



**UNIVERSIDADE CATÓLICA DO SALVADOR
CURSO DE DIREITO**

ARIELE APARECIDA DE ALQUINO MIRANDA

**RECONHECIMENTO FACIAL COMO POLÍTICA PÚBLICA DE SEGURANÇA:
ANÁLISE CONSTITUCIONAL DE SUA COMPATIBILIDADE COM OS DIREITOS
FUNDAMENTAIS**

Salvador

2026

ARIELE APARECIDA DE ALQUINO MIRANDA

**RECONHECIMENTO FACIAL COMO POLÍTICA PÚBLICA DE SEGURANÇA:
ANÁLISE CONSTITUCIONAL DE SUA COMPATIBILIDADE COM OS DIREITOS
FUNDAMENTAIS**

Artigo científico destinado ao Trabalho de Conclusão de Curso – TCC, apresentado à Coordenação do Curso de Direito da Universidade Católica do Salvador (UCSal), como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Prof. Me. Ilton Leão

Salvador

2026

ARIELE APARECIDA DE ALQUINO MIRANDA

**RECONHECIMENTO FACIAL COMO POLÍTICA PÚBLICA DE SEGURANÇA:
ANÁLISE CONSTITUCIONAL DE SUA COMPATIBILIDADE COM OS DIREITOS
FUNDAMENTAIS**

Artigo científico apresentado à Universidade Católica do Salvador (UCSal), Curso de Direito, como requisito parcial para a obtenção do grau de Bacharel em Direito.

Aprovado em _____ de _____ de 2026.

BANCA EXAMINADORA

Prof. Me. Ilton Leão (Orientador)
Universidade Católica do Salvador (UCSal)

Prof(a). [Nome do(a) Examinador(a)]
Universidade Católica do Salvador (UCSal)

Dedico, com muito amor e carinho, a obra aos meus queridos pais, aos meus familiares e por fim aos meus ilustres professores que me auxiliaram durante toda essa trajetória.

AGRADECIMENTOS

Inicialmente, agradeço primeiramente à Deus, que com toda a sua misericórdia e amor, me concedeu forças e discernimento, para persistir em busca deste sonho, que hoje se tornou realidade.

Mesmo em meio a todas as adversidades que surgiram neste longo e doloroso processo, não me deixou fraquejar, tampouco desistir. Nas inúmeras vezes em que me senti sem forças, me mostrava que eu não estava sozinha, que estava ao meu lado, que tudo fazia parte do processo. E Deus não é homem para que minta; nem filho do homem, para que se arrependa. E se Ele me prometeu, eu não tinha dúvidas de que Ele faria acontecer.

Com o passar dos dias, tenho presenciado a materialização de forma progressiva, sólida e concreta dos meus sonhos e projetos. Às vezes, parecia que a promessa estava muito distante da realização; parecia que eu estava sonhando alto demais, querendo demais, e que a finalização do curso nunca iria acontecer.

Mas, no fundo eu sentia que ele que me fez a promessa, é fiel para cumprir. Ainda que passassem céus e terras, todas as promessas, certamente se cumpriria. E, por fim, aqui me encontro, contemplando com alegria e gratidão as promessas de Deus.

Aos meus pais, todo o meu agradecimento e reconhecimento. Em especial a minha amada, “Deusa Soberana”, apelido carinhoso dado a minha mãe, que sob muito sol e chuva, foi quem sempre me sustentou e encorajou. Enquanto eu caminhava, ela enfrentava o cansaço, o medo e as renúncias em silêncio, para que eu pudesse chegar até aqui, na sombra. A vida sempre tentou cortar as asas dela a vida inteira, mas a minha amada mãe, nunca permitiu que cortassem as minhas. E mesmo sem poder voar, me ensinou a voar alto. Quando eu quase parei, ela foi o meu abrigo. Quando eu duvidei, ela sempre foi certeza. E quando o peso era grande demais para mim, ela sempre segurou por nós duas.

Hoje eu chego aonde chego, porque ela nunca soltou minha mão. Se eu venci, foi porque a minha Deusa acreditou primeiro. Se eu cheguei e estou aqui, foi porque ela sempre foi a minha base, força e amor. Essa formação é minha, mas essa conquista é nossa, minha mãe.

Ao meu pai, gratidão! O senhor abriu portas, quebrou barreiras e me ensinou, que por sermos pretos, muitas vezes precisamos ser duas vezes melhores, e que o caminho para isso é o estudo. É ocupar espaços que, por muito tempo, disseram que não eram feitos para nós. O senhor me ensinou resistência; me ensinou perseverança; me ensinou que inteligência também é força. E, quando se fala em determinação, em perseverar e insistir até alcançar meus objetivos, o Senhor sempre será a minha maior

inspiração e referência. Obrigada por ter visto em mim um potencial que, talvez, nem eu enxergasse; obrigada por não ter permitido que eu me conformasse com uma vida comum.

Presto os meus agradecimentos aos meus familiares e amigos, em especial aos amigos que ganhei durante a vida acadêmica.

E, por fim, agradeço a todos os professores que, com notável competência, transmitiram seus conhecimentos e que tive a honra de conhecer, com quem pude aprender um pouco sobre o Direito, aos quais deixo meus mais profundos agradecimentos.

Sinto-me honrada e lisonjeada por poder colocar em prática, nesta obra, parte dos ensinamentos que recebi ao longo destes anos, transmitidos por mestres que, futuramente, serão colegas de profissão. Com generosidade, dedicaram seus preciosos tempos para me ensinar e formar a profissional que me tornei.

