A POSSIBILIDADE DO USO DAS CÂMERAS DE RECONHECIMENTO FACIAL PELAS FORÇAS DE SEGURANÇA PÚBLICA[37]

Handerson Renato Deduch[38]

Data de submissão: 13/08/2025
Aceito em: 13/11/2025

Resumo: O presente artigo analisa o papel do reconhecimento facial como instrumento inovador e estratégico na promoção da segurança pública no Brasil. Partindo do dever constitucional do Estado de garantir a ordem pública e a incolumidade das pessoas, o estudo apresenta os fundamentos técnicos do reconhecimento facial, sua evolução tecnológica e as principais aplicações em diferentes unidades federativas. Demonstra-se que a utilização de câmeras inteligentes e sistemas automatizados potencializa a identificação de foragidos e a localização de desaparecidos, contribuindo para maior eficiência e celeridade das ações policiais. O artigo também examina os desafios jurídicos decorrentes da ausência de regulamentação específica, as lacunas da Lei Geral de Proteção de Dados e a necessidade de governança ética e validação humana obrigatória. São debatidos riscos e limitações técnicas, bem como os avanços recentes na acurácia dos algoritmos e a tendência de integração com big data e videomonitoramento em tempo real. A análise evidencia que o reconhecimento facial é ferramenta indispensável para a segurança pública contemporânea. Por fim, recomenda-se a consolidação de marcos regulatórios robustos e a adoção de protocolos de auditoria e controle externo, a fim de equilibrar a eficiência operacional com as garantias constitucionais do Estado Democrático de Direito.

Palavras-chave: direitos fundamentais; inteligência artificial; LGPD; reconhecimento facial; segurança pública.

Abstract: This article examines facial recognition as an innovative and strategic instrument for strengthening public security in Brazil. Grounded in the State's constitutional duty to safeguard public order and the integrity of individuals, the study outlines the technology's technical foundations, traces its evolution, and reviews key applications across Brazilian federative units. It shows how smart cameras and automated matching systems can accelerate the identification of fugitives and the location of missing persons, thereby improving the efficiency and timeliness of police operations. The article also maps the main legal challenges arising from the absence of specific regulation, gaps and interpretive uncertainties under the Brazilian General Data Protection Law (LGPD), and the need for ethical governance with mandatory human-in-the-loop validation. It discusses risks and technical limitations, as well as recent gains in algorithmic accuracy and the trend toward integration with big data analytics and real-time video monitoring. The analysis concludes that facial recognition has become an indispensable tool for contemporary public security. Finally, it recommends consolidating robust regulatory frameworks and adopting standardized audit protocols and external oversight to reconcile operational efficiency with constitutional guarantees in a democratic rule-of-law state.

Keywords: artificial intelligence; Brazilian General Data Protection Law (LGPD); facial recognition; fundamental rights; public security.

[37] O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (Capes) – Código de Financiamento 001 "*This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (Capes) – Finance Code 001*".

[38] Agente de Polícia Civil em Santa Catarina. Mestrando em Direitos e Garantias Fundamentais pela UNOESC. Pós-graduado em Ciências Policiais e Investigação Criminal, Direito Constitucional e Direito Militar. E-mail: handerson-deduch@pc.sc.gov.br.

1 INTRODUÇÃO

A segurança pública brasileira vive um período de transformações intensas, marcado pelo crescimento da criminalidade organizada, pela complexidade da violência urbana e pelo surgimento de novas modalidades delitivas que exploram a mobilidade, o anonimato e recursos tecnológicos sofisticados. Nesse cenário, a Constituição Federal impõe ao Estado, como dever inafastável, a preservação da ordem pública, da integridade das pessoas e da proteção do patrimônio (CF, art. 144) — missão que demanda constante aprimoramento de estratégias e ferramentas.

O modelo tradicional de policiamento e investigação, baseado exclusivamente na atuação humana e em técnicas convencionais, revela-se, por vezes, insuficiente para responder à velocidade e à sofisticação das dinâmicas criminais contemporâneas (Rezende, 2025). Nesse contexto, o uso de sistemas de reconhecimento facial tem se destacado como instrumento capaz de ampliar a eficiência das ações estatais, viabilizando a prisão de foragidos, a localização de pessoas desaparecidas e a prevenção de fraudes (Governo da Bahia, 2024; Saraiva, 2025).

A disseminação dessa tecnologia, contudo, não está isenta de controvérsias. O debate nacional e internacional envolve questões como a limitação do uso em espaços públicos, a proteção de dados sensíveis, a necessidade de transparência e de revisão humana, além da salvaguarda dos direitos fundamentais dos cidadãos (Santos, 2021; Hurel; Rielli, 2022).

Diante disso, o problema que orienta esta pesquisa consiste em indagar se o uso do reconhecimento facial pelas forças de segurança pública brasileiras é juridicamente legítimo, eficiente e compatível com a proteção dos direitos fundamentais. O presente estudo analisa, sob uma perspectiva crítica e multidisciplinar, a legalidade, os benefícios, as limitações e os riscos do uso dessa tecnologia. Examina-se, ainda, sua base técnica, o enquadramento na Lei Geral de Proteção de Dados, as experiências empíricas nos entes federativos, o marco regulatório em construção e recomendações para adoção ética e eficiente.

A metodologia adotada neste artigo é qualitativa, com abordagem exploratória e caráter interdisciplinar, apoiando-se em revisão bibliográfica e

documental de fontes doutrinárias, normativas e jurisprudenciais, bem como em dados empíricos de experiências práticas no Brasil. Foram analisados documentos oficiais, pareceres institucionais, relatórios técnicos, decisões judiciais, notícias jornalísticas e literatura especializada nas áreas de direito constitucional, proteção de dados, tecnologia da informação e segurança pública (CNJ, 2022; UFSM, 2024).

