

GOVERNANÇA PÚBLICA E DIREITOS FUNDAMENTAIS NO USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA: UMA REVISÃO INTEGRATIVA DA LITERATURA

PUBLIC GOVERNANCE AND FUNDAMENTAL RIGHTS IN THE USE OF FACIAL RECOGNITION IN LAW ENFORCEMENT: AN INTEGRATIVE LITERATURE REVIEW

Cherliton Martins Barbosa¹

Universidade Federal do Tocantins
<https://orcid.org/0009-0007-1925-347X>

Fabian Serejo Santana²

Universidade Estadual do Tocantins
<https://orcid.org/0000-0002-8936-987X>

Sara Brigida Farias Ferreira³

Universidade Estadual do Tocantins
<https://orcid.org/0000-0001-6588-2305>

Jeany Castro dos Santos⁴

Universidade Estadual do Tocantins
<https://orcid.org/0000-0002-4479-0839>

DOI: <https://doi.org/10.46550/ilustracao.v7i4.591>

Aceito em: 29.03.2026

Resumo: Este artigo analisa o tratamento conferido pela literatura científica aos desafios de governança pública e proteção de direitos fundamentais no uso do reconhecimento facial na segurança pública. Por meio de uma revisão integrativa de abordagem qualitativa, fundamentada na análise de 37 artigos selecionados nas bases *Web of Science*, Portal de Periódicos CAPES e Google Acadêmico, a pesquisa identifica um deslocamento do debate da eficácia técnica para os impactos institucionais e democráticos da tecnologia. Os resultados revelam que o reconhecimento facial opera em um denso campo de tensões entre promessas de modernização e riscos de vigilância massiva, opacidade algorítmica e reprodução de racismos estruturais. Conclui-se que a aceitabilidade social e a legitimidade da ferramenta não decorrem da legalidade formal, mas dependem da construção de

- 1 Mestrando pelo Programa de Desenvolvimento Regional da Universidade Federal do Tocantins (PPGDR/UFT) e especialista em Direito Administrativo e em Gestão em Segurança Pública pela Universidade Federal de Mato Grosso do Sul (UFMS). Policial Militar da Polícia Militar do Estado do Tocantins e Professor voluntário do curso de Administração do Instituto Federal do Tocantins Campus Porto Nacional. Email: cherlitonmartins@uft.edu.br
- 2 Doutorando pelo Programa de Desenvolvimento Regional (PPGDR/UFT) e Mestre em Ciências do Ambiente pela Universidade Federal do Tocantins (CIAMB/UFT). Professor efetivo do curso de Direito da Universidade Estadual do Tocantins. Email: fabian.ss@unitins.br
- 3 Doutoranda em Ciências do Ambiente pela Universidade Federal do Tocantins – UFT. Mestre em Planejamento e Desenvolvimento Regional e Urbano na Amazônia (PPGPAM) e em Propriedade Intelectual e Transferência de Tecnologia para Inovação (ProfNit), pela Universidade Federal do Sul e Sudeste do Pará (UNIFESSPA). Professora efetiva do curso de Direito da Universidade Estadual do Tocantins. Email: sara.bf@unitins.br
- 4 Doutora e Mestra em Desenvolvimento Regional pelo Programa de Pós-Graduação em Desenvolvimento Regional da Universidade Federal do Tocantins. Docente Permanente do Mestrado Profissional em Administração Pública (PROFIAP). Diretora de Ensino, professora do curso Gestão Pública. Email: jeany.cd@unitins.br



marcos regulatórios robustos, transparência procedimental e da indispensabilidade da revisão humana, exigindo que a eficiência operacional não se sobreponha às garantias fundamentais do Estado de Direito.

Palavras-chave: reconhecimento facial. segurança pública. governança pública. direitos fundamentais. racismo algorítmico.

Abstract: This article analyzes the treatment given by scientific literature to the challenges of public governance and the protection of fundamental rights regarding the use of facial recognition in law enforcement. Through an integrative literature review with a qualitative approach, based on the analysis of 37 articles selected from the Web of Science, CAPES Periodicals Portal, and Google Scholar databases, the research identifies a shift in the debate from technical efficacy to the institutional and democratic impacts of technology. The results reveal that facial recognition operates within a dense field of tension between promises of modernization and the risks of mass surveillance, algorithmic opacity, and the reproduction of structural racism. It is concluded that the social acceptability and legitimacy of the tool do not arise from formal legality alone, but depend on the construction of robust regulatory frameworks, procedural transparency, and the indispensability of human oversight, requiring that operational efficiency does not override the fundamental guarantees of the Rule of Law.

Keywords: facial recognition. law enforcement. public governance. fundamental rights. algorithmic racism.

1 Introdução

A expansão recente das tecnologias de reconhecimento facial inseriu a vigilância algorítmica no centro do debate contemporâneo sobre segurança, inteligência artificial e direitos fundamentais. Em escala internacional, a literatura tem mostrado que o reconhecimento facial passou a ocupar lugar de relevo tanto no setor privado quanto no âmbito estatal, especialmente em atividades de policiamento, controle de fronteiras, monitoramento urbano e prevenção de crimes. Nesterova (2020, p. 1-2) observa que essas tecnologias se encontram “sob o *holofote regulatório* em todo o mundo”, precisamente porque seu avanço técnico foi acompanhado por preocupações crescentes com privacidade, discriminação, democracia e Estado de Direito. Em direção semelhante, Palmiotto e González (2023, p. 4-5) sustentam que o uso de tecnologia de reconhecimento facial “altamente intrusiva”⁵ demanda proteção jurídica reforçada, sobretudo quando aplicada em espaços públicos e em tempo real.

Esse deslocamento do debate, da inovação técnica para seus efeitos institucionais e democráticos, mostra que o reconhecimento facial deixou de ser percebido apenas como ferramenta de eficiência operacional. A literatura recente insiste que sua adoção repercute sobre

5 No original, em inglês: *highly intrusive* (altamente intrusiva). No debate contemporâneo sobre proteção de dados e direitos fundamentais, o conceito de *intrusiveness* (intrusividade) refere-se ao grau de interferência ou penetração de uma determinada tecnologia na esfera privada e na autodeterminação informativa do cidadão. Tecnologias consideradas “altamente intrusivas” são aquelas que permitem a coleta de dados sensíveis ou o monitoramento constante sem o consentimento direto do titular, exigindo, por conseguinte, maior rigor regulatório e salvaguardas jurídicas.

direitos, práticas policiais e modalidades de controle estatal. Nesterova (2020, p. 2, tradução nossa) adverte que tais tecnologias podem “comprometer significativamente os direitos fundamentais, além de impactar a democracia e o Estado de Direito de modo difícil de antecipar ou mensurar”. Em chave mais crítica, Williams (2020, p. S74) argumenta que sistemas como reconhecimento facial, policiamento preditivo e biometria não devem ser avaliados apenas por critérios de precisão ou *fairness*⁶, mas também por sua inserção histórica em estruturas de vigilância anti-negra e opressão racializada.