RESUMO

O uso do reconhecimento facial como instrumento de política pública de segurança tem se expandido no Brasil, suscitando questionamentos quanto à sua compatibilidade com os direitos fundamentais. O presente artigo analisa essa tecnologia à luz da Constituição Federal de 1988, com foco na proteção da privacidade, da igualdade e do devido processo legal. Adota-se abordagem qualitativa, de natureza teórico-analítica, com base em análise normativa, revisão doutrinária e exame de dados empíricos secundários. Parte-se da hipótese de que, embora o reconhecimento facial possa constituir ferramenta legítima de atuação estatal, sua implementação atual revela tensões relevantes com o regime constitucional, especialmente em razão de riscos de discriminação algorítmica, opacidade tecnológica e fragilidade dos mecanismos de controle. Ao final, propõem-se parâmetros constitucionais para sua utilização, visando compatibilizar a eficiência da segurança pública com a proteção dos direitos fundamentais.

Palavras-chave: Reconhecimento facial. Segurança pública. Direitos fundamentais. Vigilância tecnológica. Constitucionalidade.

ABSTRACT

The use of facial recognition as a public security policy has expanded in Brazil, raising concerns regarding its compatibility with fundamental rights. This article analyzes this technology in light of the Brazilian Constitution of 1988, focusing on the protection of privacy, equality, and due process of law. A qualitative, theoretical-analytical approach is adopted, based on normative analysis, doctrinal review, and examination of secondary empirical data. The study is based on the hypothesis that, although facial recognition may constitute a legitimate tool of state action, its current implementation reveals significant tensions with the constitutional framework, particularly due to risks of algorithmic discrimination, technological opacity, and weak oversight mechanisms. Finally, the article proposes constitutional parameters for its use, aiming to reconcile public security efficiency with the protection of fundamental rights.

Keywords: Facial recognition. Public security. Fundamental rights. Technological surveillance. Constitutionality.

SUMÁRIO

1	INTRODUÇÃO	9
2	O PANORAMA DA VIGILÂNCIA BIOMÉTRICA NO BRASIL: EXPANSÃO E CONTEXTUALIZAÇÃO	10
2.1	O Papel da Portaria nº 793/2019 e o Investimento Público	10
2.2	O Processo de Digitalização da Segurança Pública	11
3	TENSÕES CONSTITUCIONAIS: RECONHECIMENTO FACIAL E A PROTEÇÃO DE DIREITOS FUNDAMENTAIS	13
3.1	Privacidade e Proteção de Dados Pessoais Sensíveis	13
3.2	Igualdade, Não Discriminação e o Risco do Racismo Algorítmico	14
3.3	Devido Processo Legal e Transparência Administrativa	15
4	ANÁLISE CRÍTICA DA IMPLEMENTAÇÃO	16
4.1	Vigilância por Lentes Opacas	16
4.2	Desconformidade com a LGPD e a Opacidade na Gestão Privada de Dados Sensíveis	16
4.3	Princípios da Eficiência e Economicidade: Investimentos Vultosos e a Inexistência de Resultados Comprovados	17
5	PROPOSTAS PARA UMA GOVERNANÇA ÉTICA	18
5.1	Marco Regulatório Específico e Suspensão Preventiva	18
5.2	Exigência de Autorização Judicial Prévia	19
5.3	Protocolos de Abordagem e Supervisão Humana	19
5.4	Fixação de Limites de Score (Threshold) e Auditorias	19
5.5	Transparência e Explicabilidade	20
6	CONCLUSÃO	20
	REFERÊNCIAS	22

1 INTRODUÇÃO

A incorporação de tecnologias digitais no âmbito da atuação estatal tem reconfigurado, de maneira profunda, as formas de exercício do poder público, especialmente no campo da segurança pública. Entre essas tecnologias, o reconhecimento facial destaca-se como uma das mais sensíveis, na medida em que permite a identificação automatizada de indivíduos em espaços públicos, a partir da coleta e do processamento de dados biométricos.

A sua adoção por órgãos estatais, com a promessa de aumento da eficiência no combate à criminalidade, tem se expandido de forma significativa no Brasil, inserindo-se no contexto mais amplo de digitalização das políticas públicas e de intensificação das práticas de vigilância.

Esse cenário, contudo, suscita questionamentos relevantes sob a perspectiva constitucional. A utilização do reconhecimento facial envolve a manipulação de dados pessoais sensíveis e a implementação de mecanismos de monitoramento contínuo da população, o que potencialmente afeta direitos fundamentais como a privacidade, a liberdade e a igualdade.

Além disso, a literatura recente tem evidenciado a existência de vieses algorítmicos capazes de produzir resultados discriminatórios, especialmente em relação a grupos historicamente vulnerabilizados, o que tensiona ainda mais a compatibilidade dessa tecnologia com os valores constitucionais.

A relevância do tema decorre, portanto, da necessidade de se estabelecer uma análise jurídica rigorosa acerca dos limites e possibilidades do uso do reconhecimento facial pelo Estado. Em um contexto de crescente adoção dessa tecnologia, a ausência de um marco regulatório específico e suficientemente detalhado amplia os riscos de utilização desproporcional ou incompatível com os direitos fundamentais, tornando imprescindível a construção de parâmetros normativos que orientem sua implementação. Trata-se de um debate que ultrapassa a dimensão meramente tecnológica, inserindo-se no núcleo das discussões contemporâneas sobre constitucionalismo, democracia e controle do poder estatal.

Nesse contexto, o problema que orienta a presente investigação consiste em compreender em que medida o uso do reconhecimento facial como política pública de segurança pública no Brasil é compatível com o regime constitucional de proteção dos direitos fundamentais, especialmente no que se refere à privacidade, à igualdade e ao devido processo legal. A análise não parte de uma rejeição apriorística da tecnologia, mas busca avaliar as condições sob as quais sua utilização pode ser considerada constitucionalmente legítima.