O objetivo é contribuir para o amadurecimento do debate e para a consolidação de uma política de segurança pública que seja atual, eficaz e alinhada aos valores constitucionais do Estado Democrático de Direito, conciliando proteção coletiva e respeito às garantias individuais (CNJ, 2024; Santos, 2021). Para tanto, o artigo organiza-se da seguinte forma: o primeiro tópico apresenta os fundamentos técnicos do reconhecimento facial; o segundo aborda sua relação com a LGPD; o terceiro discute riscos, falhas e desafios éticos; o quarto examina a evolução tecnológica e tendências futuras; e, por fim, apresentam-se as considerações finais.

2 FUNDAMENTOS TÉCNICOS DO RECONHECIMENTO FACIAL

O reconhecimento facial constitui uma das tecnologias biométricas mais avançadas disponíveis na atualidade, permitindo a identificação ou autenticação de indivíduos a partir da análise automatizada de características morfológicas únicas do rosto humano. Essa análise é realizada por meio de algoritmos de inteligência artificial (IA) e visão computacional, que capturam imagens – estáticas ou em tempo real – e as comparam com registros armazenados em bancos de dados, a fim de confirmar identidades ou localizar correspondências (Ribeiro, 2023; Almança; Rospa, 2024).

A evolução técnica dessa área foi marcada pela transição de métodos estatísticos clássicos, como *Eigenfaces* e *Fisherfaces*[39], para arquiteturas

[39] Eigenfaces e Fisherfaces são métodos clássicos de reconhecimento facial anteriores ao deep learning. "Eigenfaces" significa *faces próprias*, técnica baseada na Análise de Componentes Principais (PCA) para extrair características dominantes do rosto. Já "Fisherfaces", ou *faces de Fisher*, utiliza a Análise Discriminante Linear (LDA) para maximizar a separação entre diferentes identidades, tornando o reconhecimento mais robusto a variações de iluminação e expressão.

modernas baseadas em redes neurais convolucionais (*Convolutional Neural Networks* – CNNs[40]) e *deep learning*[41]. Essas novas abordagens elevaram a acurácia para patamares superiores a 99% em bancos de dados controlados (Braga, 2023; Kinuta et al., 2006). Contudo, desafios como viés algorítmico, condições de iluminação, ângulo de captura e envelhecimento facial ainda afetam o desempenho em cenários reais (Almança; Rospa, 2024).

O funcionamento típico do sistema de reconhecimento facial compreende cinco etapas técnicas: (i) detecção do rosto na imagem ou vídeo; (ii) alinhamento e pré-processamento para padronização; (iii) extração das características biométricas em vetores numéricos; e (iv) comparação com registros de um banco de dados. Decisão final, que, no contexto da segurança pública, deve ser validada por operador humano antes de qualquer ação (Ribeiro, 2023).

Esses sistemas podem processar milhares de faces por segundo e integrar-se a bases como o Banco Nacional de Mandados de Prisão (BNMP) e o Sistema Nacional de Informações de Segurança Pública (Sinesp), ampliando o alcance de políticas de monitoramento e investigação (Impacta, 2024).

A experiência internacional demonstra que o reconhecimento facial, embora tecnologicamente avançado, não está isento de falhas e vieses. Em diferentes países da América Latina, se observa que a ausência de protocolos claros de auditoria, revisão humana e supervisão institucional contribui para questionamentos sobre a proporcionalidade, transparência e impacto dessa tecnologia sobre os direitos fundamentais, reforçando a necessidade de governança robusta, validação humana e mecanismos de controle externo (Mascarenhas, 2023, p. 22-26).

No Brasil, além de seu uso em aeroportos, estádios e eventos, há integração com sistemas de *big data* e videomonitoramento em tempo real, potencializando

[40] Convolutional Neural Networks (CNNs), ou *redes neurais convolucionais*, são modelos de inteligência artificial projetados para processar imagens por meio de camadas que extraem padrões visuais — como bordas, formas e texturas — permitindo identificar rostos com alta precisão. Elas revolucionaram o reconhecimento facial ao substituir métodos estatísticos clássicos por arquiteturas profundas capazes de aprender representações complexas diretamente dos dados.

[41] Deep learning, ou *aprendizado profundo*, é um subcampo da inteligência artificial baseado no uso de redes neurais com múltiplas camadas capazes de aprender representações complexas dos dados, permitindo alto desempenho em tarefas como reconhecimento facial, visão computacional e processamento de linguagem natural.

tanto a prevenção e repressão quanto as discussões éticas sobre privacidade e proteção de dados (Serasa Experian, 2024). A aplicação em larga escala exige observância à Lei Geral de Proteção de Dados (LGPD) e adoção de salvaguardas como validação humana, auditorias independentes e protocolos de governança.

Assim, embora o potencial operacional seja elevado, a consolidação de seu uso legítimo na segurança pública depende da harmonização entre eficiência tecnológica e salvaguarda dos direitos fundamentais, prevenindo arbitrariedades e garantindo a conformidade com o Estado Democrático de Direito.

3 RECONHECIMENTO FACIAL E A LGPD: FUNDAMENTOS, LACUNAS E DESAFIOS JURÍDICOS

O reconhecimento facial, como tecnologia de identificação biométrica automatizada, envolve o tratamento massivo de dados sensíveis e impõe relevantes desafios à proteção da privacidade, autodeterminação informativa[42] e direitos fundamentais dos indivíduos. No Brasil, a principal referência normativa sobre o tema é a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), que regula o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica de direito público ou privado.

A LGPD classifica os dados biométricos, incluindo padrões faciais capturados e processados por sistemas de reconhecimento facial, como dados pessoais sensíveis, sujeitos a requisitos rigorosos para coleta, armazenamento e compartilhamento (LGPD, art. 5º, II e § 2º; Santos, 2021). O tratamento desses dados exige, em regra, consentimento expresso do titular ou justificativa fundamentada em hipóteses legais específicas, tais como segurança pública, proteção à vida ou execução de políticas públicas pelo Estado (LGPD, art. 11).