No Brasil, esse debate ganha particular densidade diante da centralidade histórica da segurança pública na agenda institucional e social. O *Atlas da Violência 2025* (IPEA; FBSP, 2025) destaca a persistência de dificuldades de mensuração da violência letal e o problema dos homicídios ocultos, contexto que ajuda a compreender por que políticas de segurança orientadas por tecnologia ganharam espaço crescente nas últimas décadas. No caso do reconhecimento facial, Vargas e Ribeiro (2023, p. 192) mostram que o Estado da Bahia se tornou pioneiro em sua implementação como política pública de segurança em 2018, associando a tecnologia a projetos de videopoliciamento e inteligência.

A adoção brasileira do reconhecimento facial, contudo, foi acompanhada de forte controvérsia jurídico-política. Daguer, Borri e Soares (2022, p. 1-2) afirmam que a tecnologia tem sido amplamente empregada na segurança pública nacional “sem que exista uma regulamentação sobre o assunto”, o que torna urgente a definição de critérios transparentes quanto ao funcionamento desses sistemas e à proteção da intimidade, da privacidade, da honra e da imagem. Na mesma direção, Oliveira et al. observam que

a legislação da qual dispomos atualmente não sana uma série de dúvidas quanto ao uso dos dados biométricos, sobretudo para fins de segurança pública e investigação/repressão criminais, criando um vácuo normativo o que dificulta ainda mais o debate sobre os limites do emprego de dados sensíveis nesta seara (Oliveira et al., 2022, p. 127).

Vargas e Ribeiro (2023, p. 190) acrescentam que, mesmo no caso baiano, a política pública se desenvolveu em cenário de falta de transparência e ausência de regulamentação legal específica, com potenciais impactos sobre liberdade, privacidade e proteção de dados pessoais.

Por conseguinte, embora a literatura recente tenha avançado na análise de aspectos regulatórios, discriminatórios e políticos do reconhecimento facial, ainda se observa dispersão temática e insuficiente articulação entre governança pública, segurança pública e proteção de direitos fundamentais. É nesse ponto que se situa o problema desta pesquisa: *como a literatura científica tem analisado os desafios de governança pública e proteção de direitos fundamentais no uso de tecnologias de reconhecimento facial na segurança pública?*

6 *Fairness* refere-se à ausência de viés ou discriminação em um sistema automatizado. Um algoritmo é considerado “fair” (justo) quando seus resultados não dependem de variáveis sensíveis protegidas, como raça, gênero ou idade, de modo a prejudicar grupos específicos. Williams diz que não adianta “consertar o algoritmo” para que ele seja matemático e imparcial se a finalidade política e o contexto histórico de seu uso continuarem servindo para a opressão de raça.

A partir dessa questão, o objetivo geral do estudo é analisar criticamente, por meio de revisão integrativa da literatura, como a produção científica vem abordando os desafios normativos, institucionais, sociais e políticos relacionados ao uso do reconhecimento facial na segurança pública, com ênfase nos eixos de governança pública e regulação, uso da tecnologia em segurança pública, discriminação algorítmica, direitos fundamentais, vigilância estatal e legitimidade e confiança pública.

A relevância do estudo reside em oferecer uma síntese analítica capaz de integrar dimensões frequentemente tratadas de forma separada e contribuir para o debate sobre regulação, transparência, proporcionalidade, revisão humana e participação pública na formulação de políticas de reconhecimento facial. Trata-se, portanto, de problema diretamente relacionado ao exercício do poder estatal, à possibilidade de erro e discriminação e à redefinição dos limites entre segurança, liberdade e vigilância em sociedades democráticas.

2 Referencial teórico

2.1 Governança pública, regulação e uso do reconhecimento facial na segurança pública

O debate sobre reconhecimento facial na segurança pública deslocou-se de uma abordagem centrada na inovação tecnológica para uma abordagem voltada aos problemas de governança pública, regulação e controle institucional. Esse deslocamento decorre do fato de que a adoção de sistemas biométricos por órgãos estatais revelou que seus efeitos não se esgotam no plano técnico, alcançando também transparência decisória, definição de responsabilidades, legitimidade do uso estatal da tecnologia e proteção de direitos.

No caso brasileiro, Almeida (2022, p. 274) sustenta que o reconhecimento facial, quando incorporado à segurança pública sem disciplina específica, compromete parâmetros fundamentais do Estado de Direito e cria cenário de “vigilância massiva”. Em direção semelhante, Daguer, Borri e Soares (2022, p. 9) defendem critérios “transparentes e seguros” para o uso da tecnologia, dada a sensibilidade dos dados biométricos envolvidos. Gültekin-Várkonyi (2024, p. 4) analisa, sob uma ótica comparada, que os riscos do reconhecimento facial na segurança pública perpassam a acurácia e o devido processo administrativo, alertando que falhas nesses pontos podem “corroer a confiança pública, prejudicando o interesse público”. Na mesma direção, Guo e Kennedy (2023, p. 399, tradução nossa) sustentam que “O discurso sobre as tecnologias de AFR [Reconhecimento Facial Automatizado] deve ser uma questão de debate público e fiscalização regulatória”, defendendo regulação efetiva e limitação de finalidade para prevenir *function creep*⁷.

⁷ O termo *function creep* (ou alastramento de funções) refere-se ao fenômeno do *desvio de finalidade*, em que um sistema tecnológico ou banco de dados, originalmente criado para um propósito específico e restrito, passa a ser utilizado para fins secundários sem que haja uma nova base legal, transparência ou consentimento. No contexto do reconhecimento facial, o *function creep* representa um risco crítico ao princípio da limitação de finalidade (Art. 6º, I, da LGPD), uma vez que dados coletados para segurança pública podem ser indevidamente desviados para monitoramento comercial, político ou vigilância generalizada de comportamentos sociais.

No plano do uso concreto, a literatura mostra que o reconhecimento facial não pode ser compreendido como simples automatização objetiva da atividade policial.

Há uma analogia clara aqui com a forma como o Direito no policiamento passou a ser compreendido há mais de meio século. Os algoritmos de AFR [Reconhecimento Facial Automatizado] orientam e guiam a tomada de decisão dos agentes, mas não a determinam inteiramente. As regras codificadas nos algoritmos não são ‘inflexíveis’ e rígidas, mas sim configuradas e construídas por meio de uma gama de influências policiais. Os agentes tomam decisões ativas sobre os critérios de inclusão em listas de monitoramento (*watchlists*) e sobre como configurar a sensibilidade do sistema e, portanto, quais correspondências (*matches*) ele está habilitado a realizar ou não. (Fussey; Davies; Innes, 2021, p. 342, tradução nossa)

No mesmo sentido, Chen e Dai (2026, p. 1) mostram que a tecnologia combina promessa de eficiência com normalização do monitoramento cotidiano, reforçando o controle estatal “em detrimento dos direitos individuais”. Assim, a literatura indica que regulação fiscalizatória e uso da tecnologia são inseparáveis: quanto mais o reconhecimento facial reorganiza a suspeição e a intervenção estatal, mais decisiva se torna a exigência de controle democrático.