O estudo tem como propósito central examinar a compatibilidade do reconhecimento facial, enquanto instrumento de política pública de segurança, com os direi-

tos e garantias fundamentais previstos na Constituição Federal de 1988. Para tanto, pretende-se compreender o funcionamento e a inserção dessa tecnologia no âmbito das políticas públicas, identificar os direitos fundamentais potencialmente afetados, analisar os riscos estruturais associados à sua utilização e, por fim, estabelecer parâmetros constitucionais que orientem sua implementação de forma compatível com o Estado Democrático de Direito.

A pesquisa desenvolve-se a partir de uma abordagem qualitativa, de natureza teórico-analítica, com a utilização de diferentes estratégias metodológicas. Em primeiro lugar, realiza-se uma análise normativa, centrada na Constituição Federal e na legislação infraconstitucional pertinente, especialmente no que se refere à proteção de dados e à atuação estatal em matéria de segurança pública.

Em seguida, procede-se à revisão da literatura jurídica e interdisciplinar sobre o tema, com o objetivo de identificar os principais debates e categorias analíticas mobilizadas na compreensão das relações entre tecnologia e direitos fundamentais. Além disso, recorre-se à análise de conteúdo de relatórios institucionais e estudos empíricos secundários, que permitem identificar padrões e riscos associados ao uso do reconhecimento facial no contexto brasileiro.

A escolha por essa abordagem metodológica justifica-se pela complexidade do objeto analisado, que exige a articulação entre diferentes campos do conhecimento e a superação de uma perspectiva estritamente normativa. Ao conjugar análise jurídica, reflexão teórica e elementos empíricos, busca-se construir uma compreensão mais abrangente e crítica do fenômeno, capaz de contribuir para o debate acadêmico e para a formulação de políticas públicas mais compatíveis com os direitos fundamentais.

2 O PANORAMA DA VIGILÂNCIA BIOMÉTRICA NO BRASIL: EXPANSÃO E CONTEXTUALIZAÇÃO

2.1 O Papel da Portaria nº 793/2019 e o Investimento Público

A expansão da vigilância biométrica no Brasil não ocorreu de maneira espontânea, estando diretamente vinculada a políticas públicas de incentivo financeiro e institucional. Nesse contexto, a Portaria nº 793/2019 desempenha papel central ao regulamentar a destinação de recursos do Fundo Nacional de Segurança Pública para o fortalecimento de projetos tecnológicos voltados à segurança pública, incluindo sistemas de reconhecimento facial.

A partir dessa iniciativa normativa, observou-se um aumento significativo nos investimentos públicos destinados à implementação de soluções baseadas em biometria, contribuindo para a disseminação dessas tecnologias em diversas unidades

da federação. Os aportes financeiros já ultrapassam R\$ 160 milhões, com destaque para estados como Bahia e Pará, que figuram entre os principais beneficiários desses investimentos, evidenciando o protagonismo regional na adoção dessas ferramentas.

Ademais, é imperativo observar que a Portaria nº 793/2019 atua como um mecanismo indutor de comportamento estatal, ao condicionar o repasse de verbas do Fundo Nacional de Segurança Pública (FNSP) à adoção de tecnologias de monitoramento biométrico pelos Estados.

No entanto, essa indução ocorre em um cenário constitucional transformado pela Emenda Constitucional nº 115/2022 (BRASIL, 2022), que elevou a proteção de dados pessoais à categoria de direito fundamental (Art. 5º, LXXIX), exigindo que a busca pela “eficiência” administrativa, preconizada no Art. 37 da Constituição Federal, não seja interpretada de forma meramente quantitativa.

Como adverte Gilmar Ferreira Mendes (2022), a finalidade legítima da segurança pública não autoriza o sacrifício desproporcional de garantias individuais, sendo necessário que o investimento vultoso, que já supera R\$ 160 milhões, seja acompanhado de transparência e de uma avaliação rigorosa dos custos sociais, sob pena de a tecnologia converter-se em instrumento de vigilância incompatível com o Estado Democrático de Direito.

Contudo, a ampliação do investimento estatal em tecnologias de vigilância demanda análise crítica sob a ótica constitucional. A Constituição Federal de 1988 estabelece, em seu art. 37, que a administração pública deve obedecer aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. Nesse sentido, a alocação de recursos públicos em sistemas de monitoramento deve observar não apenas critérios de eficiência, mas também a compatibilidade com os direitos fundamentais.

Conforme destaca Gilmar Ferreira Mendes (2022), a atuação estatal, mesmo quando orientada por finalidades legítimas, encontra limites nos direitos fundamentais, sendo indispensável a observância do princípio da proporcionalidade como parâmetro de controle. Assim, o investimento público em reconhecimento facial deve ser acompanhado de mecanismos de transparência, avaliação de impacto e controle institucional, sob pena de violação ao regime constitucional.

2.2 O Processo de Digitalização da Segurança Pública

A incorporação de tecnologias digitais no âmbito da segurança pública brasileira reflete um processo mais amplo de transformação estrutural do Estado, marcado pela adoção de ferramentas automatizadas para coleta, processamento e análise de dados. Nesse cenário, a vigilância biométrica, especialmente por meio do reconhecimento facial, insere-se como elemento central da chamada segurança pública digital.

Esse processo de digitalização foi impulsionado por fatores como a necessidade de maior eficiência no combate à criminalidade, a ampliação da capacidade de monitoramento urbano e a integração de bancos de dados. Como resultado, verifica-se a existência de ao menos 337 projetos ativos de reconhecimento facial no país, com potencial de atingir aproximadamente 81 milhões de brasileiros, o que evidencia a consolidação de um modelo de vigilância em larga escala.