Contudo, a própria LGPD estabelece limites ao seu campo de incidência ao excluir expressamente de sua aplicação o tratamento de dados realizado para fins

[42] A autodeterminação informativa consiste no direito do indivíduo de controlar os próprios dados pessoais, decidindo quando, como e para que finalidade eles serão coletados, processados, utilizados ou compartilhados. A noção, formulada originalmente pelo Tribunal Constitucional Alemão (BVerfG, 1983) no célebre *Censo Decision*, foi incorporada à doutrina brasileira por autores como Danilo Doneda e Stefano Rodotà, tornando-se fundamento central das políticas de proteção de dados e da própria LGPD, ao assegurar ao titular o poder de governar sua identidade digital e limitar ingerências estatais ou privadas indevidas.

exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão penal, conforme dispõe o art. 4º, III. O legislador, atento à sensibilidade desses contextos, determinou que tais hipóteses "*serão objeto de legislação específica, que deverá prever regras proporcionais e adequadas para regular o tratamento dos dados pessoais*" (LGPD, art. 4º, § 1º).

Na prática, entretanto, essa legislação específica ainda não foi aprovada, produzindo um vácuo normativo relevante no tratamento de dados por forças de segurança pública. O chamado "*Anteprojeto da LGPD Penal*", elaborado por grupo de trabalho coordenado pelo Ministério da Justiça e por especialistas em proteção de dados, tramita há anos sem conversão em lei, deixando órgãos policiais, peritos, delegados e demais operadores do sistema de justiça sem parâmetros claros quanto a bases legais, limites, salvaguardas e mecanismos de controle aplicáveis ao tratamento de dados sensíveis, especialmente dados biométricos faciais (Santos, 2021; CNJ, 2022).

A ausência desse marco normativo compromete a autodeterminação informativa, princípio estruturante da proteção de dados no Brasil defendido por autores como Danilo Doneda, Bruno Bioni e Laura Schertel Mendes, ao permitir que atividades estatais de vigilância e identificação tecnológica ocorram sem balizas proporcionais, critérios uniformes de minimização ou instrumentos efetivos de transparência e responsabilização. Compatibilizar as necessidades operacionais de segurança pública com a tutela dos direitos fundamentais no ambiente digital exige, portanto, uma legislação específica que discipline o uso de tecnologias de identificação automatizada.

Essa lacuna regulatória contribui para que sistemas de reconhecimento facial empregados por órgãos de segurança pública funcionem em uma verdadeira "*zona cinzenta*"[43], sem garantias claras de proteção à privacidade, limites de uso, auditorias independentes, direitos do titular ou mecanismos robustos de responsabilização por abusos (Santos, 2021; Revista Forças de

[43] O termo "zona cinzenta" é utilizado para designar contextos em que a atuação estatal ocorre sem regulamentação específica, sem critérios claros de controle e com baixa previsibilidade normativa. No campo da proteção de dados e da segurança pública, a expressão descreve situações em que tecnologias de vigilância — como o reconhecimento facial — são empregadas sem parâmetros definidos de transparência, auditoria, proporcionalidade ou responsabilização, criando um ambiente de indeterminação jurídica e fragilização das garantias fundamentais.

Segurança & Tecnologia, 2024). Esse cenário tampouco é exclusivo do Brasil: estudos comparativos multinacionais demonstram que países com legislações fragmentadas ou lacunares enfrentam riscos maiores de uso abusivo da tecnologia e maior insegurança jurídica, reforçando a necessidade de marcos normativos abrangentes, específicos e alinhados aos parâmetros de direitos fundamentais (Dp et al., 2023).

Nesse contexto, princípios fundamentais da LGPD, como adequação, necessidade, segurança, não discriminação e responsabilização, deveriam ser observados como parâmetros mínimos, mesmo na ausência de regulação específica (Santos, 2021; Almança; Rospa, 2024). O artigo *Facial Recognition Technology: A Multinational Analysis of Regulatory Framework, Ethics, and Legal Implications in Security and Privacy*[44] reforça que, internacionalmente, modelos regulatórios eficazes tendem a adotar não apenas princípios genéricos de proteção de dados, mas também disposições operacionais claras sobre transparência, auditoria e controle social, prevenindo tanto o uso discriminatório quanto a vigilância excessiva (Dp et al., 2023).

No debate doutrinário, recomenda-se que, enquanto não houver legislação própria, a implantação de sistemas de reconhecimento facial no setor público obedeça aos seguintes parâmetros mínimos: (i) finalidade legítima e definida (segurança pública, prevenção de crimes, localização de foragidos ou desaparecidos); (ii) proporcionalidade e minimização dos dados coletados; (iii) armazenamento seguro e temporário, com exclusão de dados não utilizados após prazo definido; (iv) transparência, relatório de impacto e prestação de contas à sociedade e órgãos de controle (Ministério Público, Defensoria, CNJ); (v) validação humana obrigatória antes de qualquer medida restritiva; (vi) direito de revisão e contestação em caso de erro; e (vii) auditoria independente e divulgação de estatísticas de uso, eficácia e falhas (Santos, 2021; Silva et al., 2024; Conselho Nacional de Justiça, 2022; Dp et al., 2023).

O anteprojeto da "*LGPD Penal*" propõe avanços significativos, como a obrigatoriedade de relatórios de impacto de vigilância, a necessidade de

[44] Tecnologia de Reconhecimento Facial: Uma Análise Multinacional dos Marcos Regulatórios, da Ética e das Implicações Jurídicas em Segurança e Privacidade

autorização judicial para uso contínuo em espaços públicos, a fiscalização centralizada pelo CNJ e a avaliação de risco prévia à implementação (Santos, 2021). No entanto, outros projetos recentes, como o Projeto de Lei nº 1012/2025, ainda se limitam a disciplinar o uso do reconhecimento facial em rodoviárias, sem abordar de forma abrangente a proteção de dados, os direitos do titular ou protocolos de auditoria, lacuna que reforça a urgência de um marco legal completo.

Em síntese, o reconhecimento facial no Brasil não conta com marco legal específico para sua aplicação em segurança pública, tornando imprescindível a observância dos princípios da LGPD, a adoção de boas práticas de governança e a aprovação célere de legislação própria. Experiências internacionais demonstram que a regulação clara e detalhada reduz riscos e aumenta a confiança social, permitindo equilibrar eficiência na segurança e proteção efetiva dos direitos fundamentais (Santos, 2021; Almança; Rospa, 2024; Dp et al., 2023).

