O USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA BRASILEIRA: UMA ANÁLISE JURÍDICA DAS IMPLICAÇÕES QUANTO AO DIREITO À PRIVACIDADE

Alice Maria Fontineles Val [1]
Angela Vitorya Pimentel de Araújo [2]
Emanuely Cristini dos Santos Mendes[3]
Renildo Barbosa Estevão[4]

RESUMO:

O presente artigo examina o uso do reconhecimento facial (RF) na segurança pública brasileira. A pesquisa, de natureza bibliográfica e documental, tem como propósito compreender suas implicações jurídicas, especialmente no que se refere ao direito à privacidade, garantia assegurada pelo artigo 5º, inciso X, da Constituição Federal. Com abordagem interdisciplinar, o estudo analisa a legislação brasileira, os princípios constitucionais, a Lei Geral de Proteção de Dados Pessoais (LGPD), além de casos noticiados e jurisprudências. O RF, técnica biométrica utilizada para identificar suspeitos e auxiliar investigações, representa avanço tecnológico, mas traz riscos relacionados à precisão dos algoritmos e à ausência de regulamentação. Tais fatores têm resultado em prisões indevidas, abordagens discriminatórias e violações ao direito à privacidade. A inexistência de regulamentação específica sobre o uso do RF nos estados brasileiros configura um vácuo normativo, onde dificulta a responsabilização por abusos e possibilita arbitrariedades estatais. Atualmente, sua aplicação se baseia em interpretações genéricas da LGPD e em disposições administrativas estaduais e municipais. Conclui-se que o reconhecimento facial, embora apresente potencial para aprimorar a segurança pública, exige regulamentação clara e específica que assegure o equilíbrio entre a eficiência estatal e a proteção dos direitos fundamentais.

Palavras- chave: Reconhecimento Facial; Segurança Pública; Direito à Privacidade; Implicações Jurídicas; Dados Biométricos.

[1]Acadêmico de Direito da Afya Parnaíba
[2] Acadêmico de Direito da Afya Parnaíba
[3] Acadêmico de Direito da Afya Parnaíba
[4] Docente da Faculdade de Direito Afya Parnaíba

INTRODUÇÃO

O presente artigo tem como propósito examinar o uso do reconhecimento facial na segurança pública brasileira, buscando compreender suas implicações jurídicas, especialmente no que tange ao direito de privacidade. Parte-se da premissa de que a aplicação crescente dessa tecnologia pelas forças de segurança pública tem suscitado intensos questionamentos quanto à sua compatibilidade com o direito à privacidade, garantia assegurada no art. 5, inciso X da Carta Magna.

Nesse sentido, torna-se imprescindível refletir sobre os fatores que influenciam e moldam o desenvolvimento dessa temática, relacionando os avanços tecnológicos às exigências de um Estado Democrático de Direito. O reconhecimento facial, como técnica biométrica de identificação, representa uma inovação significativa no campo da vigilância e do controle social.

Apesar da utilidade aparente dos sistemas de reconhecimento facial, os riscos quanto à funcionalidade, critérios de identificação dos algoritmos utilizados nos sistemas e à ausência de regulamentação jurídica são notórios, resultando em prisões indevidas, abordagens discriminatórias e violações ao direito à privacidade.

A relevância do estudo justifica-se não apenas pela atualidade do tema, mas também pelo impacto direto que ele exerce sobre a sociedade. O reconhecimento facial insere-se em um cenário mais amplo de digitalização e coleta massiva de dados pessoais, em que o cidadão passa a ser constantemente monitorado em espaços públicos, muitas vezes sem seu conhecimento ou consentimento. Tal realidade evidencia um dilema entre segurança e liberdades individuais, exigindo uma análise crítica que supere apenas a eficiência tecnológica.

Outro aspecto de destaque consiste na inexistência de regulamentação específica acerca do uso dessa tecnologia nos Estados brasileiros. Sua aplicação, até o presente momento, encontra respaldo apenas em interpretações genéricas da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e em disposições administrativas estaduais e municipais, o que configura um vácuo normativo.

Nesse sentindo, essa ausência compromete a efetiva responsabilização diante de abusos e amplia a margem para condutas arbitrárias por parte do poder público. Contudo, há um projeto de lei em trâmite no Congresso Nacional que dispõe acerca da definição do reconhecimento facial e seu funcionamento na segurança pública (Projeto de Lei nº 3069/2022).