Entretanto, essa transformação tecnológica não ocorre sem implicações jurídicas relevantes. A Constituição Federal de 1988 assegura, em seu art. 5º, incisos X e XII, a proteção à intimidade, à vida privada e ao sigilo de dados, impondo limites à atuação estatal no tratamento de informações pessoais. Nesse contexto, a digitalização da segurança pública deve ser compatibilizada com tais garantias, sob pena de configurar práticas de vigilância incompatíveis com o Estado Democrático de Direito.

De acordo com Ingo Wolfgang Sarlet (2021), os direitos fundamentais assumem função de proteção frente às novas formas de intervenção estatal, especialmente aquelas mediadas por tecnologias capazes de ampliar significativamente o poder de controle social. Na mesma linha, Daniel Sarmento (2020) ressalta que a inovação tecnológica não pode servir como justificativa para flexibilização de garantias constitucionais, devendo ser submetida a critérios rigorosos de legitimidade.

No plano jurisprudencial, o Supremo Tribunal Federal tem reiteradamente afirmado a centralidade dos direitos fundamentais como limites à atuação do poder público. A Súmula Vinculante 14, ao assegurar o acesso a informações em procedimentos que possam afetar direitos individuais, reforça a importância da transparência, elemento essencial também na utilização de sistemas de vigilância biométrica.

O texto oficial diz:

É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa.

A implementação desses sistemas, contudo, é frequentemente marcada pela opacidade tecnológica, uma espécie de “caixa-preta” algorítmica que impede o cidadão e seu defensor de compreenderem os critérios técnicos que levaram a uma identificação ou abordagem.

Esse cenário de obscuridade desafia diretamente a Súmula Vinculante 14, que assegura ao defensor o acesso amplo aos elementos de prova já documentados em procedimentos investigatórios. No contexto da segurança pública digital, o direito de defesa, pilar do devido processo legal, não pode ser plenamente exercido se a base da acusação for um resultado automatizado cujos parâmetros de erro e vieses permane-

cem ocultos. Portanto, a aplicação da SV 14 deve ser recontextualizada para garantir que o acesso aos “elementos de prova” inclua a transparência sobre o funcionamento da ferramenta tecnológica, impedindo que o sigilo comercial ou a complexidade técnica anulem as garantias constitucionais do investigado.

De modo complementar, a Súmula 611 evidencia a necessidade de observância estrita das garantias legais e constitucionais em contextos que envolvam restrição de direitos, lógica que pode ser aplicada, por analogia, à implementação de tecnologias de monitoramento em larga escala.

O princípio da autotutela autoriza a administração pública a revisar seus próprios atos, quando eivados de vícios que os tornem ilegais, porque deles não se originam direitos; ou revogá-los, por motivo de conveniência ou oportunidade, respeitados os direitos adquiridos e ressalvada, em todos os casos, a apreciação judicial.

Dessa forma, o panorama da vigilância biométrica no Brasil revela não apenas um processo de expansão tecnológica e institucional, mas também um campo de tensão entre a busca por segurança pública e a preservação dos direitos e garantias fundamentais, exigindo uma análise crítica à luz da ordem constitucional vigente.

3 TENSÕES CONSTITUCIONAIS: RECONHECIMENTO FACIAL E A PROTEÇÃO DE DIREITOS FUNDAMENTAIS

3.1 Privacidade e Proteção de Dados Pessoais Sensíveis

O reconhecimento facial opera a partir do tratamento de dados biométricos, classificados como dados pessoais sensíveis, pois permitem a identificação automatizada e precisa de indivíduos, inclusive em espaços públicos. A adoção dessa tecnologia por órgãos estatais é frequentemente justificada por ganhos de eficiência na segurança pública, especialmente na identificação de suspeitos e na prevenção de ilícitos. Contudo, sua utilização amplia a capacidade de monitoramento contínuo da população, exigindo análise jurídica rigorosa quanto aos limites impostos pelos direitos fundamentais.

A Constituição Federal de 1988 estabelece parâmetros claros para a atuação estatal nesse campo. O art. 5º, incisos X e XII, assegura a inviolabilidade da intimidade, da vida privada e do sigilo de dados. Com o advento da Emenda Constitucional nº 115/2022, a proteção de dados pessoais foi elevada ao status de direito fundamental, o que impõe maior rigor no tratamento de informações biométricas.

A doutrina constitucional destaca que os direitos fundamentais devem ser interpretados de forma expansiva diante das novas tecnologias. Nesse sentido, Ingo Wolf-

gang Sarlet afirma que os direitos fundamentais atuam como mecanismos de contenção do poder estatal, destacando que constituem “direitos oponíveis contra o Estado, limitando sua atuação” (SARLET, 2021, p. 35). Tal compreensão reforça a necessidade de controle jurídico sobre práticas de vigilância tecnológica.

A legitimidade da utilização do reconhecimento facial depende da observância do princípio da proporcionalidade. Nesse contexto, a doutrina aponta que os direitos fundamentais não possuem caráter absoluto, devendo ser ponderados diante de outros valores constitucionais. Conforme a literatura jurídica, “os direitos fundamentais não são absolutos”, o que exige a análise de adequação, necessidade e proporcionalidade em sentido estrito para validar medidas restritivas.

Além disso, a incorporação de novas tecnologias não autoriza a flexibilização indiscriminada das garantias constitucionais. Daniel Sarmento sustenta que o Estado não apenas deve se abster de violar direitos fundamentais, mas também protegê-los, inclusive contra ameaças decorrentes de novas dinâmicas sociais e tecnológicas, ao reconhecer que há “obrigação [...] de protegê-los diante de lesões e ameaças” (SARMENTO, 2020, p. 13).