Diante da complexidade jurídica apresentada e das lacunas regulatórias ainda existentes, o próximo capítulo analisará as experiências concretas de implementação do reconhecimento facial em diferentes estados e municípios brasileiros, destacando resultados, desafios e boas práticas que auxiliam na conciliação entre eficácia operacional e proteção dos direitos fundamentais.

3.1 Aplicações práticas e resultados do reconhecimento facial na segurança pública

Desde 2018, o reconhecimento facial se consolidou como uma ferramenta estratégica no Brasil, acompanhando a expansão dos sistemas de videomonitoramento, a integração de bancos de dados e o avanço das soluções tecnológicas voltadas à segurança pública. Estados como Bahia, São Paulo, Santa Catarina, Paraná e o Distrito Federal têm liderado iniciativas, implementando modelos regionais que integram câmeras públicas e privadas a sistemas de inteligência artificial. Entre 2020 e 2024, o número de municípios brasileiros com uso dessa tecnologia mais que dobrou, de cerca de 40 para mais de 90, resultado

de políticas públicas, investimentos estaduais e parcerias público-privadas (Souza, 2024; Gazeta do Povo, 2025).

A Bahia tornou-se referência nacional na adoção em larga escala. Desde a ativação do sistema em 2018, já foram efetuadas mais de 1.100 prisões de foragidos até setembro de 2024, além de localizações de desaparecidos e suporte a operações de grande porte (Ascom, 2024). O protocolo adotado prevê emissão de alerta automático, checagem presencial por policiais e validação humana obrigatória antes de qualquer ação, o que reduz riscos de falsos positivos e assegura o devido processo legal. Situações de erro já foram registradas, mas corrigidas de forma institucional, reforçando a importância da revisão manual (Melo; Serra, 2022; Santos, 2021).

Em São Paulo, o projeto *Smart Sampa* integra até 40 mil câmeras, entre públicas e privadas, ao sistema de reconhecimento facial (Estratégia Jurídico, 2025). Desde sua implementação, foram contabilizadas 1.902 prisões em flagrante, 719 capturas de foragidos e 41 localizações de pessoas desaparecidas. O sistema opera com protocolos rigorosos de validação e conta com participação ativa da Defensoria Pública e de órgãos de controle, buscando equilíbrio entre eficácia policial e respeito aos direitos fundamentais, especialmente em eventos de grande porte (Gazeta do Povo, 2025).

Em Santa Catarina, o governo investiu mais de R$ 40 milhões na universalização da tecnologia, instalando mil câmeras em 60 municípios, cobrindo cerca de 70% da população (Gazeta do Povo, 2025). O sistema, integrado ao CIASC, é utilizado em eventos como o Carnaval de Florianópolis, a Oktoberfest e a Festa do Pinhão. Os protocolos incluem criptografia, anonimização de dados e uso de drones para cobertura aérea, garantindo conformidade com a LGPD (Gazeta do Povo, 2025; Silva, 2025).

No Paraná, projetos como Olho Vivo e Falcão ampliam o alcance da vigilância ao integrar câmeras públicas e privadas, com monitoramento em tempo real pela Polícia Militar. O modelo de parceria público-privada tem sido eficaz na prisão de foragidos, prevenção de crimes e controle de acesso a terminais e eventos de massa (Kinape, 2025).

O Distrito Federal destaca-se por possuir regulamentação específica (Lei nº 6.712/2020) e por integrar o reconhecimento facial ao Centro Integrado de Operações de Brasília (CIOB) (Correio Braziliense, 2025). A operação é acompanhada por auditorias externas, exclusão automática de dados não utilizados e publicação periódica de relatórios. Desde 2022, o sistema contribuiu para a prisão de centenas de foragidos e para a prevenção de fraudes em concursos públicos, sempre sob fiscalização do Ministério Público, da Defensoria Pública e da Ordem dos Advogados do Brasil, seccional Distrito Federal.

No cenário internacional, há diversidade de abordagens. O Reino Unido emprega a tecnologia em eventos esportivos e áreas públicas, com forte supervisão judicial e protocolos de auditoria (Melo; Serra, 2022). A China adota o uso massivo, mas enfrenta críticas relacionadas à vigilância em larga escala e à privacidade. Já nos Estados Unidos e na União Europeia, predominam debates sobre restrições, moratórias e proibições locais, diante de riscos de erros e violações de direitos.

Os exemplos analisados demonstram que o reconhecimento facial oferece benefícios concretos para a segurança pública: identificação rápida de foragidos e desaparecidos, prevenção de crimes em áreas críticas, elucidação de fraudes e suporte à persecução penal (Impacta, 2024; Revista Segurança Eletrônica, 2024). A presença ostensiva de câmeras e alertas automáticos tem efeito dissuasório sobre a criminalidade e aumenta a sensação de segurança (Metodotelecom, 2024; Gazeta do Povo, 2025).

Entretanto, mesmo diante dos avanços, importantes desafios permanecem. A ocorrência de falsos positivos, especialmente em situações de baixa qualidade de imagem, ângulo inadequado ou variações de iluminação, continua sendo um ponto crítico na utilização da tecnologia (Santos, 2021; Almança; Rospa, 2024). Diante desse cenário, organizações da sociedade civil, como ONGs e Defensorias Públicas, têm defendido a adoção de salvaguardas robustas, incluindo a validação humana obrigatória, auditorias independentes e mecanismos efetivos de contestação para qualquer cidadão indevidamente identificado (Silva et al., 2024).

A experiência brasileira revela que a legitimidade e a aceitação social dessa tecnologia dependem da adoção de protocolos claros, como validação e revisão

humana, exclusão automática de dados não utilizados, transparência nos resultados e participação efetiva de órgãos de controle e sociedade civil (Correio Braziliense, 2025; Silva, 2025). Investimentos em campanhas educativas e treinamento contínuo de operadores também se mostram fundamentais para mitigar riscos e garantir o uso ético e eficiente (Kinape, 2025; Santos, 2021).