2.2 Discriminação algorítmica e direitos fundamentais

Entre os temas mais recorrentes da literatura recente está a relação entre reconhecimento facial, viés algorítmico e desigualdade racial. O debate científico evoluiu de uma crítica inicial à acurácia desigual dos sistemas para uma crítica mais ampla à sua inserção em estruturas institucionais racializadas. Em consequência, a discriminação algorítmica passou a ser tratada como uma das categorias analíticas centrais para compreender os riscos da tecnologia.

No plano brasileiro, Almeida e Souza (2025, p. 202; p. 202-212) associam o uso do reconhecimento facial à reprodução de práticas seletivas dirigidas a grupos racializados, destacando a Bahia como “grande laboratório de testes” e chamando atenção para possíveis “falsos positivos”. Coimbra, Silva e Moraes (2023, p. 139) reforçam essa leitura ao afirmarem que “o racismo jamais pode ser tido como produto de uma problemática individual”. Na argumentação de Brandner e Hirsbrunner (2023, p. 24-25), os autores mostram que a quantificação da *fairness* pode ocultar a forma concreta pela qual discriminação e opressão se traduzem socialmente, produzindo e automatizando injustiça. Esse debate se conecta diretamente aos direitos fundamentais, pois, como mostram Daguer, Borri e Soares (2022, p. 1-3), Almeida (2022, p. 265), Palmiotto e González (2023, p. 4-5) e Oliveira et al. (2022, p. 114-116), o reconhecimento facial afeta privacidade, proteção de dados, liberdade, dignidade e devido processo, especialmente quando empregado sem base normativa clara ou sem possibilidade de revisão humana. Em Macedo (2023, p. 226; p. 241-242), essa articulação aparece de forma explícita na defesa da “inafastável possibilidade de revisão humana” e do “direito à participação humana” em decisões automatizadas.

Em síntese, a literatura indica que discriminação algorítmica e violação de direitos fundamentais não são problemas paralelos, mas dimensões articuladas de um mesmo fenômeno:

o reconhecimento facial afeta direitos precisamente porque opera em contextos institucionais marcados por opacidade, seletividade penal e assimetrias raciais.

2.3 Vigilância estatal e reconfiguração do espaço público

A literatura tem compreendido o reconhecimento facial como tecnologia de vigilância estatal ampliada, cujo problema não se resume à identificação de indivíduos, mas envolve a expansão de infraestruturas de observação, rastreamento e classificação contínua da população.

Abbas da Silva, Franqueira e Hartmann (2021, p. 172) afirmam que a incorporação do reconhecimento facial às câmeras de monitoramento “elevou a política de vigilância a outro patamar”. Na mesma direção, Krivokapić et al. (2021, p. 6-7) mostram que a videovigilância constitui infraestrutura de base para ferramentas ainda mais invasivas, como reconhecimento facial e leitura automática de placas, podendo representar “ameaça substancial aos direitos humanos fundamentais”.

Sob uma perspectiva analítica, Smith (2020, p. 5) interpreta a cidade datificada⁸ como *black box city*, onde a face se converte em superfície de rastreamento e governo, enquanto Hood (2020, p. 167, tradução nossa) lê a convergência entre *body-worn cameras*⁹ e reconhecimento facial como um problema de justiça social, argumentando que a vigilância policial contemporânea cria uma nova realidade de ‘discriminação orientada por dados’ que afeta desproporcionalmente as populações mais vulneráveis. Aradau e Blanke (2021, p. 10, tradução nossa) acrescentam que o erro, no *machine learning*, tende a ser absorvido como parte da própria lógica de otimização do sistema, convertendo-se em “erro aceitável” e em “experimentação permanente através do erro”¹⁰.

Assim, o reconhecimento facial aparece na literatura não como ferramenta isolada de identificação, mas como intensificação de um regime de vigilância em que o espaço público se torna cada vez mais mensurável, classificável e governável.

2.4 Legitimidade, confiança pública e participação social

A literatura também destaca que a adoção do reconhecimento facial em segurança pública não depende apenas de base legal ou desempenho técnico, mas de legitimidade institucional

8 No original, em inglês: *datified city* (cidade datificada). O conceito refere-se ao fenômeno em que os fluxos urbanos, comportamentos e interações físicas no espaço público são convertidos em dados digitais processáveis. No contexto da *black box city* (cidade caixa-preta) proposta por Smith (2020), essa datificação permite que o Estado e algoritmos de reconhecimento facial transformem a face e o corpo dos cidadãos em objetos de mensuração, rastreamento e governança automatizada, muitas vezes sem transparência sobre os critérios de análise.

9 Trata-se de dispositivos de captura de áudio e vídeo acoplados ao uniforme ou ao corpo de agentes de segurança pública, projetados para registrar interações entre a polícia e o cidadão. No debate contemporâneo, a integração dessas câmeras com softwares de reconhecimento facial é analisada sob a ótica da vigilância biométrica em tempo real, levantando preocupações sobre a transformação do policiamento de proximidade em uma infraestrutura de monitoramento massivo e automatizado.

10 No original, em inglês: *acceptable error* (erro aceitável) e *permanent experimentation through error* (experimentação permanente através do erro). Os termos descrevem a tendência de sistemas de *machine learning* em naturalizar falhas algorítmicas (como falsos positivos) não como defeitos operacionais, mas como dados necessários para o refinamento contínuo do sistema, transformando a segurança pública em um campo de experimentação constante sobre a população.

e confiança pública. Esse eixo recoloca o debate no terreno da aceitação social, da justiça procedimental e da relação entre Estado e cidadania.

Bradford et al. (2020, p. 1516) demonstram que a opinião pública sobre o reconhecimento facial em tempo real em Londres permaneceu “praticamente dividida em 50/50”, Enquanto Li (2024, p. 10, tradução nossa) mostra que a aceitabilidade da tecnologia depende da integridade institucional, sustentando que “assegurar a integridade é mais relevante do que provar a eficácia do reconhecimento facial na resolução de crimes”. Em convergência, Brewer et al. (2022, p. 133) e Miethe et al. (2025, p. 1042-1044) indicam que o apoio social varia conforme a finalidade atribuída ao uso, o contexto policial e o nível de confiança na polícia. A literatura, no entanto, vai além da simples análise de aceitação social, com Hill, O'Connor e Slane (2022, p. 325-331) sustentando a necessidade de uma participação pública efetiva no processo de elaboração de políticas para o reconhecimento facial e Hillo, Vento e Erkkilä (2025, p. 1-2; p. 10; p. 14) evidenciando que transparência procedimental e manutenção de controle humano aumentam a legitimidade percebida de decisões automatizadas.