No contexto brasileiro, a ausência de regulamentação específica sobre o uso do reconhecimento facial amplia riscos como discriminação algorítmica, erros de identificação e vigilância massiva. Diante disso, a implementação dessa tecnologia exige critérios normativos claros, mecanismos de controle e garantias efetivas aos titulares de dados, sob pena de violação ao núcleo essencial dos direitos fundamentais.

3.2 Igualdade, Não Discriminação e o Risco do Racismo Algorítmico

A compatibilidade do reconhecimento facial com a Constituição também deve ser analisada sob o Princípio da Igualdade. A ideia de que algoritmos são neutros por serem baseados em modelos estatísticos é falaciosa, pois estas ferramentas incorporam os vieses inconscientes de seus criadores e as desigualdades estruturais da sociedade. Conforme destacam de (Paula, Barros e Oliveira 2024), a tecnologia pode se tornar uma ferramenta de potencialização de opressões, validando processos racializados de criminalização.

Estudos técnicos comprovam essa falibilidade: relatórios do NIST (2019) apontam que sistemas de IA apresentam taxas de erro (“falsos positivos”) de 10 a 100 vezes maiores para pessoas negras e asiáticas em comparação a caucasianos. No Brasil, essa seletividade algorítmica é alarmante, com pesquisas indicando que 90,5% das pessoas presas com auxílio dessa tecnologia eram negras.

Esse cenário produz erros judiciais graves, como o caso de Danilo Félix, jovem negro acusado injustamente por três vezes devido a falhas de identificação.

Além disso, a discriminação é agravada pela interseccionalidade, uma vez que mulheres negras apresentam os maiores índices de má-identificação pelos sistemas. A logística de implementação também reforça o estigma social, pois a vigilância costuma ser direcionada a áreas periféricas, promovendo um policiamento seletivo de alta intensidade sobre grupos historicamente vulnerabilizados. Portanto, sem controles rigorosos e auditorias de diversidade, o uso do reconhecimento facial afronta o Art. 5º, caput, da CF, ao converter a tecnologia em instrumento de exclusão racial e violação da dignidade humana.

3.3 Devido Processo Legal e Transparência Administrativa

A aplicação do reconhecimento facial no campo da segurança pública brasileira tensiona o princípio do devido processo legal (Art. 5º, LIV, CF), especialmente pela carência de critérios objetivos na fase de alimentação do sistema. As chamadas "listas de procurados" (watchlists) muitas vezes replicam desigualdades prévias do sistema penal. Segundo De Paula, Barros e Oliveira (2024, pág. 2), o perigo reside no fato de que a programação desses sistemas frequentemente "amplifica e valida o racializado e estereotipado processo de criminalização e responsabilização penal". Sem uma curadoria transparente desses bancos de dados, a tecnologia deixa de ser um meio de prova neutro e passa a ser uma ferramenta de segregação social.

A formação dessas listas sem controle judicial prévio ou revisão periódica gera o risco da "caixa-preta algorítmica". Conforme destaca Castilho (2024, pág. 13), essa falta de transparência técnica compromete diretamente as garantias constitucionais do réu, uma vez que "a impossibilidade de compreender os critérios técnicos usados para gerar decisões e alertas da IA, pode configurar um grave obstáculo ao direito ao contraditório e à ampla defesa". Se a defesa não possui acesso aos parâmetros de similaridade (threshold) ou à taxa de erro demográfico do software, a "paridade de armas" é anulada.

Outro ponto crítico é a omissão da utilização da tecnologia nos Autos de Prisão em Flagrante (APF). Quando a autoridade policial não declara que a abordagem foi motivada por um alerta de reconhecimento facial, impede-se que o defensor questione a legalidade da "fundada suspeita". Sobre a fragilidade desse modelo como prova isolada, Soares (2024, pág. 148) reforça a diretriz do Regulamento Europeu, que serve de inspiração ao Brasil, ao asseverar que "não podem ser tomadas decisões com efeitos jurídicos adversos somente com base nos resultados saídos do sistema de identificação biométrica à distância 'em tempo real'".

A ausência de uma moldura legal que obrigue a menção à tecnologia no processo gera insegurança jurídica. Como adverte Medeiros (2024 apud MARIANO, 2025,

p. 7), "a ausência de uma legislação detalhada torna a prova coletada por meio dessa tecnologia vulnerável a questionamentos sobre sua validade e confiabilidade em tribunal". Portanto, para o respeito ao devido processo legal, é imprescindível que o reconhecimento facial seja tratado como um elemento de informação que deve ser corroborado por outras provas, em estrita observância ao rito do Art. 226 do Código de Processo Penal e à jurisprudência do Superior Tribunal de Justiça.

4 ANÁLISE CRÍTICA DA IMPLEMENTAÇÃO

4.1 Vigilância por Lentes Opacas

A implementação prática no Brasil revela um cenário de profunda opacidade. Segundo o relatório "Vigilância por lentes opacas", os mecanismos de controle social são sistematicamente obstruídos. Lima et al. (2024, p. 33) destacam que "pedidos feitos via LAI frequentemente encontram obstáculos adicionais", como a exigência de dados pessoais sensíveis do solicitante para acesso às plataformas de informação.

A gestão financeira também carece de transparência, ferindo o princípio da economicidade. O levantamento do CESeC (2024) aponta que "47,5% dos projetos não divulgam os custos totais envolvidos", o que impossibilita aferir se o investimento público que na Bahia atingiu R\$ 728 milhões, resulta em efetiva redução da criminalidade

Por fim, há um vácuo de conformidade com a LGPD, visto que a maioria dos órgãos não esclarece se elabora o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) antes de ativar os sistemas.

