-web-veja-videos/>. Acesso em: 07 jan. 2026.

NORA, H. D.; FREITAS, C. O. A.; SOUSA, D. R. A aplicação da tecnologia de reconhecimento facial na segurança pública brasileira e seus desafios. **Revista Eletrônica Direito e Política**, v. 20, n. 3, p. 563–591, 2025. Disponível em: <https://periodicos.univali.br/index.php/rdp/article/view/20557>. Acesso em: 26 fev. 2026.

NUNES, P.; LIMA, T. Algoritmos decidem, mas quem se responsabiliza? Os riscos da adoção desregulada de tecnologias digitais na Justiça criminal brasileira. **Fonte Segura**, 2025. Disponível em: <https://fontesegura.forumseguranca.org.br/algoritmos-decidem-mas-quem-se-responsabiliza-os-riscos-da-adocao-desregulada-de-tecnologias-digitais-na-justica-criminal-brasileira/>. Acesso em: 11 mar. 2026.

O que é Reconhecimento facial? Uma introdução técnica. **Nina da Hora**, 2021. Disponível em: <https://www.ninadahora.dev/post/reconhecimento-facial-introdu%C3%A7%C3%A3o>. Acesso em: 11 mar. 2026.

OLIVEIRA, L. V. *et al.* Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil. **Revista Tecnologia e Sociedade**, Curitiba, v. 18, n. 50, p. 114-135, 2022. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/view/12968>. Acesso em: 10 jan. 2026.

PERKOWITZ, S. The bias in the machine: Facial recognition technology and racial disparities. **MIT Case Studies in Social and Ethical Responsibilities of Computing**, 2021. Disponível em: <https://mit-serc.pubpub.org/pub/bias-in-machine>. Acesso em: 05 dez. 2025.

QUANDO corpos se tornam dados: tecnologias biométricas e liberdade de expressão **Article 19**, 2022. Disponível em: <https://www.article19.org/wp->

content/uploads/2023/06/Biometric-Report_Portuguese_13-06-23.pdf. Acesso em: 11 mar. 2026.

RECONHECIMENTO Facial e Direitos: Desafios Legais no Brasil. **Galícia Educação Blog**, 2025. Disponível em: <https://www.galiciaeducacao.com.br/blog/reconhecimento-facial-e-direitos-desafios-legais-no-brasil/>. Acesso em: 02 nov. 2025.

RELATÓRIO da DPU e CESeC alerta para riscos do reconhecimento facial na segurança pública. **Portal da Defensoria Pública da União**, 2025. Disponível em: <https://direitoshumanos.dpu.def.br/relatorio-da-dpu-e-cesec-alerta-para-riscos-do-reconhecimento-facial-na-seguranca-publica/>. Acesso em: 11 dez. 2025.

RETAILERS Secretively Using Face Recognition to Spot "Persons of Interest". **American Civil Liberties Union**, 20 jan. 2026. Disponível em: <https://www.aclu.org/news/privacy-technology/retailers-secretively-using-face-recognition>. Acesso em: 11 fev. 2026.

RODOTÀ, S. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda e Luciana R. de Moraes. Rio de Janeiro: Renovar, 2017.

ROTHER, E. T. **Revisão sistemática X revisão narrativa**. Acta Paulista de Enfermagem, v. 20, n. 2, p. 1-5, 2007. Disponível em: <https://actaape.org/en/article/systematic-literature-review-x-narrative-review/>. Acesso em: 10 fev. 2026.

SILVA, R. V.; VIEIRA, P. H. B.; BARBUDA, A. S. de. A aplicação da inteligência artificial na atividade de inteligência de segurança pública. **Revista Jurídica do Nordeste Mineiro**, v. 8, n. 1, 2024. Disponível em: <https://jrnrm.ojsbr.com/juridica/article/view/2936>. Acesso em: 17 fev. 2026.

SOUZA, C. J. Biometria facial na segurança pública: avanços, desafios e reflexões éticas. **UNINQ**, 2025. Disponível em: <https://uninq.com.br/biometria-facial-na-seguranca-publica-avancos-desafios-e-reflexoes-eticas/>. Acesso em: 10 fev. 2026.

SMITH, M.; MILLER, S. The ethical application of biometric facial recognition technology. **AI & Society**, [S. l.], v. 37, p. 1677-1685, 2022. DOI: 10.1007/s00146-021-01199-9. Disponível em: <https://link.springer.com/article/10.1007/s00146-021-01199-9>. Acesso em: 12 mar. 2026.

TECNOLOGIAS de reconhecimento facial e direitos em risco. **Anistia Internacional**, 2024. Disponível em: <https://anistia.org.br/informe/tecnologias-de-reconhecimento-facial-e-direitos-em-risco/>. Acesso em: 11 fev. 2026.

TÍSSIA, C. Bahia ultrapassa 900 prisões através do reconhecimento facial este ano. **CNN Brasil**, 2025. Disponível em: <https://www.cnnbrasil.com.br/nacional/nordeste/ba/bahia-ultrapassa-900-prisoos-atraves-do-reconhecimento-facial-este-ano/>. Acesso em: 05 jan. 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119/1, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L:2016:119:FULL>. Acesso em: 11 fev. 2026.

UNIÃO EUROPEIA. **Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Lei da Inteligência Artificial — AI Act)**. Bruxelas: Parlamento Europeu, 2024. Disponível em: <https://artificialintelligenceact.eu/>. Acesso em: 08 nov. 2025.

VIEIRA, M. de S.; HERDMAN, E. A utilização de tecnologias de reconhecimento facial como facilitadores da segurança pública. **Revista Caderno Pedagógico**, Curitiba, v. 21, n. 10, p. 1-15, 2024. Disponível em: <https://periodicos.univali.br/index.php/rdp>. Acesso em: 01 nov. 2025.

ZUBOFF, S. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. New York: PublicAffairs, 2019. 704 p. Disponível em: https://raggeduniversity.co.uk/wp-content/uploads/2024/08/1_x_Shoshana-Zuboff-The-Age-of-Surveillance-Capitalism_-The-Fight-for-a-Human-Future-at-the-New-Frontier-of-Power-PublicAffairs-Books-2019.pdf . Acesso em: 11 fev. 2026.