Dessa forma, a literatura indica que legitimidade e confiança pública não são efeitos automáticos da legalidade formal ou da promessa de eficiência; elas dependem de integridade institucional, transparência, explicabilidade, possibilidade de contestação e participação democrática. Em conjunto, os quatro eixos do referencial mostram que o reconhecimento facial, quando aplicado à segurança pública, mobiliza problemas simultaneamente normativos, institucionais, raciais, democráticos e de direitos fundamentais.

3 Metodologia

3.1 Delineamento da pesquisa e pergunta norteadora

Este trabalho caracteriza-se como uma revisão integrativa da literatura de abordagem qualitativa desenvolvida para reunir, comparar e sintetizar criticamente produções científicas acerca do uso de tecnologias de reconhecimento facial na segurança pública, com foco nos desafios de governança pública e proteção de direitos fundamentais.

A escolha desse delineamento decorre de sua adequação ao tratamento de problemas complexos e interdisciplinares, especialmente quando a literatura disponível reúne estudos com diferentes desenhos metodológicos, enfoques teóricos e estratégias analíticas que Whittemore e Knafl (2005) destacam como atributos da Revisão Integrativa, que permite a amálgama de metodologias, enquanto Souza, Silva e Carvalho (2010) e Mendes, Silveira e Galvão (2008) reconhecem a Revisão integrativa na qualidade de procedimento que busca, analisa criticamente e sintetiza as evidências disponíveis sobre um tema delimitado.

A investigação foi norteadora pela seguinte questão: de que forma a literatura científica tem tratado a respeito dos desafios da governança pública e do respeito a direitos fundamentais em face do uso de tecnologias de reconhecimento facial destinadas à segurança pública?

Para respondê-la, a revisão foi estruturada em seis eixos analíticos: (i) governança e marcos regulatórios; (ii) emprego do reconhecimento facial na segurança pública; (iii) discriminação algorítmica; (iv) direitos fundamentais; (v) vigilância estatal; e (vi) legitimidade e confiança pública. Tais eixos serviram como operadores interpretativos para examinar os processos de controle da tecnologia, suas manifestações operacionais e suas repercussões institucionais, jurídicas e sociopolíticas.

3.2 Estratégia de busca e fontes do conhecimento.

A coleta de dados foi realizada nas bases *Web of Science*, Portal de Periódicos da CAPES e Google Acadêmico. A estratégia de busca consistiu na combinação de descritores nos idiomas português e inglês, articulados por meio de operadores booleanos (*AND*, *OR*). Os termos-chave incluíram variações de “reconhecimento facial” (*facial recognition*) cruzados com “policiamento” (*policing*), “governança algorítmica” (*algorithmic governance*), “direitos fundamentais” (*fundamental rights*), “viés algorítmico” (*algorithmic bias*), “segurança pública” e “racismo”. As buscas foram customizadas conforme as especificidades de cada base, utilizando aspas para a exata delimitação de termos compostos.

Estabeleceu-se o recorte temporal prioritário entre 2021 e 2026, com extensões pontuais a 2020 para a inclusão de obras seminais ou para suprir a baixa incidência de publicações estritamente alinhadas ao problema de pesquisa em eixos específicos. Devido à relativa escassez de estudos sobre o objeto nas bases indexadas, realizou-se uma busca complementar em língua portuguesa, prioritariamente no Google Acadêmico e no Portal de Periódicos CAPES. Reitera-se, contudo, que o critério de elegibilidade restringiu a seleção final apenas a artigos publicados em periódicos científicos revistos por pares.

3.3 Critérios para inclusão, exclusão e seleção do corpus

Foram incluídos artigos de periódicos científicos que apresentassem conexão direta com o reconhecimento facial, biometria ou vigilância algorítmica, desde que articulados aos eixos de segurança pública, governança, proteção de dados e direitos fundamentais. Estabeleceu-se como requisito a disponibilidade do texto integral e a publicação nos idiomas português, inglês ou espanhol.

Como critérios de exclusão, descartaram-se: (i) documentos duplicados; (ii) estudos estritamente técnicos ou de engenharia sem discussão sobre governança ou impactos sociais; e (iii) literatura cinzenta (monografias, trabalhos de conclusão de curso e teses), priorizando-se a produção científica submetida à revisão por pares.

Na etapa de identificação, foram levantados 219 registros. Após a remoção de duplicidades e triagem preliminar, restaram 133 documentos, os quais foram exportados em formato RIS para

o gerenciador bibliográfico Zotero para a fase de triagem analítica. Esta etapa consistiu no exame de títulos, resumos e palavras-chave sob o prisma da aderência temática.

Para a fase de seleção, procedeu-se à leitura integral dos textos mais promissores. Ao final, foram analisados 40 documentos em PDF, resultando em um *corpus* final de 37 artigos. Os 3 documentos remanescentes foram excluídos por não atenderem ao critério de tipo documental (duas monografias e uma tese), servindo apenas como apoio bibliográfico contextual.

3.4 Extração, organização e análise dos dados

A extração e a sistematização dos dados foram viabilizadas por uma matriz de síntese, desenvolvida como instrumento central para assegurar a comparabilidade entre os estudos. Para cada artigo, registraram-se: autoria e ano; título; contexto geográfico; objetivos; delineamento metodológico; principais resultados; categorias teóricas; e a relação direta com a pergunta norteadora. A leitura integral dos documentos permitiu o mapeamento de trechos citáveis com indicação exata de páginas, garantindo a rastreabilidade analítica e a fidedignidade das fontes consultadas.

A análise do *corpus* fundamentou-se em uma síntese temática orientada pelos seis eixos analíticos previamente definidos. Esse processo levou em conta os conceitos mobilizados e as contribuições específicas de cada obra para a compreensão dos desafios da governança e dos direitos fundamentais. A análise crítica, de natureza qualitativa e integrativa, buscou articular os argumentos dos estudos incluídos, evitando uma simples enumeração descritiva.

A avaliação da qualidade dos textos baseou-se em uma análise de consistência interna, examinando-se a coerência entre o problema proposto, o rigor metodológico, a fundamentação teórica e a contribuição efetiva para o campo da segurança pública e do direito.