4.2 Desconformidade com a LGPD e a Opacidade na Gestão Privada de Dados Sensíveis

A aplicação do reconhecimento facial na segurança pública brasileira ocorre em um cenário de insegurança jurídica, pautado pela interpretação extensiva das exceções previstas na Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Embora o Art. 4º, inciso III, da LGPD estabeleça que a lei não se aplica ao tratamento de dados para fins de segurança pública e investigação criminal, o parágrafo 1º do mesmo dispositivo impõe que tal tratamento deve observar "o devido processo legal, os princípios gerais de proteção e os direitos do titular". No entanto, a prática revela um vácuo de conformidade, especialmente no que tange à transparência das parcerias com o setor privado.

A participação de empresas privadas na operacionalização desses sistemas é a regra, e não a exceção, o que agrava os riscos de mau uso das informações. Con-

forme aponta Soares (2024), a transferência de atribuições tecnológicas do Estado para corporações ocorre frequentemente sem a devida publicidade. Sobre essa relação, Whittaker (2020, apud SOARES, 2024, p. 57) adverte que:

A formalização de contratos entre o setor público e empresas privadas configura uma relação jurídica de elevada complexidade, na qual se verifica, com frequência, a imposição de restrições ao acesso a informações, resultando em um alto grau de sigilo.

Essa opacidade é confirmada por dados empíricos alarmantes. O levantamento "Vigilância por lentes opacas" revela que a maioria dos órgãos de segurança não cumpre o dever de prestar contas à sociedade e aos órgãos reguladores. Segundo Lima et al. (2024, p. 19), a negligência institucional é evidente, visto que "72,5% das entidades não esclareceram se elaboram relatórios de impacto à proteção de dados pessoais". A ausência do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) impede que a Autoridade Nacional de Proteção de Dados (ANPD) e a sociedade civil avaliem se os riscos aos direitos fundamentais foram mitigados antes da ativação dos sistemas.

Além disso, a falta de comunicação oficial à ANPD sobre o envolvimento de empresas privadas na gestão de dados sensíveis anula os mecanismos de accountability. Como o tratamento de biometria facial envolve dados pessoais sensíveis (Art. 5º, II, LGPD), o compartilhamento com entes privados deveria ser estritamente regulado para evitar o que a doutrina chama de "comercialização da vigilância". Conforme reforça o relatório do CESeC, a dificuldade de fiscalização é tamanha que, em "55% dos casos analisados, não foi possível obter" sequer a identificação da empresa responsável pelo fornecimento da tecnologia.

Portanto, a implementação atual fere o princípio da publicidade administrativa (Art. 37, CF) e a autodeterminação informativa dos cidadãos. Sem a obrigatoriedade de auditorias independentes e sem a transparência nos fluxos de dados entre Estado e empresas, o sistema de segurança pública digital converte-se em uma "caixa-preta algorítmica", operando à margem do controle democrático e dos parâmetros protetivos da LGPD.

4.3 Princípios da Eficiência e Economicidade: Investimentos Vultosos e a Inexistência de Resultados Comprovados

A validade de uma política pública no Estado Democrático de Direito não se esgota na sua legalidade formal, exigindo também a observância dos princípios da eficiência e economicidade (Art. 37, caput, CF). No caso do reconhecimento facial, observa-se um vultoso aporte de recursos públicos sem a correspondente demonstra-

ção de resultados na redução dos índices de criminalidade, os aportes financeiros já ultrapassam R\$ 160 milhões, em nível Nacional (DIESTER, 2023)

A despeito da magnitude desses gastos, a implementação ocorre sob um "vácuo de evidências". Ao analisar a expansão desse modelo de vigilância em solo baiano, Marques (2025, p. 91) adverte que o sistema abrange dezenas de municípios "sem que haja evidências concretas de sua efetividade na redução da criminalidade"

Essa desconexão entre o custo e o benefício social configura uma violação direta à racionalidade administrativa, uma vez que o Estado prioriza gastos em tecnologias de alta complexidade em detrimento de áreas sociais básicas sem comprovar que tal escolha produz uma segurança pública mais efetiva.

A falta de transparência financeira agrava a suspeita de ineficiência e dificulta o controle social sobre o Erário. O levantamento "Vigilância por lentes opacas", conduzido pelo CESeC, revela que a maioria dos projetos de segurança digital opera à margem da publicidade orçamentária. Segundo Lima et al. (2024, apud MARQUES, 2025, p. 92), a opacidade é a regra, visto que "47,5% dos projetos não divulgam os custos totais envolvidos".

Além disso, o relatório aponta que a gestão desses recursos é frequentemente marcada pela falta de relatórios públicos de eficácia, o que impossibilita aferir se a tecnologia realmente auxilia na resolução de crimes ou se constitui apenas um "fetiche tecnológico" dispendioso.

Portanto, a manutenção e expansão desses sistemas sem auditorias de impacto e sem a demonstração de retorno social ferem o princípio da economicidade. Sob a ótica da "proporcionalidade em sentido estrito", o sacrifício de verbas públicas em sistemas que operam com altas taxas de erro, como os "96% de alertas imprecisos" registrados em eventos na Bahia não se justifica perante o regime constitucional, tornando a política pública financeiramente ilegítima e tecnicamente inidônea para os fins que se propõe.

5 PROPOSTAS PARA UMA GOVERNANÇA ÉTICA

5.1 Marco Regulatório Específico e Suspensão Preventiva

A primeira e mais urgente recomendação das fontes é a necessidade de uma lei nacional detalhada. A ausência de regras claras fragiliza a validade das provas, pois, como assevera Medeiros (2024, apud MARIANO, 2025, p. 7), "a ausência de uma legislação detalhada torna a prova coletada por meio dessa tecnologia vulnerável a questionamentos sobre sua validade e confiabilidade em tribunal".