Além disso, a discussão em torno do reconhecimento facial não pode ser dissociada de seu viés discriminatório. Erros de identificação ocorrem majoritariamente com pessoas negras e mulheres, que aprofunda as desigualdades raciais e sociais existentes no país, e intensifica a problemática da seletividade penal no sistema carcerário.

Diante desse cenário, a pesquisa proposta neste artigo será fundamentada em revisão bibliográfica e documental, adotando uma abordagem qualitativa, teórica e reflexiva. O propósito é possibilitar uma análise crítica dos conceitos jurídicos, das interpretações doutrinárias e jurisprudenciais e das experiências práticas relacionadas ao uso do reconhecimento facial. O presente estudo tem como objetivo geral analisar juridicamente os impactos do uso do reconhecimento facial na segurança pública brasileira, com ênfase na observância ao direito à privacidade.

Especificamente, busca-se compreender como essa tecnologia vem sendo empregada pelas forças de segurança pública no país, identificar os principais entraves enfrentados tanto pelos cidadãos afetados quanto pelas instituições responsáveis por sua implementação, avaliar os efeitos decorrentes da ausência de regulamentação jurídica específica sobre o tema e examinar as implicações dessa tecnologia para os direitos fundamentais, especialmente no que se refere à privacidade e à igualdade.

A reflexão sobre esses aspectos permite situar o debate em um panorama jurídico contemporâneo, no qual a inovação tecnológica e a proteção de direitos fundamentais coexistem de forma complexa e muitas vezes tensionada. Ademais, desafios surgem na criação de normas eficazes e mecanismos de controle, especialmente para prevenir abusos e proteger grupos vulneráveis, exigindo equilíbrio entre eficiência e garantias constitucionais

Dessarte, o presente artigo pretende constituir não apenas um exercício acadêmico, mas também uma contribuição prática e crítica ao debate sobre o uso de tecnologias de reconhecimento facial no Brasil. Ao consolidar os

fundamentos teóricos, a delimitação metodológica e a problematização do tema, espera-se oferecer subsídios para a construção de soluções jurídicas que conciliem a eficiência tecnológica com a proteção ao direito à privacidade.

2 DESENVOLVIMENTO

2.1 Reconhecimento Facial na Segurança Pública: Benefícios e Limitações

O avanço das tecnologias biométricas e da inteligência artificial tem ampliado a coleta de dados e a criação de padrões de identificação, viabilizando um maior controle social no setor público e privado. Diariamente, somos submetidos à captação de dados biométricos para acessar diversos sistemas e serviços. Entre eles, destacam-se o reconhecimento facial, a leitura de impressões digitais, a autenticação biométrica utilizada em transações bancárias, na identificação civil e em cadastros públicos.

Além dos dados fornecidos voluntariamente, há também aqueles captados sem o conhecimento direto dos indivíduos, como imagens de câmeras de monitoramento em locais públicos. Esses sistemas, geralmente integrados à inteligência artificial e ao reconhecimento facial (RF), possibilitam a identificação e o rastreamento de pessoas em tempo real, sendo utilizados também em investigações forenses, na identificação de suspeitos e no combate a crimes.

Os sistemas biométricos se dividem em dois grandes grupos: os invasivos, que necessitam da colaboração do indivíduo para a sua identificação, como a coleta de impressões digitais ou de íris; e os não invasivos, que podem ser utilizados até mesmo sem o conhecimento do identificado, como a captação de imagens à distância. Nesse sentido, o RF é um mecanismo de elevada amplitude de monitoramento, uma vez que a maioria das pessoas observadas desconhece que seus dados estão sendo processados (TEIXEIRA, 2011 apud MELO; NEVES; NETO, 2021, p. 131).

Essa característica, embora aumente a eficiência da vigilância, também eleva os riscos à privacidade, pois permite o tratamento de informações sensíveis sem o consentimento explícito do titular.

Tal prática deve ser analisada à luz dos direitos e garantias fundamentais previstos na Constituição Federal (Brasil, 1988), em especial no artigo 5º, incisos X e XII, que asseguram o direito à intimidade, vida privada e sigilo das comunicações. Igualmente relevantes são os incisos LIV e LV do mesmo artigo, que garantem o devido processo legal, o contraditório e a ampla defesa, princípios indispensáveis a qualquer intervenção estatal que envolva coleta e uso de dados pessoais. Ademais, o artigo 37 da Constituição (Brasil, 1988)

impõe à Administração Pública a observância dos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, aplicáveis também às práticas de monitoramento e vigilância eletrônica.