3.5 Transparência do fluxo de seleção, limitações e aspectos éticos.

A descrição das etapas de identificação, triagem, elegibilidade e inclusão dos estudos seguiu as diretrizes de transparência do PRISMA 2020 (Page et al., 2021). Ressalte-se que o protocolo não foi adotado como método autônomo, mas como ferramenta de relato do fluxo de seleção, em consonância com o modelo de revisão integrativa proposto por Whitemore e Knafl (2005) e Souza, Silva e Carvalho (2010).

Como em toda revisão bibliográfica, este estudo apresenta limitações. A primeira reside na heterogeneidade do *corpus*, que reúne abordagens jurídicas, empíricas e teórico-críticas; embora tal diversidade amplie a riqueza analítica, impõe desafios a comparações lineares entre os resultados. A segunda refere-se à delimitação do escopo de busca, restrito a bases e descritores específicos, ainda que mitigada pela busca complementar em língua portuguesa. A terceira diz respeito ao recorte documental, que priorizou artigos de periódicos em detrimento da literatura cinzenta (teses e monografias), visando assegurar a certificação por pares. Por fim, reconhece-se a

ausência de um protocolo de pontuação (*scoring*) metodológico, visto que a qualidade dos textos foi aferida por meio de leitura analítica orientada pela coerência e contribuição ao problema de pesquisa.

No âmbito ético, esta revisão integrativa fundamentou-se exclusivamente em textos científicos de domínio público, sem envolver experimentação com seres humanos ou coleta de dados identificáveis. Consequentemente, o trabalho é isento de registro e avaliação pelo Sistema CEP/Conep, nos termos da Resolução CNS nº 510/2016 (Art. 1º, parágrafo único, incisos III e VI). A despeito da dispensa de submissão formal, a pesquisa foi conduzida sob os princípios da integridade científica e da honestidade intelectual, assegurando a fidedignidade das citações e a responsabilidade na interpretação crítica das fontes. A Resolução CNS nº 466/2012, por sua vez, disciplina pesquisas envolvendo seres humanos, hipótese que não se verifica no presente estudo (BRASIL, 2012).

4 Resultados e discussão

A análise do *corpus* de 37 artigos revela que a literatura científica contemporânea deixou de tratar o reconhecimento facial na segurança pública como uma mera inovação operacional. O que emerge dos estudos é a compreensão da tecnologia como um dispositivo situado em um denso campo de tensões, onde se cruzam promessas de eficiência, práticas de vigilância, vieses discriminatórios e crises de legitimidade institucional sob um cenário de nítido déficit regulatório. Em conjunto, as evidências indicam que o debate atual superou a pergunta inicial sobre a viabilidade técnica da ferramenta; o foco agora recai sobre as condições de sua implementação, as fronteiras jurídicas de sua aplicação e, sobretudo, os custos democráticos e sociais impostos por sua adoção.

4.1 Governança pública e regulação: do déficit normativo à exigência de controle democrático

O primeiro achado recorrente desta revisão é o descompasso entre a velocidade da inovação tecnológica e a construção de anteparos jurídicos. A literatura converge para a percepção de que o reconhecimento facial tem sido integrado às forças de segurança em um ritmo muito superior à consolidação de marcos administrativos e institucionais capazes de disciplinar seu uso.

No contexto brasileiro, nota-se uma preocupação central com a metamorfose do espaço público. Os estudos de Almeida (2022) e Daguer, Borri e Soares (2022) sinalizam que, sem uma disciplina específica, a tecnologia transita de uma ferramenta de investigação para um sistema de vigilância massiva, onde a sensibilidade dos dados biométricos exige critérios de transparência que o atual estágio regulatório ainda não alcança plenamente.

Essa lacuna normativa é apontada por Oliveira et al. (2022) como um fator de risco para o uso indevido de dados pessoais, reforçando a tese de que a regulamentação não deve ser apenas um ato burocrático, mas um processo de construção democrática. Nessa perspectiva, Chenou e

Rodríguez Valenzuela (2021) observam que a intervenção algorítmica no setor público, quando legitimada apenas por discursos de eficiência, tende a aprofundar opacidades e exclusões. Em linha complementar, Meloni (2026) adverte que respostas regulatórias meramente corretivas são insuficientes para enfrentar, por si sós, os problemas estruturais inerentes ao policiamento algorítmico. Assim, autores como Magalhães e Gomes (2021) destacam que a legitimidade dessas ferramentas depende de um diálogo aberto com a comunidade acadêmica e a sociedade civil, evitando que o imperativo da eficiência se sobreponha às garantias de privacidade e imagem dos cidadãos.

4.2 Uso do reconhecimento facial na segurança pública: promessa de eficiência e reconfiguração da suspeição

Os achados da revisão indicam que o reconhecimento facial não opera como uma automatização isolada ou puramente objetiva. Pelo contrário, o que emerge da literatura é um arranjo sociotécnico em que o algoritmo atua como um vetor de orientação, e não de substituição, da decisão humana. Essa distinção é fundamental: ao analisarem o caráter “assistido” da tecnologia, Fussey, Davies e Innes (2021) demonstram que a ferramenta não encerra a discricionariedade policial, mas a desloca para uma nova moldura técnica. Nesse cenário, o que se observa é a consolidação de uma suspeição burocrática de matriz tecnológica, na qual os critérios de monitoramento e os *thresholds*¹¹ algorítmicos passam a mediar quem é, ou não, digno de intervenção estatal.

Essa reconfiguração da vigilância ganha contornos específicos quando confrontamos contextos globais e locais. Enquanto no cenário internacional a tecnologia é frequentemente associada a uma normalização do controle que fragiliza garantias individuais — como aponta a análise de Chen e Dai (2026) sobre o modelo chinês —, no Brasil o fenômeno assume uma gramática própria. A expansão territorial do reconhecimento facial em estados como a Bahia revela uma narrativa de modernização institucional que, por vezes, ignora a profundidade dos riscos envolvidos.

Nota-se, conforme o levantamento, que programas governamentais tendem a omitir as criticidades da ferramenta (Melo; Serra, 2022), favorecendo uma lógica de “urbanismo militar” e vigilância preventiva (Pereira, 2025). Ainda que vozes na literatura enfatizem o ganho em eficiência operacional e a otimização do policiamento (Oliveira; Mello, 2025), a síntese dos dados aponta para uma tensão insolúvel: o imperativo da modernização técnica raramente é acompanhado pela transparência necessária para conter o arbítrio institucional.

11 O termo *threshold* (limiar de similaridade ou de confiança) designa o parâmetro estatístico predefinido que converte a pontuação de probabilidade gerada pelo algoritmo em uma decisão binária de identificação. Na prática do reconhecimento facial, a calibração deste índice representa um ponto crítico de governança: limiares mais baixos tendem a aumentar a taxa de “falsos positivos” (identificações errôneas de inocentes), ampliando o risco de abordagens policiais indevidas; já limiares excessivamente altos podem elevar os “falsos negativos”, reduzindo a eficácia operacional do sistema. A definição desse valor não é meramente técnica, mas envolve uma escolha política e jurídica sobre a margem de erro tolerada pelo Estado e a distribuição social desses riscos.