Assim, embora os resultados obtidos sejam expressivos, o reconhecimento facial na segurança pública deve ser constantemente acompanhado de mecanismos de supervisão, auditoria e salvaguarda de direitos fundamentais. O capítulo seguinte analisará justamente os riscos, falhas e desafios éticos associados ao uso intensivo dessa tecnologia, identificando medidas que podem assegurar seu emprego legítimo, proporcional e socialmente aceitável no Brasil.

4 RISCOS, FALHAS E DESAFIOS ÉTICOS DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

Apesar dos avanços expressivos das últimas décadas, a precisão do reconhecimento facial permanece fortemente condicionada a fatores ambientais e operacionais. Aspectos como iluminação inadequada, ângulo desfavorável da câmera, baixa qualidade de imagens, movimentação intensa de pessoas e alterações naturais da fisionomia, como o envelhecimento, impactam diretamente a performance dos sistemas. Em cenários de grande fluxo, como eventos de massa, rodoviárias e centros urbanos, é comum a ocorrência de falsos positivos (identificação incorreta de uma pessoa como outra) e falsos negativos (não reconhecimento de uma pessoa registrada), situações que podem resultar em abordagens injustificadas e até prisões indevidas (Almança; Rospa, 2024; Kinape, 2025).

Casos concretos, tanto no Brasil quanto no exterior, demonstram que tais falhas não são meramente teóricas. Muitas vezes, problemas decorrem da utilização de imagens captadas em condições não ideais ou da existência de bancos de dados incompletos ou desatualizados (Impacta, 2024; Gazeta do Povo, 2025).

No setor público, o uso dessa tecnologia suscita implicações diretas sobre direitos constitucionais, notadamente o direito à privacidade, à proteção de dados pessoais, à presunção de inocência e à liberdade de circulação. Sem critérios claros de utilização, protocolos de validação humana e auditorias independentes, sistemas de reconhecimento facial podem contribuir para a formação de cenários de vigilância massiva, capazes de gerar efeitos inibitórios sobre a livre expressão e o convívio social (Santos, 2021; Silva et al., 2024).

Outro desafio estrutural é a ausência de legislação específica que regule a aplicação do reconhecimento facial na segurança pública, especialmente no que se refere à coleta, armazenamento e uso dos dados. Essa lacuna normativa, aliada à falta de transparência sobre os critérios técnicos e operacionais, aumenta o risco de uso desproporcional e dificulta o controle institucional (Almança; Rospa, 2024; CNJ, 2022).

A transparência, nesse contexto, é elemento central. É imprescindível que haja divulgação pública de relatórios contendo informações como: (i) critérios técnicos que orientam o funcionamento dos algoritmos; (ii) quantidade de alertas emitidos; (iii) número de abordagens decorrentes; e (iv) indicadores de acerto, erro e eficácia. Sem tais relatórios e sem auditorias externas periódicas, torna-se difícil avaliar se a tecnologia está, de fato, contribuindo para a segurança pública e se seu uso atende aos princípios da proporcionalidade e da legitimidade (Silva et al., 2024; Melo; Serra, 2022; CNJ, 2022).

A ausência de mecanismos robustos de prestação de contas prejudica a responsabilização institucional e pode corroer a confiança da população nas forças de segurança. Essa confiança, uma vez perdida, é de difícil recuperação e compromete a legitimidade de políticas públicas de vigilância.

A literatura técnica e a experiência de países com regulamentações mais avançadas sugerem medidas para mitigar riscos e reforçar a legitimidade do uso dessa tecnologia. Entre as recomendações mais recorrentes, destacam-se: (i) validação humana obrigatória de todos os alertas antes de qualquer abordagem ou medida restritiva; (ii) relatórios públicos periódicos com estatísticas detalhadas de acertos, erros e impactos práticos; (iii) auditorias externas independentes, preferencialmente com participação de órgãos de controle e sociedade civil; (iv)

garantia do direito de revisão e contestação para indivíduos eventualmente prejudicados por erros; (v) exclusão automática de dados não utilizados, com critérios objetivos e prazos claros para armazenamento; e (vi) treinamento contínuo de operadores, visando reduzir erros de interpretação e dependência excessiva da máquina.

Avanços recentes em inteligência artificial, como o desenvolvimento de modelos mais explicáveis (*Explainable AI*[45]) e o aprimoramento de algoritmos de redes neurais, têm aumentado a acurácia e reduzido a incidência de vieses. Esses progressos indicam uma tendência promissora para os próximos anos, sobretudo se acompanhados de protocolos rigorosos, regulação robusta e controle social efetivo.

Assim, compreender e enfrentar os riscos não significa inviabilizar o uso do reconhecimento facial, mas, sim, criar as bases para que sua aplicação seja legítima, proporcional e socialmente aceita. O próximo capítulo examinará justamente essa evolução tecnológica e as perspectivas futuras, identificando como as inovações em curso podem superar parte dos desafios atuais e consolidar o papel estratégico dessa ferramenta na segurança pública brasileira.

5 A FRANCA EVOLUÇÃO TECNOLÓGICA E O FUTURO DO RECONHECIMENTO FACIAL

Apesar dos desafios operacionais e das limitações apontadas nos capítulos anteriores, o reconhecimento facial desponta como uma tecnologia em franca e contínua evolução, impulsionada pelo avanço acelerado tanto do hardware quanto do software. O desenvolvimento de câmeras de altíssima resolução, a melhoria dos sensores ópticos e a integração com sistemas de processamento de ponta permitem capturar imagens mais nítidas e detalhadas, mesmo em condições adversas (Braga, 2023).

[45] Explainable AI (XAI) refere-se a técnicas e modelos de inteligência artificial capazes de fornecer explicações compreensíveis sobre seu funcionamento, critérios de decisão e variáveis relevantes. Seu objetivo é aumentar transparência, confiabilidade e auditabilidade, especialmente em sistemas sensíveis como reconhecimento facial e tomada de decisões automatizadas (Adadi & Berrada, 2018).