Diante disso, diversos setores defendem a aplicação do princípio da precaução,

sustentando que "sua implementação acontecerá de maneira limitada ou não acontecerá até que estudos técnicos, pareceres interdisciplinares e consultas públicas possam incumbir a ela uma legitimidade real" (CASTILHO, 2024, p. 9).

5.2 Exigência de Autorização Judicial Prévia

Para evitar o monitoramento massivo e indiscriminado, as fontes apontam que a utilização do reconhecimento facial em investigações deve ser tratada com o mesmo rigor de uma interceptação telefônica. Seguindo o modelo do Regulamento Europeu, cada uso individualizado "está sujeito a autorização prévia concedida por uma autoridade judiciária, ou uma autoridade administrativa independente cuja decisão seja vinculativa" (SOARES, 2024, p. 147).

No Brasil, o Anteprojeto de LGPD Penal reforça essa tese ao vedar o uso da tecnologia em tempo real "quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial" (BRASIL, 2019, apud SOARES, 2024, p. 168).

5.3 Protocolos de Abordagem e Supervisão Humana

A governança ética exige que a tecnologia seja apenas um auxílio à decisão humana, e não sua substituta. É indispensável a criação de "parâmetros legais claros, que assegurem a transparência e a auditoria dos sistemas utilizados" (MARIANO, 2025, p. 8).

Nesse sentido, as fontes são enfáticas quanto à "necessidade da inclusão de uma etapa de verificação humana neste processo para evitar os falsos positivos e negativos" (MARQUES, 2025, p. 82). A revisão humana qualificada serve como filtro essencial contra o arbítrio e o erro algorítmico demográfico.

5.4 Fixação de Limites de Score (Threshold) e Auditorias

Para mitigar os riscos de discriminação, propõe-se a regulação técnica dos parâmetros de similaridade. O treinamento do sistema deve ser rigoroso e pautado por "índices de precisão para cada grupo demográfico relevante" (SOARES, 2024, p. 187). Além disso, a governança ética deve incluir a "estipulação do trade-off adequado do threshold (falsos positivos/falsos negativos), o que impõe uma decisão política acerca de eventuais equívocos do sistema" (SOARES, 2024, p. 206). Complementarmente, defende-se a "fixação de um organismo independente de supervisão que valide o sis-

tema previamente ao uso”, garantindo que a tecnologia não exacerbe a vigilância sobre minorias e grupos marginalizados.

5.5 Transparência e Explicabilidade

Por fim, o dever de transparência administrativa impõe que os critérios de decisão da IA sejam auditáveis. O princípio da explicabilidade deve ser adotado como uma “forma de superar a opacidade, ao se racionalizar o processo decisório da máquina e tornar o resultado obtido pelo sistema compreensível ao ser humano” (DE PÁDUA; LORENZETTO, 2024, apud SOARES, 2024, p. 98). Sem essa clareza técnica, o devido processo legal é anulado pela “caixa-preta algorítmica”.

6 CONCLUSÃO

A investigação realizada demonstra que a expansão das tecnologias de reconhecimento facial (TRF) na segurança pública brasileira, impulsionada pelo fomento financeiro da Portaria nº 793/2019, ocorreu de forma acelerada e desprovida de um marco regulatório que assegure a proteção dos direitos fundamentais.

O cenário mapeado revela uma profunda assimetria entre a promessa de eficiência tecnológica e a realidade prática, marcada pela opacidade institucional e por riscos severos à dignidade da pessoa humana.

A tensão constitucional manifesta-se em três frentes principais:

Privacidade e Proteção de Dados Pessoais: O reconhecimento facial opera mediante o tratamento de dados biométricos sensíveis, aptos a permitir a identificação automatizada e o monitoramento contínuo da população em espaços públicos. Essa prática tensiona a inviolabilidade da intimidade, da vida privada e do sigilo de dados, assegurados pelo art. 5º, incisos X e XII, da Constituição Federal, sobretudo após a Emenda Constitucional nº 115/2022, que elevou a proteção de dados pessoais à condição de direito fundamental. A ausência de marco regulatório específico amplia, nesse contexto, os riscos de vigilância massiva e de tratamento desproporcional de informações pessoais.

Igualdade e Não Discriminação: O fenômeno do “racismo algorítmico” não é meramente teórico, mas empírico. Sistemas treinados em bases de dados viciadas apresentam taxas de erro (“falsos positivos”) de “10 a 100 vezes maiores” para pessoas negras e asiáticas do que para caucasianos. No Brasil, essa falibilidade resulta em uma seletividade penal alarmante, evidenciada por dados de que “90,5% das pessoas presas com o auxílio dessa tecnologia eram negras”.

Devido Processo Legal e Transparência: A opacidade dos sistemas de reco-

nhecimento facial — a denominada "caixa-preta algorítmica" — compromete o contraditório e a ampla defesa, ao impedir que o investigado e seu defensor conheçam os critérios técnicos que fundamentam identificações e abordagens. A formação de bancos de dados sem curadoria transparente e sem controle judicial prévio fragiliza o devido processo legal (art. 5º, LIV, da Constituição Federal) e dificulta o controle social sobre a atuação estatal, impondo o dever de transparência quanto ao funcionamento da tecnologia e às suas margens de erro.