4.3 Discriminação algorítmica: do problema do viés à crítica da estrutura racializada

A revisão bibliográfica aponta uma convergência nítida: a discriminação algorítmica, especialmente em seu recorte racial, é o nó crítico da implementação do reconhecimento facial na segurança pública. O que emerge da análise dos textos é o entendimento de que a tecnologia não inaugura novos preconceitos, mas atua como um catalisador de estruturas institucionais já atravessadas pela seletividade penal e pela racialização do controle social.

No cenário brasileiro, a experiência acumulada em estados como a Bahia serve de evidência para o risco dos “falsos positivos”, conforme discutido por Almeida e Souza (2025). Essa falibilidade técnica, contudo, ganha contornos de violência institucional quando se observa que o erro não é distribuído de forma aleatória: ele recai, de modo desproporcional, sobre corpos negros. Como sugerem Coimbra, Silva e Moraes (2023) e Garcia, Oliveira e Teló (2025), a opacidade desses sistemas — as chamadas “caixas-pretas” — acaba por automatizar padrões históricos de suspeição, impossibilitando a transparência necessária para a defesa de direitos fundamentais.

A literatura mais recente transcende a mera métrica de acurácia para questionar a própria neutralidade do aparato técnico. Ao invés de buscar apenas sistemas “mais justos”, autores como Brandner e Hirsbrunner (2023), Sievers e Guadalupe Silveira (2023), Silva (2023) e Williams (2020) apontam que a quantificação da justiça (*fairness*) pode mascarar opressões sociais concretas. O resultado central deste eixo revela, portanto, que o viés algorítmico não deve ser tratado como um defeito reparável por meio de ajustes de código, mas como um dispositivo inscrito em lógicas de vigilância e necro-política que exigem uma resistência não apenas técnica, mas profundamente política e jurídica.

4.4 Direitos fundamentais: privacidade, proteção de dados, devido processo e revisão humana

Os achados deste eixo consolidam a percepção de que o reconhecimento facial atua como uma tecnologia de alta densidade interventiva, cujas repercussões transcendem a esfera da privacidade individual. O *corpus* analisado aponta que a ferramenta impacta um feixe de garantias constitucionais, incluindo a liberdade de expressão, a dignidade da pessoa humana e o devido processo legal. Ao examinarem precedentes internacionais, como o caso *Glukhin v. Russia*, Palmiotto e González (2023) argumentam que a intrusividade desse monitoramento em contextos de manifestação pública é frontalmente incompatível com as premissas de uma sociedade democrática.

Essa preocupação com a integridade do Estado de Direito é reforçada pela exigência de proporcionalidade. De acordo com Macri Júnior, Macri e Frontini (2023), a tecnologia não pode ser naturalizada como um recurso ordinário do policiamento sem que haja uma demonstração clara de sua necessidade e adequação em cada caso concreto. No contexto brasileiro, a garantia

dessa barreira contra o arbítrio encontra amparo na tese de Macedo (2023), que defende a indispensabilidade da revisão humana. Para o autor, a participação de um agente no ciclo decisório não é apenas uma etapa técnica, mas um direito do cidadão de não ser submetido exclusivamente a julgamentos automatizados.

Por fim, a proteção da identidade biométrica emerge como um pilar central de segurança jurídica. A convergência entre os estudos de Daguer, Borri e Soares (2022), Oliveira et al. (2022) e Nesterova (2020) demonstra que a gestão desses dados exige um rigoroso controle sobre a finalidade do uso e a segurança informacional. O resultado mais expressivo desta análise é a rejeição da falsa dicotomia entre segurança e privacidade; o que a literatura revela é que o reconhecimento facial, se desprovido de limites claros, corre o risco de converter o indivíduo em um objeto permanente de rastreamento e suspeição antecipada.

4.5 Vigilância estatal: infraestrutura, cidade monitorada e normalização do controle

O que se depreende da análise do *corpus* é que o reconhecimento facial deixou de ser um fenômeno periférico para se tornar o epicentro de um ecossistema de vigilância estatal em expansão. Os dados revelam que a ferramenta opera como um motor de integração entre *smart cities*, bases biométricas e *body-worn cameras*, consolidando uma estrutura de monitoramento sem precedentes. Como colocam Abbas da Silva, Franqueira e Hartmann (2021), essa articulação leva o controle no domínio público a um novo patamar de ubiquidade, o que encontra eco na metáfora do ‘big brother’ público, criada por Melo e Serra (2022). Sob esse olhar, a videovigilância convencional deixa de ser um princípio em si mesma e se torna, como chamam Krivokapić et al. (2021), o ponto de partida para tecnologias ainda mais “intrusivas”.

Em uma perspectiva teórica, a convergência dos dados implica uma mudança na própria essência do espaço urbano. A face humana é despojada do seu tratamento de traço de identidade e ganha contornos como superfície de rastreamento e de governo, em particular na “cidade caixa-preta” (*black box city*), conceito esse empregado por Smith (2020) para falar da opacidade destes fluxos datificados. Para além do avanço técnico, o que se pode retirar da literatura é que há uma inquietação com o tema da justiça social; Hood (2020) aduz que a articulação entre câmeras corporais e biometria facial sobrecarregam as populações mais vulneráveis, fazendo do policiamento de proximidade uma rede de captura biométrica em massa.

Finalmente, um dos resultados mais provocantes deste eixo reside na naturalização da falha. A lógica do machine learning permite ao erro deixar de ser encarado como defeito para ser absorvido como conhecimento inerente ao aperfeiçoamento do sistema. Este movimento de “experimentação permanente através do erro”, sinalizado por Aradau e Blanke (2021), parece indicar que a sociedade assimilaria um laboratório contínuo, no qual as falhas algorítmicas seriam toleradas em nome da otimização técnica. Em suma, o reconhecimento facial institucionaliza uma mutação do policing (policiamento) reativo para um regime de vigilância preventiva e remota, ressignificando a relação entre o Estado e o cidadão em espaço público.

4.6 Legitimidade e confiança pública: aceitação social, integridade institucional e participação

O eixo final da revisão revela que a viabilidade do reconhecimento facial não se esgota na precisão do algoritmo ou na existência de uma lei autorizativa; ela reside, fundamentalmente, na percepção de legitimidade por parte da sociedade. Os dados mostram que a opinião pública está longe de um consenso. Ao analisar o cenário de Londres, Bradford et al. (2020) sinalizam uma divisão profunda na aceitação da tecnologia, evidenciando que, para parcela significativa da população, o monitoramento em tempo real é percebido como intrusivo ou eticamente questionável.