Esses direitos foram reforçados pela Emenda Constitucional nº 115/2022 (Brasil, 2022), que incluiu expressamente a proteção de dados pessoais entre os direitos e garantias fundamentais. Assim, o tratamento de dados biométricos como imagens faciais deve observar o princípio da finalidade, da necessidade e da proporcionalidade, conforme previsto na Lei nº 13.709/2018 - Lei Geral de Proteção de Dados - LGPD (Brasil, 2022).

Nesse contexto, o tratamento de dados biométricos como as imagens faciais deve obedecer aos princípios da finalidade, necessidade e proporcionalidade, conforme dispõe a LGPD (BRASIL, 2018). Essa legislação estabelece parâmetros rigorosos para o uso e compartilhamento de dados pessoais, impondo limites à atuação do poder público e condicionando o tratamento dessas informações à observância de bases legais específicas.

Assim, compreender esses parâmetros legais é essencial para avaliar o funcionamento da tecnologia de reconhecimento facial, a qual se baseia na captação de imagens por câmeras de segurança e as compara com registros de bases governamentais, como as da Polícia Federal, Secretarias de Segurança Pública estaduais e o Instituto Nacional de Identificação (INI).

De acordo com Eduarda Costa Almeida (2022, p. 267-268), o sistema extrai pontos biométricos do rosto, como distância entre os olhos e formato do queixo, convertendo-os em um código matemático conhecido como “face template, uma assinatura facial”. O resultado da análise dos dados faciais gera uma porcentagem de semelhança entre as assinaturas biométricas comparadas nos bancos de dados. Essa correspondência gerada pelo sistema de RF, indica a probabilidade de identidade, aciona um alerta imediato aos agentes de segurança para a potencial abordagem do suspeito.

Em junho de 2022, o Banco Nacional de Mandados de Prisão registrava 330.849 pessoas procuradas e 24.159 foragidos da justiça no Brasil (BRASIL, 2022). Reconhecer essas pessoas no meio da população seria uma tarefa complexa para os olhos humanos. No entanto, com o uso do reconhecimento facial, a identificação desses foragidos pode ser feita em segundos. Quando um criminoso passa pelas câmeras de segurança, sistemas emitem notificações

instantâneas à polícia, permitindo que as forças de segurança ajam rapidamente (VARGAS, 2022).

Diante desse cenário, o reconhecimento facial na segurança pública oferece benefícios consideráveis, como a identificação rápida de suspeitos, facilitando a localização de infratores e a resolução de casos, especialmente em locais de grande público, como aeroportos. Ao automatizar a identificação, a tecnologia otimiza o tempo necessário para reconhecer criminosos, aumentando a eficiência das abordagens policiais.

Somente no ano de 2025, o sistema de reconhecimento facial implantado no município de São Paulo identificou 585 foragidos da Justiça, até março, conforme registros do “Prisômetro”, um painel de monitoramento instalado no Centro da cidade, que exibe em tempo real dados de segurança pública (Prefeitura de São Paulo, 2025). Esse número representa uma média de sete prisões de foragidos por dia realizadas pelo programa Smart Sampa (EXPRESSO- ESTADÃO, 2025).

Apesar de sua utilidade no combate à criminalidade, essa tecnologia enfrenta desafios técnicos e jurídicos. Falsos positivos e negativos são riscos inerentes ao sistema, uma vez que fatores como iluminação, ângulo de captura, baixa qualidade da imagem e o uso de acessórios, como bonés, máscaras e óculos podem comprometer a acurácia da identificação.

Casos documentados no Brasil já demonstraram as falhas do sistema, como prisões indevidas baseadas apenas na correspondência do reconhecimento facial, sem confirmação por outros meios de prova. Um episódio amplamente divulgado ocorreu em 2024, durante a final do Campeonato Sergipano, quando um homem foi detido após ser erroneamente detectado por um sistema de reconhecimento facial (FANTÁSTICO, 2024; G1, 2024). Em razão desse incidente, o uso da tecnologia foi suspenso temporariamente pelo poder executivo estadual até que novos protocolos fossem implementados.