Ademais, a pesquisa evidenciou que os elevados investimentos públicos destinados à implementação de sistemas de reconhecimento facial não têm sido acompanhados de demonstrações consistentes quanto à sua efetividade na redução dos índices de criminalidade. Em âmbito nacional, os aportes financeiros ultrapassam R\$ 160 milhões, alcançando, em determinados estados, valores ainda mais expressivos, como os R\$ 728 milhões investidos pela Bahia. Contudo, a ausência de estudos independentes e de indicadores objetivos que correlacionem esses investimentos aos resultados obtidos compromete a avaliação da real eficiência da política pública adotada.

Esse descompasso entre o volume de recursos empregados e a comprovação de benefícios concretos à coletividade suscita questionamentos sob a perspectiva dos princípios constitucionais da eficiência e da economicidade, previstos no art. 37 da Constituição Federal. A destinação de expressivos recursos públicos para tecnologias cuja efetividade permanece insuficientemente demonstrada exige maior rigor na análise de custo-benefício e na prestação de contas à sociedade.

Diante desse cenário, conclui-se que a atual implementação do reconhecimento facial na segurança pública apresenta incompatibilidades com as garantias estabelecidas pela ordem constitucional inaugurada pela Constituição Federal de 1988, especialmente no que se refere à proteção dos direitos fundamentais, à transparência administrativa e ao devido processo legal. Nesse contexto, mostra-se necessária a adoção de medidas regulatórias específicas antes da ampliação do uso dessas tecnologias.

Entre essas medidas, destacam-se a instituição de uma legislação nacional que estabeleça parâmetros claros para sua utilização, a previsão de mecanismos de supervisão independente e auditoria periódica, bem como a exigência de revisão humana qualificada nos procedimentos que envolvam identificação biométrica. Tais providências são essenciais para assegurar que a incorporação de inovações tecnológicas na segurança pública ocorra em conformidade com os princípios constitucionais e com a proteção dos direitos e garantias individuais.

Somente mediante a implementação de estruturas robustas de governança, transparência e responsabilização será possível compatibilizar o emprego de tecnologias de reconhecimento facial com os valores democráticos e com a centralidade da dignidade da pessoa humana no Estado Democrático de Direito.

REFERÊNCIAS

AGENDAS PARA O BRASIL. *Mapeando a vigilância biométrica: levantamento nacional sobre o uso do reconhecimento facial na segurança pública*. Disponível em: <https://agendasparaobrasil.org.br/mapeando-a-vigilancia-biometrica-levantamento-nacional-sobre-o-uso-do-reconhecimento-facial-na-seguranca-publica/>. Acesso em: 06/06/2026.

ANPD. Autoridade Nacional de Proteção de Dados. *Radar Tecnológico: Biometria e Reconhecimento Facial*. Brasília, DF: ANPD, 2024.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, 11 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 02/03/2026.

CASTILHO, Luis Henrique Laureano Viana. *Inteligência Artificial e Segurança Pública: limites e desafios jurídicos*. [S.l.], 2024.

DE PAULA, A. V.; BARROS, F.; OLIVEIRA, L. R. A discriminação racial no sistema de reconhecimento facial no Brasil e seus impactos na política criminal. *Revista de Direitos Humanos e Desenvolvimento Social*, v. 5, e2413770, 2024. Disponível em: <https://doi.org/10.24220/2675-9160v5a2024e13770>. Acesso em: 01/04/2026.

DIESTER, J. Reconhecimento facial: jovem negro prova inocência pela terceira vez após ser acusado por erro. *Brasil de Fato RJ*, Rio de Janeiro, 14 abr. 2023. Disponível em: <https://www.brasildefatorj.com.br/2023/04/12/reconhecimento-facial-jovem-negro-prova-inocencia-pela-terceira-vez-apos-ser-acusado-por-erro>. Acesso em: 02/03/2026.

DW BRASIL. Banalização da biometria no Brasil aumenta risco de fraudes. *DW Brasil*, [s.d.]. Disponível em: <https://www.dw.com/pt-br/banaliza%C3%A7%C3%A3o-da-biometria-no-brasil-aumenta-risco-de-fraudes/a-72621650>. Acesso em: 01/05/2026.

LIMA, Thallita et al. *Vigilância por lentes opacas: mapeamento da transparência e responsabilização de projetos de reconhecimento facial no Brasil*. Rio de Janeiro: CEsEC, 2024.

MARIANO, Júlia Helena Lima. *Reconhecimento facial como meio de prova e os riscos às garantias processuais*. Rio de Janeiro, 2025.

MARQUES, Daniel da Silva. *Reconhecimento facial e segurança pública: Lawethics by design como novo paradigma regulatório*. 2025. 288 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2025.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. 17. ed. rev. e atual. São Paulo: Saraiva, 2022.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, Passo Fundo, v. 16, n. 1, p. 1-33, 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. Gaithersburg, MD: NIST, 2019.

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. In: CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA. *Retratos da violência: cinco meses de monitoramento, análises e descobertas*. Rio de Janeiro: CESeC, 2019. p. 67-71.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 13. ed. Porto Alegre: Livraria do Advogado, 2021.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 10. ed. São Paulo: Saraiva, 2021.

SARMENTO, Daniel. *Direito constitucional: teoria, história e métodos de trabalho*. 2. ed. Belo Horizonte: Fórum, 2020.

SARMENTO, Daniel. *Direitos fundamentais e relações privadas*. 2. ed. Rio de Janeiro: Lumen Juris, 2020.

SOARES, Thiago Alves Duarte Faerman. *Reconhecimento facial em tempo real e segurança pública: perspectivas a partir do Direito Europeu*. São Paulo: PUC-SP, 2024.

UOL. Vigilância facial: pesquisadores apontam falhas em sistema de "alto risco". *UOL Notícias*, 6 jul. 2025. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2025/07/06/vigilancia-facial-pesquisadores-apontam-falhas-em-sistema-de-alto-risco.htm>. Acesso em: 20/05/2026.