Essa hesitação social encontra uma explicação direta no fator confiança. Os achados de Li (2024) sugerem que a integridade da instituição que opera o sistema é mais determinante para o apoio público do que a própria promessa de redução da criminalidade. Em outras palavras, a eficácia técnica não substitui a confiança institucional. Essa percepção é reforçada por Brewer et al. (2022) e Miethe et al. (2025), que ponderam que o suporte social é volátil e depende estritamente do contexto de aplicação, da finalidade do uso e do histórico de relação entre a polícia e a comunidade.

A literatura, contudo, aponta que a legitimidade não deve ser apenas medida, mas construída. Nesse sentido, Hill, O'Connor e Slane (2022) defendem que a formulação de políticas sobre biometria facial exige um engajamento público substantivo, retirando o debate dos gabinetes técnicos para a arena democrática. Complementarmente, os estudos de Hillo, Vento e Erkkilä (2025) demonstram que a transparência sobre os processos e a garantia de que um ser humano mantenha o controle final sobre as decisões são elementos que elevam a confiança percebida. Em síntese, os resultados indicam que a autoridade estatal não basta para legitimar a tecnologia; a aceitação depende de um ecossistema de transparência, integridade e participação ativa do cidadão.

5 Considerações finais

A análise empreendida nesta revisão integrativa revela que a literatura científica deixou de tratar o reconhecimento facial como uma mera ferramenta de eficiência para situá-lo em um campo de profundas disputas éticas e políticas. O que emerge do *corpus* analisado é a compreensão de que os desafios de governança e a proteção de direitos fundamentais não são agendas paralelas, mas dimensões intrinsecamente interdependentes. A tecnologia, portanto, não é um instrumento neutro; ela é um dispositivo que tensiona os limites entre a segurança pública e as garantias democráticas.

No eixo da governança, os achados confirmam um crônico descompasso: a velocidade da implementação técnica atropela a construção de marcos regulatórios. No plano do uso concreto, a literatura prova que a inteligência artificial não elimina o arbítrio policial, mas o camufla sob

uma aparência de objetividade técnica, reorganizando a suspeição em molduras sociotécnicas opacas. Quanto à discriminação algorítmica, o estudo demonstra que o viés não é apenas um erro de programação, mas um sintoma de estruturas institucionais racializadas. Nesse sentido, o reconhecimento facial não apenas herda, mas automatiza e escala a seletividade penal histórica.

No campo dos direitos fundamentais, a revisão evidencia que a intrusividade da biometria facial afeta um feixe de garantias que vai muito além da privacidade, alcançando a dignidade e o devido processo legal — o que torna a revisão humana uma salvaguarda inegociável. Por fim, a discussão sobre legitimidade indica que a eficácia operacional não é capaz de fabricar confiança pública; esta depende, necessariamente, de transparência, integridade institucional e da participação ativa da sociedade civil na formulação de políticas tecnológicas.

Dessa forma, o principal achado desta pesquisa transcende a identificação de riscos isolados. A evidência central é que o reconhecimento facial reconfigura o modo como o Estado observa, classifica e exerce poder sobre os cidadãos no espaço público. A literatura mais consistente, portanto, não advoga por uma aceitação cega, nem por uma recusa abstrata, mas propõe uma reavaliação crítica sobre as condições sob as quais o Estado pode — ou não deve — vigiar sua população. Como contribuição, esta síntese oferece uma moldura interpretativa integrada para futuras pesquisas e políticas públicas, reforçando que, em uma democracia, a eficiência técnica jamais deve ser buscada à revelia do controle social e do respeito incondicional aos direitos fundamentais.

Referências

ABBAS DA SILVA, Lorena; FRANQUEIRA, Bruna Diniz; HARTMANN, Ivar A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. *Revista Digital de Direito Administrativo*, Ribeirão Preto, v. 8, n. 1, p. 171-204, 2021.

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para perseguição penal. *Revista Brasileira de Segurança Pública*, [S. l.], v. 16, n. 2, p. 264-283, 2022.

ALMEIDA, José Antonio Caldeira de; SOBRAL DE SOUZA, Patrícia Verônica Nunes Carvalho. Tecnologias de reconhecimento facial: o racismo algorítmico como instrumento de política de segurança pública. *Revista Eletrônica Direito e Política*, [S. l.], v. 20, n. 1, p. 202-219, 2025.

ARADAU, Claudia; BLANKE, Tobias. Algorithmic surveillance and the political life of error. *Journal for the History of Knowledge*, [S. l.], v. 2, n. 1, p. 1-13, 2021.

BRADFORD, Ben et al. Live facial recognition: trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology*, [S. l.], v. 60, n. 6, p. 1502-1522, 2020.

BRANDNER, Lou Therese; HIRSBRUNNER, Simon David. Algorithmic fairness in police investigative work: ethical analysis of machine learning methods for facial recognition. *TATuP*

- *Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, [S. l.], v. 32, n. 1, p. 24-29, 2023.

BRASIL. Conselho Nacional de Saúde. Resolução nº 466, de 12 de dezembro de 2012. Aprova as diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos. Brasília, DF: Conselho Nacional de Saúde, 2012.

BRASIL. Conselho Nacional de Saúde. Resolução nº 510, de 7 de abril de 2016. Dispõe sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais. Brasília, DF: Conselho Nacional de Saúde, 2016.

BREWER, Paul R. et al. Eyes on the streets: media use and public opinion about facial recognition technology. *Bulletin of Science, Technology & Society*, [S. l.], v. 42, n. 4, p. 133-143, 2022.

CHEN, Xinyuan; DAI, Mengliang. Dilemmas of facial recognition technology in Chinese digital policing: a qualitative exploration. *Asian Journal of Criminology*, [S. l.], v. 21, art. 2, 2026.

CHENOU, Jean-Marie; RODRÍGUEZ VALENZUELA, Laura Estefanía. Habeas data, habemus algorithms: algorithmic intervention in public interest decision-making in Colombia. *Law, State and Telecommunications Review*, [S. l.], v. 13, n. 2, p. 56-77, 2021.

COIMBRA, Jéssica Pérola Melo; SILVA, Adrian Barbosa e; MORAES, Liliane Correia. Interseções entre racismo algorítmico, reconhecimento facial e segurança pública no Brasil. *Revista Direito, Políticas Públicas e Desenvolvimento na Amazônia*, [S. l.], v. 4, n. 2, p. 136-160, 2023.

DAGUER, Beatriz; BORRI, Luiz Antonio; SOARES, Rafael Junior. O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia fundamental. *Revista de Direito e as Novas Tecnologias*, São Paulo, v. 16, ano 5, jul./set. 2022.

FUSSEY, Pete; DAVIES, Bethan; INNES, Martin. 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. *The British Journal of Criminology*, [S. l.], v. 61, n. 2, p. 325-344, 2021.