Outrossim, para evitar erros e garantir a efetividade do RF, é essencial capacitar os profissionais da área para realizarem uma verificação humana após a análise automatizada, antes de qualquer abordagem ou prisão. Além disso, a atualização periódica do banco de dados, com imagens mais recentes e nítidas, aprimorará a precisão do sistema. Ademais, é necessário a definição de um percentual mínimo de similaridade, a fim de evitar abordagens indevidas,

garantindo que apenas casos com alta precisão sejam considerados para a atuação policial.

Além disso, o alto custo compromete a viabilidade do RF na segurança pública, exigindo altos investimentos em manutenção e expansão. O Estado da Bahia, por exemplo, destinou cerca de R$ 665 milhões para essa finalidade até julho de 2026. Os recursos empregados reduzem investimentos em áreas essenciais, como saúde e educação, setores determinantes para o desenvolvimento social em longo prazo. Diante disso, questiona-se a justificativa dos altos custos, dada a incerta eficácia na redução da criminalidade (PAULO NASCIMENTO, 2023).

Portanto, o RF na segurança pública representa um avanço tecnológico relevante, proporcionando maior eficiência na identificação de criminosos e no combate à criminalidade. No entanto, desafios como falsos positivos, impacto financeiro elevado e questões jurídicas evidenciam a necessidade de aprimoramento contínuo da tecnologia. Para garantir seu uso adequado e minimizar riscos, é essencial a implementação de protocolos rigorosos, capacitação de agentes de segurança e revisão periódica das bases de dados. Dessa forma, busca-se um equilíbrio entre inovação, segurança e respeito aos direitos fundamentais dos cidadãos.

2.2 A urgência da regulamentação do reconhecimento facial no Brasil

O crescente uso da tecnologia de reconhecimento facial no Brasil, tanto no setor público como no privado, levanta questionamentos acerca da falta de regulamentação jurídica dessa ferramenta. Nesse viés, com a ausência de um arcabouço legal, a utilização dessa tecnologia pode violar direitos constitucionais como o direito à privacidade. Dessa forma, assim como a falta de regulamentação compromete a proteção de direitos fundamentais, também cria um cenário de incerteza para o desenvolvimento e aplicação correta dessa tecnologia.

De acordo com Araújo, Cardoso e De Paula, “o problema mais preocupante ocasionado pela falta de regulamentação é a fragilidade na proteção dos cidadãos submetidos a essa tecnologia”. Não há clareza sobre como os dados são coletados, de que maneira a falta de consentimento pode

impactar o uso das informações contidas nos bancos de dados, quais medidas tomar para evitar discriminações e, principalmente, quais os mecanismos disponíveis para responsabilização do Estado em caso de abusos, (ARAÚJO; CARDOSO; DE PAULA, 2021).

As informações armazenadas pelo RF são dados biométricos, ou seja, a identificação é feita com base em um aglomerado de informações especificas de cada pessoa, (THALES, 2020). O art. 5, II da Lei Geral de Proteção de Dados (Brasil, 2018) ressalta que um dado biométrico de uma pessoa natural é um dado sensível e Doneda (2019, p.143) afirma que caso esses dados "sejam conhecidos e submetidos a tratamento, podem se prestar a uma potencial utilização discriminatória ou lesiva e que apresentariam maiores riscos potenciais do que outros tipos de informação".

Importante ressaltar que a EC nº 115/2022 (Brasil, 2022) alterou a Constituição Federal e incluiu no artigo 5 a proteção de dados pessoais como direito fundamental autônomo, como garantia de que os indivíduos tenham controle sobre a coleta de seus dados. Portanto, é necessário que a coleta de dados biométricos seja realizada de forma transparente e com consentimento específico e destacado, nos termos do artigo 11, I da LGPD (Brasil, 2018).

Nesse viés, conforme artigo 23 da LGPD (Brasil, 2018) , a utilização desses dados pelo poder público deverá atender ao interesse público, para cumprimento das atribuições legais do serviço público, desde que sejam fornecidas informações claras e atualizadas sobre a "previsão legal, finalidade, os procedimentos e as práticas utilizadas para execução dessas atividades".

Os arts. 24 a 30 (Brasil, 2018)**,** por sua vez**,** complementam esse dever, estabelecendo mecanismos de comunicação, compartilhamento e responsabilização dos agentes públicos que tratam dados pessoais, bem como a obrigação de manter registros das operações realizadas.