No campo algorítmico, as redes neurais convolucionais (CNNs) e arquiteturas de ponta, como *FaceNet*[46], *DeepFace*[47] e *ArcFace*[48], alcançam hoje índices de acurácia superiores a 99% em bases de dados controladas, aproximando-se, e em alguns casos superando, a capacidade humana de identificação facial. Tais modelos incorporam mecanismos capazes de corrigir automaticamente variações de iluminação, ângulo, expressões faciais e até pequenas alterações decorrentes do envelhecimento, ampliando a confiabilidade das identificações em contextos operacionais (Braga, 2023; Impacta, 2024).

Esses avanços permitem que sistemas modernos processem comparações em tempo real com milhões de registros simultaneamente, reduzindo drasticamente o tempo de resposta das forças de segurança e potencializando operações preventivas e investigativas (Metodotelecom, 2024). No Brasil, experiências como o ***Smart Sampa*** (São Paulo), o sistema da Bahia e as soluções integradas de Santa Catarina adotam plataformas de última geração, alcançando resultados operacionais cada vez mais expressivos (Gazeta do Povo, 2025; Estratégia Jurídico, 2025).

Entretanto, como alertam Rambe e Abdurrahman (2024), a evolução técnica, por si só, não garante legitimidade nem eficácia social. A adoção de tecnologias de alta precisão precisa ser acompanhada de marcos regulatórios claros, políticas públicas transparentes e protocolos de governança que assegurem proporcionalidade, respeito aos direitos fundamentais e mecanismos robustos de auditoria. A experiência internacional demonstra que o avanço tecnológico sem salvaguardas jurídicas e institucionais pode resultar em riscos

[46] FaceNet é um modelo de reconhecimento facial desenvolvido pelo Google, baseado em redes neurais profundas, que transforma imagens de rostos em vetores numéricos altamente discriminantes (*embeddings*). Ele utiliza *triplet loss* para maximizar a distância entre identidades distintas e minimizar a distância entre imagens da mesma pessoa, tornando-se um dos sistemas mais precisos e influentes da área (Schroff; Kalenichenko; Philbin, 2015).

[47] DeepFace é um modelo criado pelo Facebook que utiliza uma rede neural profunda com nove camadas para mapear rostos em representações tridimensionais, alcançando precisão próxima à humana em tarefas de verificação facial. Foi um dos primeiros sistemas a demonstrar o potencial do *deep learning* no reconhecimento facial em larga escala (Taigman et al., 2014).

[48] ArcFace é um modelo avançado de reconhecimento facial que introduz a função de perda angular (*Additive Angular Margin Loss*), aumentando a separabilidade entre identidades e melhorando a robustez do sistema. Tornou-se referência em benchmarks internacionais devido à alta precisão e à estabilidade em cenários com grande variação de iluminação, pose e expressão (Deng et al., 2019).

ampliados, incluindo violações de privacidade, discriminação e uso abusivo por autoridades.

Além disso, cresce o investimento em soluções que buscam maior explicabilidade algorítmica (*explainable AI*), permitindo rastrear e justificar as decisões automatizadas. Essa transparência é essencial para que operadores e órgãos de controle compreendam como o sistema chegou a determinada conclusão, garantindo maior possibilidade de contestação em caso de erro.

A tendência é que, nas próximas décadas, o reconhecimento facial seja cada vez mais integrado a outros recursos tecnológicos, como Big Data, análise preditiva e monitoramento inteligente, formando ecossistemas de segurança pública mais responsivos e eficazes. No entanto, como defendem Rambe e Abdurrahman (2024), essa integração deve ocorrer sob um modelo de governança colaborativa, envolvendo Estado, sociedade civil, academia e setor privado na formulação de diretrizes e na avaliação constante dos impactos.

Assim, o consenso entre especialistas é claro: com boa governança, fiscalização permanente e uso responsável, a evolução tecnológica tende a reduzir falhas e riscos operacionais, potencializando a eficiência da segurança pública sem renunciar à proteção dos direitos fundamentais. O desafio, portanto, é equilibrar inovação e garantias, de forma a construir uma política tecnológica que seja, ao mesmo tempo, eficaz e legítima no contexto democrático.

5.1 Tendências e perspectivas futuras do reconhecimento facial na segurança pública

As próximas décadas deverão consolidar o reconhecimento facial como ferramenta estratégica e transversal na segurança pública global, impulsionada não apenas pelo rápido avanço tecnológico, mas também pelo amadurecimento do debate ético, regulatório e de governança (Braga, 2023). A integração dessa tecnologia com Big Data, inteligência artificial preditiva e videomonitoramento em tempo real tende a permitir respostas policiais mais ágeis e precisas, inclusive em cenários urbanos altamente complexos e dinâmicos (Metodotelecom, 2024; Gazeta do Povo, 2025).

O futuro aponta para o desenvolvimento de algoritmos mais transparentes e auditáveis (explainable AI), capazes de fornecer rastreabilidade detalhada e permitir revisão humana criteriosa sobre as decisões automatizadas (Santos, 2021; Kinape, 2025). Além disso, espera-se a adoção de padrões internacionais de interoperabilidade, fortalecendo redes de cooperação policial e sistemas de alerta transnacional para o combate a crimes de natureza transfronteiriça, como terrorismo, tráfico de pessoas e cibercriminalidade (Braga, 2023; Impacta, 2024).

Paralelamente, segundo Rambe e Abdurrahman (2024), cresce a exigência de marcos regulatórios robustos e alinhados a princípios universais de direitos humanos, que estabeleçam protocolos claros de validação, auditorias externas independentes, participação social e prestação de contas. Essa governança democrática será determinante para assegurar que a tecnologia seja utilizada de forma legítima, proporcional e transparente, evitando abusos e garantindo confiança pública (Almança; Rospa, 2024; Melo e Serra, 2022).