GARCIA, Danielly; OLIVEIRA, Lorena Gonçalves; TELÓ, Vinícius Pedro. Reconhecimento facial na segurança pública no Brasil: riscos e seletividade penal. *Revista Camalotes*, Campo Grande, v. 4, n. 1, 2025.

GÜLTEKIN-VÁRKONYI, Gizem. Navigating data governance risks: facial recognition in law enforcement under EU legislation. *Internet Policy Review*, [S. l.], v. 13, n. 3, 2024.

GUO, Zhilong; KENNEDY, Lewis. Policing based on automatic facial recognition. *Artificial Intelligence and Law*, [S. l.], v. 31, p. 397-443, 2023.

HILL, Dallas; O'CONNOR, Christopher D.; SLANE, Andrea. Police use of facial recognition technology: the potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, [S. l.], v. 24, n. 3, p. 325-335, 2022.

HILLO, Jaakko; VENTO, Isak; ERKKILÄ, Tero. Algorithmic governance: experimental evidence on citizens' and public administrators' legitimacy perceptions of automated decision-

making. *Public Administration*, [S. l.], p. 1-16, 2025.

HOOD, Jacob. Making the body electric: the politics of body-worn cameras and facial recognition in the United States. *Surveillance & Society*, [S. l.], v. 18, n. 2, p. 157-169, 2020.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA; FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. *Atlas da violência 2025*. Brasília, DF: Ipea; FBSP, 2025.

KRIVOKAPIĆ, Đorđe et al. Comparative analysis of video surveillance regulation in data protection laws in the former Yugoslav states. *Journal of Regional Security*, [S. l.], v. 16, n. 1, p. 5-26, 2021.

LI, Robin Guohuibin. Institutional trustworthiness on public attitudes toward facial recognition technology: evidence from U.S. policing. *Government Information Quarterly*, [S. l.], v. 41, art. 101941, 2024.

MACEDO, Caio Sperandeo de. O direito à revisão das decisões automatizadas de reconhecimento facial e o princípio antropológico. *Revista de Direito Brasileira*, Florianópolis, SC, v. 36, n. 13, p. 226-246, 2023.

MACRI JÚNIOR, José Roberto; MACRI, Bianka Jaquetti; FRONTINI, Helena. Considerações acerca do uso de tecnologias de reconhecimento facial como instrumento de segurança pública. *Revista Científica Integrada*, [S. l.], v. 6, n. 1, e202320, 2023.

MAGALHÃES, Alice Azevedo; GOMES, Tício Spínola. Regulação de sistemas de reconhecimento facial para fins de segurança pública no Brasil: riscos e desafios. *Humanidades & Inovação*, [S. l.], v. 8, n. 47, p. 168-182, 2021.

MELO, Paulo Victor; SERRA, Paulo. Tecnologia de reconhecimento facial e segurança pública nas capitais brasileiras: apontamentos e problematizações. *Comunicação e Sociedade*, [S. l.], v. 42, p. 205-220, 2022.

MELONI, Francesca. Facial recognition on trial: data protection, discrimination, and the ethics of algorithmic governance in policing. *Information & Communications Technology Law*, [S. l.], 2026.

MENDES, Karina Dal Sasso; SILVEIRA, Renata Cristina de Campos Pereira; GALVÃO, Cristina Maria. Revisão integrativa: método de pesquisa para a incorporação de evidências na saúde e na enfermagem. *Texto & Contexto – Enfermagem*, Florianópolis, v. 17, n. 4, p. 758-764, 2008.

MIETHE, Terance D. et al. Facial recognition technology in policing: a national survey of public support for this technology and privacy/safety concerns. *Crime & Delinquency*, [S. l.], v. 71, n. 4, p. 1025-1051, 2025.

NESTEROVA, Irena. Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world. *SHS Web of Conferences*, [S. l.], v. 74, art. 03006, 2020.

OLIVEIRA, Cesar Augusto de; MELLO, Carlos Cesar de. O uso da tecnologia pela Polícia Militar do Paraná: inovações e impactos na eficiência do policiamento. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, São Paulo, v. 11, n. 1, p. 1063-1073, jan. 2025.

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, jan./mar. 2022.

PAGE, Matthew J. et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, London, v. 372, art. n71, 2021. Disponível em: <https://www.bmj.com/content/372/bmj.n71>. Acesso em: 28 mar. 2026.

PALMIOTTO, Francesca; GONZÁLEZ, Natalia Menéndez. Facial recognition technology, democracy and human rights. *Computer Law & Security Review*, [S. l.], v. 50, 2023.

PEREIRA, Letícia Pádua. Dispersão da tecnologia de reconhecimento facial no âmbito da segurança pública brasileira: sintomas da mescla do urbanismo militar à retórica de guerra preventiva. *Res Severa Verum Gaudium*, Porto Alegre, v. 10, n. 1, p. 65-91, ago. 2025.

ROSA, Pablo Ornelas et al. Efeitos da biometria na segurança pública brasileira: uma análise sobre reconhecimento facial e racismo algorítmico. *Revista de Geopolítica*, São José dos Pinhais, v. 16, n. 5, p. 1-19, 2025.

SIEVERS, Juliele Maria; GUADALUPE SILVEIRA, Luís Gustavo. Reflexões filosóficas sobre racismo e tecnologia. *Trilhas Filosóficas*, Caicó, ano 16, n. 2, p. 261-277, 2023.

SILVA, Tarcízio. Algorithmic Necropolitics. *Sexualidad, Salud y Sociedad – Revista Latinoamericana*, [S. l.], n. 39, e22304, 2023.

SMITH, Gavin J. D. The politics of algorithmic governance in the black box city. *Big Data & Society*, [S. l.], v. 7, n. 2, p. 1-9, jul./dez. 2020.

SOUZA, Marcela Tavares de; SILVA, Michelly Dias da; CARVALHO, Rachel de. Revisão integrativa: o que é e como fazer. *Einstein (São Paulo)*, São Paulo, v. 8, n. 1, p. 102-106, jan. 2010.

VARGAS, Érica Nascimento Pinheiro; RIBEIRO, Mônica Matos. Reconhecimento facial como política de segurança pública no estado da Bahia. *Terceiro Milênio: Revista Crítica de Sociologia e Política*, [S. l.], v. 22, n. 3, p. 190-216, set./dez. 2023.

WHITTEMORE, Robin; KNAFL, Kathleen. The integrative review: updated methodology. *Journal of Advanced Nursing*, Oxford, v. 52, n. 5, p. 546-553, dez. 2005.

WILLIAMS, Damien Patrick. Fitting the description: historical and sociotechnical elements of facial recognition and anti-black surveillance. *Journal of Responsible Innovation*, [S. l.], v. 7, supl. 1, p. 74-83, 2020.