O uso descontrolado e sem base jurídica do RF permite que forças policiais tenham acesso sobre todas as pessoas que transitam em espaços públicos, como em protestos e manifestações públicas. Assim, para Oliveira (2022, p.275), os direitos de inviolabilidade da intimidade e da privacidade, ainda que exercidos em espaços públicos, são violados a partir da vigilância massiva e controle de dados biométricos pelo Estado.

Além disso, outro fator que corrobora a problemática da ausência de normas para uso do reconhecimento facial é o alto potencial de erro na identificação de suspeitos. A identificação correta feita por RFs depende de fatores como proximidade, iluminação e ângulo o qual dificulta a confiabilidade em imagens capturadas por exemplo, no período noturno, (SILVA, 2019). Logo, há elevadas possibilidades de o sistema identificar rostos com características similares entre imagens já armazenadas nos bancos de dados, sobretudo com pessoas de pele escura.

Segundo reportagem do Portal R7, em outubro de 2020, José Domingos Leitão, residente no município de Ilha Grande – PI, passou 3 dias preso após ser erroneamente identificado por uma tecnologia de reconhecimento facial. O crime aconteceu a mais de 2.000km de distância de onde José mora e o mesmo nunca sequer esteve na cidade onde o fato ocorreu. O sistema do Instituto de Identificação da PCDF comparou as imagens do suspeito feitas por câmeras à uma foto de José disponível no banco de dados nacional de todas as pessoas que possuem documento de identidade (PORTAL R7, 2021).

Concomitantemente, imagens de delitos em delegacias são frequentemente mantidas em bancos de dados, ainda que o suspeito não tenha sido oficialmente acusado pelo ato criminoso e antes mesmo da determinação de sua culpabilidade ou inocência por sentença penal condenatória transitada em julgado, (ALMEIDA, 2022). Indubitavelmente, a repetição dessa situação potencializa a ameaça à presunção de inocência dos indivíduos, à medida que o resultado do tratamento dos dados faciais indica apenas probabilidades de ser ou não a pessoa que cometeu um crime.

A regulação dessa ferramenta é essencial para garantir que os órgãos de segurança pública possam usar TRFs com respaldo jurídico para evitar comprometer os direitos fundamentais dos cidadãos. Ademais, a carência de uma base legal sólida e transparente agrava as desigualdades e o desequilíbrio de poder entre os indivíduos da sociedade e o Estado, especialmente diante do avanço acelerado das tecnologias de vigilância, que estabelecem um elevado nível de monitoramento. (OLIVEIRA, 2022).

Em suma, é notório os impactos causados pela utilização dessa ferramenta sem devida lei que regulamente e padronize o funcionamento na segurança pública e que, além disso, seja proporcional e assegure o equilíbrio

entre o direito à privacidade e a aplicação da lei para melhor funcionamento da segurança pública no Brasil, (ALMEIDA, 2022). Conforme Oliveira e Maldonado (2022, p.178), a inexistência de alicerce jurídico “pode resultar em um monitoramento massivo, sob controle de forças policiais e na limitação da privacidade dos cidadãos, enfraquecendo os pilares do Estado Democrático de Direito”.

Diante disso, conclui-se que a regulamentação do reconhecimento facial é imprescindível para assegurar a proteção de dados pessoais, a transparência administrativa e o controle social sobre o uso de tecnologias de vigilância, de modo a preservar os direitos e garantias constitucionais previstos no artigo 5º da Constituição Federal (Brasil, 1988) e na LGPD (Brasil, 2018).

2.3 Impactos da Tecnologia em Grupos Vulneráveis: Discriminação e Violação de Direitos Fundamentais

A ausência de regulamentação clara sobre o uso do reconhecimento facial, conforme discutido nas seções anteriores, produz efeitos diretos sobre os grupos socialmente vulneráveis, ampliando desigualdades históricas e expondo cidadãos a práticas discriminatórias. A falta de observância aos princípios constitucionais da igualdade e da dignidade da pessoa humana (art. 1º, III e art. 5º, caput, da Constituição Federal) (Brasil, 1988) e ao princípio da não discriminação previsto no art. 6º, IX, da Lei nº 13.709/2018 (Brasil, 2018) revela que o problema não se limita à esfera técnica, mas configura uma violação de direitos fundamentais.