Tais tendências revelam que o reconhecimento facial tende a tornar-se onipresente nas políticas de segurança pública moderna, mas a sua aceitação social e jurídica dependerá de um delicado equilíbrio entre eficiência operacional e proteção de direitos individuais. Mais do que um avanço técnico, trata-se de uma transformação institucional e cultural, exigindo do Estado a capacidade de inovar sem abrir mão das salvaguardas constitucionais.

Nesse cenário promissor, torna-se essencial compreender como a utilização prática das câmeras inteligentes já vem contribuindo, no Brasil, para a proteção dos cidadãos e para o aumento da eficiência das operações policiais. Por isso, o próximo capítulo analisará especificamente o papel dessas câmeras no contexto nacional, ressaltando como elas reforçam a responsabilidade constitucional do Estado de garantir segurança pública de qualidade para toda a sociedade.

5.2 As câmeras de reconhecimento facial e a segurança pública nacional

O reconhecimento facial, enquanto tecnologia de identificação biométrica, consolidou-se como ferramenta estratégica no apoio ao Estado para o

cumprimento do dever constitucional de garantir a segurança pública. A Constituição Federal de 1988 estabelece que "*a segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio*" (Brasil, 1988). Dessa premissa decorre o compromisso estatal de empregar meios legítimos, tecnológicos e humanos, capazes de proteger a sociedade e assegurar o exercício pleno da cidadania.

O uso de câmeras inteligentes com reconhecimento facial tem ampliado significativamente as ações de policiamento preventivo, ostensivo e investigativo. A automatização da identificação de pessoas procuradas, a localização de desaparecidos, a prevenção de fraudes e o monitoramento de grandes eventos ilustram a versatilidade da tecnologia, hoje presente em festas populares, terminais urbanos, aeroportos e rodoviárias (Ascom, 2024; Saraiva, 2025; Almança; Rospa, 2024). Os alertas em tempo real permitem respostas mais rápidas e precisas, otimizando recursos e fortalecendo a sensação coletiva de segurança (Impacta, 2024; Rebello, 2025).

Além de incrementar a eficiência operacional, a presença dessas câmeras desempenha papel relevante na dissuasão de condutas criminosas e na elucidação de delitos, contribuindo para investigações mais céleres e assertivas. Experiências concretas demonstram sua eficácia: a Bahia contabiliza mais de mil prisões de foragidos realizadas com base na tecnologia, enquanto estados como São Paulo, Santa Catarina, Paraná e o Distrito Federal vêm registrando resultados expressivos em operações policiais e na gestão da segurança urbana (Ascom, 2024; Rezende, 2025; Silva, 2025; Saraiva, 2025).

Entretanto, a adoção dessa tecnologia deve ser permanentemente condicionada aos princípios da legalidade, proporcionalidade, proteção de dados e respeito aos direitos fundamentais. Quando utilizada dentro de parâmetros legais claros e respaldada por protocolos robustos de validação humana, o reconhecimento facial não apenas fortalece a efetivação do direito constitucional à segurança pública, mas também reafirma o compromisso estatal com a manutenção da ordem e da tranquilidade social (CNJ, 2024; Brasil, 1988).

No âmbito internacional, diversos estudos têm demonstrado que a aceitação social e a legitimidade democrática do uso de tecnologias biométricas dependem diretamente da existência de marcos regulatórios sólidos, mecanismos de auditoria e níveis adequados de transparência. Entre essas pesquisas, destaca-se o estudo de Rambe e Abdurrahman (2024), que analisou experiências na Tailândia e em outros países asiáticos. Os autores observaram que a confiança pública só se consolidou onde salvaguardas efetivas, como controle externo, revisão humana obrigatória e normas de proporcionalidade, foram plenamente implementadas.

Dessa forma, é possível afirmar que o reconhecimento facial, quando empregado de forma responsável, ética e regulada, representa não apenas uma inovação tecnológica, mas uma necessidade estratégica para a segurança pública nacional. À luz dos resultados já obtidos e dos desafios ainda presentes, aprimoramento normativo, mitigação de riscos e consolidação da confiança social, torna-se imprescindível discutir como o Brasil pode transformar essa ferramenta em política pública sustentável, capaz de equilibrar eficiência operacional e proteção de direitos fundamentais. Essa reflexão prepara o terreno para as conclusões deste artigo, que enfatizarão a urgência de uma adoção transparente e devidamente regulamentada do reconhecimento facial como instrumento essencial para o fortalecimento da segurança pública e a proteção efetiva da sociedade brasileira.

6 CONSIDERAÇÕES FINAIS

O reconhecimento facial, enquanto expressão concreta do avanço tecnológico aplicado à segurança pública, assume papel cada vez mais estratégico diante da crescente complexidade e sofisticação dos desafios enfrentados pela sociedade brasileira contemporânea. Em um cenário marcado pela expansão do crime organizado, pela mobilidade social e pela emergência de novas modalidades de delitos, frequentemente praticados com elevado grau de anonimato e uso intensivo de tecnologia, o Estado, amparado pelo artigo 144 da Constituição Federal, tem o dever indeclinável de adotar todos os meios legítimos

e proporcionais para garantir a ordem pública, proteger a vida e o patrimônio, e assegurar o pleno exercício da cidadania (Brasil, 1988).

A integração de câmeras inteligentes e sistemas de reconhecimento facial às políticas públicas de segurança já demonstrou, em diversas unidades federativas, resultados concretos e mensuráveis. A identificação e prisão de milhares de foragidos, a localização de pessoas desaparecidas, a prevenção de fraudes e o monitoramento eficaz de eventos de grande porte são exemplos claros de como a tecnologia amplia a capacidade operacional das forças policiais, confere celeridade à persecução penal e contribui para a criação de ambientes urbanos mais seguros e confiáveis (Ascom, 2024; Rezende, 2025; Saraiva, 2025; Impacta, 2024; Almança; Rospa, 2024).

Todavia, não se pode ignorar que a aplicação dessa tecnologia traz consigo riscos e desafios éticos, jurídicos e técnicos, sobretudo no que diz respeito à proteção de dados pessoais, à preservação da privacidade, à garantia da transparência e ao respeito aos direitos fundamentais. Experiências internacionais, como a analisada por Rambe e Abdurrahman (2024) no contexto da Tailândia e de outros países asiáticos, evidenciam que a aceitação social e a legitimidade do reconhecimento facial dependem diretamente da existência de marcos regulatórios sólidos, protocolos de governança transparentes e mecanismos de fiscalização efetivos.