Sob a perspectiva infraconstitucional, o artigo 6º, inciso IX, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados — LGPD) (BRASIL, 2018) estabelece o princípio da não discriminação como diretriz essencial no tratamento de dados pessoais. O uso de tecnologias de reconhecimento facial sem observância a esse princípio compromete o equilíbrio entre inovação e proteção de direitos fundamentais, sobretudo quando algoritmos e bancos de dados são utilizados sem critérios transparentes e auditáveis. O resultado é o risco de viés algorítmico e de práticas de vigilância que atingem, de maneira desproporcional, pessoas negras, mulheres e integrantes de grupos economicamente marginalizados.

Diante desse cenário, partindo do viés racial, é inegável que o sistema prisional brasileiro formou-se a partir de uma sociedade com histórico segregacionista e seletivo, com raízes fincadas na escravidão de negros africanos. Como bem pontua Sueli Carneiro (2019, p.43), a sociedade brasileira foi fundada sobre a ideologia do “dispositivo racialidade”, que “ao demarcar o estatuto humano como sinônimo de brancura irá por consequência redefinir todas as demais dimensões humanas e hierarquizá-las de acordo com a sua proximidade ou distanciamento desse padrão”.

Dessa forma pode funcionar o algoritmo do sistema de reconhecimento facial caso as faces utilizadas no treinamento não possuam representatividade equilibrada, com variações de cor e etinia (ICO, 2019). Uma pesquisa realizada pelo Massachusetts Institute of Technology (MIT), aponta que algoritmos vendidos para sistemas de reconhecimento de rostos possuem porcentagem de erro de 34,7% na identificação de mulheres negras e apenas 0,8% para homens brancos (BUOLAMWINI; GEBRU, 2018).

A autora O’Neil (2016) destaca que nenhum algoritmo é dotado de capacidade para captar toda a complexidade do mundo real e o objetivo seria separar informações relevantes e irrelevantes para facilitação do processo sob influência de seus criadores. Logo, é impossível afirmar que essas tecnologias são neutras em seu funcionamento, pelo contrário, essas revelam os valores daqueles que as criam e são formadas a partir dos mesmos conceitos discriminatórios vigentes na sociedade, (ACHIUME, 2020).

A problemática da discriminação ligada ao uso de RFs torna-se ainda mais delicada quando a ferramenta é usada no auxílio à segurança pública de um país que abriga as mais variadas etnias e um sistema penal seletivo (ALMEIDA, 2022). Como consequência do viés racista com a utilização das TRFs, não somente o direito à privacidade sofre violações, mas principalmente o direito à igualdade, um dos pilares fundamentais da democracia (SILVA, 2005).

No Brasil, casos concretos ilustram a gravidade dos riscos associados ao uso do reconhecimento facial na segurança pública. Em 2022, durante um evento no Parque de Exposições, em Salvador (BA), um homem negro foi preso erroneamente após ser identificado por um sistema de reconhecimento facial (G1, 2023). A capital baiana, um dos estados que lidera a implementação dessa

tecnologia no país, tem registrado diversos episódios de prisões equivocadas, majoritariamente envolvendo vítimas negras.

Esses episódios não constituem fatos isolados. De acordo com levantamento realizado pela Defensoria Pública do Estado do Rio de Janeiro (DPRJ), mais de 80% dos casos de erros cometidos em reconhecimentos faciais no estado envolvem pessoas negras (CONSELHO NACIONAL DE JUSTIÇA, 2023). Esses dados evidenciam que o viés discriminatório não é apenas uma possibilidade teórica, mas uma realidade concreta, agravando desigualdades raciais.

A utilização da tecnologia de reconhecimento facial, tende a reforçar práticas históricas de controle racializado e de criminalização da pobreza. Sob o argumento de modernização e eficiência, acabam-se perpetuando padrões seletivos que há muito marcam o sistema penal brasileiro. A inexistência de regulamentação específica para o uso dessa tecnologia agrava ainda mais o quadro, ampliando os riscos de violações sistemáticas a direitos fundamentais.

Portanto, é imprescindível reconhecer que o uso do reconhecimento facial, sem amparo normativo e sem salvaguardas técnicas eficazes, perpetua desigualdades raciais e viola direitos fundamentais. A eficiência tecnológica não pode se sobrepor à dignidade humana, devendo o Estado brasileiro assegurar que as inovações digitais sejam implementadas com transparência, proporcionalidade e respeito à igualdade, conforme os valores consagrados na Constituição Federal (Brasil, 1988) e na LGPD (Brasil, 2018).

CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste estudo permitiu compreender que o reconhecimento facial na segurança pública brasileira constitui um avanço tecnológico de grande impacto, capaz de otimizar procedimentos de identificação e fortalecer estratégias de investigação. No entanto, a pesquisa também demonstrou que a utilização dessa ferramenta está cercada por inúmeras controvérsias, especialmente no que diz respeito à ausência de regulamentação específica e à necessidade de conciliar eficiência operacional com a observância dos direitos e garantias fundamentais previstos na Constituição Federal.

Verificou-se que, apesar de oferecer benefícios evidentes, como a agilidade na identificação de suspeitos e a contribuição para a elucidação de crimes, o reconhecimento facial também apresenta riscos significativos. A falta de transparência quanto ao tratamento dos dados biométricos e a ausência de mecanismos claros de responsabilização favorecem práticas abusivas, expondo os cidadãos a situações de vigilância indevida e violação da privacidade. Essa realidade evidencia um cenário de desequilíbrio entre o poder tecnológico do Estado e o direito individual à proteção de dados pessoais.

O estudo revelou ainda que a implementação desordenada dessa tecnologia pode reproduzir desigualdades sociais e raciais já existentes no sistema penal brasileiro. Os erros de identificação, que afetam majoritariamente pessoas negras e grupos vulneráveis, indicam a urgência de uma regulação técnica e ética mais rigorosa. Assim, percebe-se que o avanço tecnológico, quando não acompanhado de critérios normativos bem definidos e de supervisão constante, pode reforçar padrões discriminatórios e comprometer o princípio da igualdade.

Além disso, a pesquisa evidenciou que o reconhecimento facial, enquanto ferramenta de vigilância estatal, precisa ser analisado sob uma perspectiva ampla, que leve em conta não apenas a sua eficiência, mas também os impactos sociais e humanos decorrentes de sua aplicação. A coleta massiva de dados biométricos, sem o devido controle jurídico, ameaça direitos fundamentais e pode instaurar uma cultura de monitoramento permanente, incompatível com os valores de um Estado Democrático de Direito.

Diante dessas constatações, torna-se indispensável a criação de uma legislação específica que estabeleça parâmetros claros para o uso dessa tecnologia, determinando as responsabilidades dos órgãos públicos e privados, as finalidades legítimas do tratamento de dados e os limites de atuação do poder público. É essencial que essa legislação garanta a transparência dos processos, o consentimento informado dos titulares dos dados e a fiscalização constante por órgãos competentes.

Somente com uma base legal sólida será possível assegurar que o reconhecimento facial seja utilizado de forma ética, proporcional e em conformidade com os princípios constitucionais da legalidade, da finalidade e da necessidade. O desenvolvimento tecnológico deve caminhar lado a lado com a proteção da dignidade humana, preservando a liberdade individual e a confiança da sociedade nas instituições públicas.

Conclui-se, portanto, que o reconhecimento facial pode contribuir para o fortalecimento da segurança pública, desde que utilizado com responsabilidade, critério técnico e respeito às normas jurídicas. O desafio que se impõe à sociedade brasileira é o de harmonizar o progresso tecnológico com a proteção dos direitos fundamentais, de modo que a inovação sirva ao bem comum e não à restrição de liberdades. Somente com esse equilíbrio será possível construir um modelo de segurança pública moderno, justo e comprometido com os valores democráticos de liberdade, igualdade e justiça social.

REFERÊNCIAS BIBLIOGRÁFICAS

ACCOUNTABILITY, and Transparency. *Proceedings of Machine Learning Research*, v. 81, p. 1–15, 2018.

ACHIUME, Tendayi. Racial discrimination and emerging digital technologies: a human rights analysis: report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance. **United Nations Digital Library**, 2020.

ALENCAR, Itana. **Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por 'racismo algorítmico**'; inocente ficou preso por 26 dias. G1: Bahia, Salvador, 1 set. 2023. Disponível em: https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoes-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-preso-por-26-dias.ghtml. Acesso em: 22 out 2025.

ALMEIDA, E. C. Os grandes irmãos: O uso de tecnologias de reconhecimento facial para persecução penal. Revista Brasileira de Segurança Pública. p. 264–283, 2022.

ARAÚJO, R. A.; CARDOSO, N. D.; DE PAULA, A. M. **Regulação e uso do reconhecimento facial na segurança pública do Brasil.** Revista de Doutrina Jurídica. v. 112, 2021.

BAHIA DE VALOR. **Governo baiano investe R$ 665 milhões e amplia o serviço de reconhecimento facial e de placas**. Salvador, 25 jul. 2023. Disponível em: <https://badevalor.com.br/governo-baiano-investe-r665-milhoes-e-amplia-o-servico-de-reconhecimento-facial-e-de-placas/>. Acesso em: 22 out.

BRASIL. **Constituição (1988). Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 out. 2025.

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 a matéria. *Diário Oficial da União*: seção 1, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 26 out. 2025

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Brasília, DF:** Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 6 abril 2025

BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. **Conference on Fairness, Accountability, and Transparency, Proceedings of Machine Learning Research,** v. 81, p. 1–15, 2018.

CARNEIRO, Sueli. **A construção do outro como não-ser como fundamento do ser.** 2005. 339 p. Tese (Doutorado em Educação). Universidade de São Paulo, São Paulo, 2005, p. 43. Disponível em: https://negrasoulblog.wordpress.com/wp-content/uploads/2016/04/a-construc3a7c3a3o-do-outro-como-nc3a3o-ser-como-fundamento-do-ser-sueli-carneiro-tese1.pdf.

DONEDA, D. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. *[S.l.]*: Thomson Reuters Brasil, 2019.

EXPRESSO – ESTADÃO. **Smart Sampa ajuda a prender 7 foragidos da Justiça por dia**. *São Paulo,* 26 mar. 2025. Disponível em: <https://expresso.estadao.com.br/sao-paulo/2025/03/26/smart-sampa-ajuda-a-prender-7-foragidos-da-justica-por-dia/>. Acesso em: 22 out. 2025.

G1 – FANTÁSTICO. *'Medo, frustrado e constrangido', diz homem detido por engano em estádio após erro do sistema de reconhecimento facial.* Rio de Janeiro, 21 abr. 2024. Disponível em:

<https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml>. Acesso em: 22 out. 2025.

MELO, Jairo Simão Santana; NEVES, Thiago Arruda; NETO, Celso Oliveira. AMON: Controle de acesso do jurisdicionado no TJDFT a partir de técnicas de reconhecimento facial**. Revista Eletrônica do CNJ**, Brasília, v. 5, n. 1, p. 128-140, jan./jun. 2021.

NASCIMENTO, Paulo. Dinheiro gasto por ano com reconhecimento facial na Bahia custearia um hospital por 32 anos e 1,5 mil ambulâncias. **The Intercept Brasil**, [*s.l.*], 31 jul. 2023. Disponível em: https://www.intercept.com.br/2023/07/31/reconhecimento-facial-na-bahia-custearia-um-hospital-e-mil-ambulancias-com-uti/. Acesso em: 22 out 2025.

OLIVEIRA, B. B.; MALDONADO, G. S. A necessária regulação do reconhecimento facial no Brasil diante dos riscos à intimidade e à privacidade. **Revista RIOS**, v. 35, p. 160–182, 2022.

OLIVEIRA, Loryne Viana *et al.* Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil. **Revista Tecnologia e Sociedade**, v. 18, n. 50, p. 114, 2022.

O'NEIL, Cathy. Weapons of math destruction. New York: Broadway Books, 2016.

PORTAL R7. *Programa da Polícia Civil identifica homem errado e inocente é preso.* Disponível em: <https://noticias.r7.com/brasilia/programa-da-policia-civil-identifica-homem-errado-e-inocente-e-preso-17122021/>. Acesso em: 22 out. 2025.

SÃO PAULO (Município). Secretaria Municipal de Segurança Urbana. *Programa Smart Sampa.* São Paulo, [2023]. Disponível em: https://capital.sp.gov.br/web/seguranca_urbana/w/smart-sampa-2. Acesso em: 22 out. 2025.

SÃO PAULO (Município). Prefeitura. *Smart Sampa: Prisômetro.* São Paulo, 2025. Disponível em: https://smartsampa.prefeitura.sp.gov.br/#prisometro. Acesso em: 22 out. 2025.

SILVA, Rosane Leal da; SILVA, Fernanda dos Santos Rodrigues da. "Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro". In: **ANAIS DO 5º CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE: MÍDIAS E DIREITOS DA SOCIEDADE EM REDE**, Santa Maria (RS), 2 e 3 set. 2019. Santa Maria: Universidade Federal de Santa Maria, 2019. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/5.23.pdf. Acesso em: 3 nov.