Diante disso, eventuais riscos não devem ser interpretados como justificativa para o retrocesso tecnológico ou para a omissão estatal, mas sim como incentivos para a formulação de um arcabouço normativo robusto e abrangente. Diante disso, eventuais riscos não devem ser interpretados como justificativa para o retrocesso tecnológico ou para a omissão estatal, mas sim como incentivos à formulação de um arcabouço normativo robusto e abrangente. Esse marco deve prever, de forma clara, requisitos como: (i) validação humana obrigatória antes da adoção de qualquer medida restritiva; (ii) auditorias independentes e periódicas, voltadas à avaliação de acurácia e identificação de vieses; (iii) mecanismos de controle social, garantindo participação institucional e comunitária; (iv) transparência ativa sobre métricas de desempenho, erros e

resultados operacionais; e (v) respeito inegociável aos princípios da legalidade, proporcionalidade e não discriminação.

Portanto, o reconhecimento facial, quando aplicado de forma ética, regulada e tecnicamente qualificada, não se limita a ser uma ferramenta de combate à criminalidade: ele se consolida como instrumento de concretização do pacto constitucional entre Estado e sociedade. Mais do que uma opção de política pública, sua adoção responsável e segura configura-se como exigência inadiável do tempo presente, condição essencial para que o Brasil esteja à altura do desafio de proteger seus cidadãos de maneira efetiva, inovadora e compatível com os valores democráticos.

REFERÊNCIAS

ALMANÇA, Camille; ROSPA, Aline. **Tecnologias de reconhecimento facial e algoritmos discriminatórios:** implicações e desafios na proteção de dados. Santa Maria: UFSM, 2024. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2024/12/3.10.pdf. Acesso em: 4 ago 2025.

ASSESSORIA DE COMUNICAÇÃO SOCIAL - ASCOM. **Em menos de 24 horas, sistema de reconhecimento facial da SSP localiza 4 foragidos da Justiça**. Salvador: Governo do Estado da Bahia, 2024. Disponível em: https://www.ba.gov.br/comunicacao/2024/09/noticias/em-menos-de-24-horas-sistema-de-reconhecimento-facial-da-ssp-localiza-4-foragidos-da-justica. Acesso em: 4 ago 2025.

BRAGA, Luiz Filipe Zenicola. **Reconhecimento Facial: Análise de Técnicas**. USP/BDTA, 2023. Disponível em: https://bdta.abcd.usp.br/directbitstream/46b694a0-715b-462d-a8b7-546ea4ef259d/Braga_Luiz_Filipe_Zenicola.pdf.Acesso em: 4 ago 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais – LGPD). Diário Oficial da União, Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 ago 2025.

BRASIL. **Projeto de Lei nº 1012/2025**. Obriga a instalação de câmeras de reconhecimento facial em terminais rodoviários interestaduais do país. Brasília, DF: Câmara dos Deputados, 2025. Disponível em:

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2885415&filename=Avulso+PL+1012%2F2025.Acesso em: 4 ago 2025.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Manual de Procedimentos de Reconhecimento de Pessoas: Resolução n. 484/2022.** Brasília: CNJ, 2024. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2024/10/manual-resolucao-cnj-484-2022-v8-2024-10-09.pdf. Acesso em: 4 ago 2025.

DP, A.; Mamonto, A. A. N.; Amiq, B.; Rambe, K. M.; Syahputra, A. R. **Facial Recognition Technology: A Multinational Analysis of Regulatory Framework, Ethics, and Legal Implications in Security and Privacy.** The International Journal of Science in Society, v. 5, n. 4, p. 1-15, 2023. Disponível em: https://www.ijsoc.goacademica.com/index.php/ijsoc/article/view/808. Acesso em: 4 ago 2025.

GAZETA DO POVO. **Tecnologia catarinense de reconhecimento facial ganha destaque na segurança pública**. Curitiba: Gazeta do Povo, 2025. Disponível em: https://www.gazetadopovo.com.br/conteudo-publicitario/governo-santa-catarina/tecnologia-catarinense-reconhecimento-facial/. Acesso em: 4 ago. 2025.

MELO, Paulo Victor.; SERRA, Paulo. **Tecnologia de reconhecimento facial e segurança pública nas capitais brasileiras**: apontamentos e problematizações. OpenEdition Journals, n. 42, 2022. Disponível em: https://journals.openedition.org/cs/8111. Acesso em: 4 ago 2025.

IMPACTA. **Como o reconhecimento facial combate a criminalidade**. Blog Impacta, 2024. Disponível em: https://www.impacta.com.br/blog/como-reconhecimento-facial-combate-criminalidade/.Acesso em: 4 ago 2025.

KINAPE, Rolyssom Miranda Melo. **Uso de câmeras com reconhecimento facial para identificação de pessoas com mandado de prisão:** benefícios da tecnologia e desafios frente à Lei Geral de Proteção de Dados. Brazilian Journal of Development, v. 11, n. 5, p. 1-25, 2025. Disponível em> https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/77795. Acesso em: 4 ago. 2025.

KINUTA, Cristiane *et al.* **Estudo comparativo de algoritmos para reconhecimento facial**. São Paulo, 2006. Disponível em: https://www.aedb.br/seget/arquivos/artigos06/916_Copia%20de%20Artigo%20Comparativo%20Facial.pdf. Acesso em: 3 ago 2025.

METODOTELECOM. **Reconhecimento facial: tecnologia a serviço da segurança pública**. São Paulo: Metodotelecom, 2024. Disponível em: https://www.metodotelecom.com.br/reconhecimento-facial-tecnologia-a-servico-da-seguranca-publica. Acesso em: 4 ago 2025.

REBELLO, Aiuri. **Reconhecimento facial e videomonitoramento avançam pelo Brasil.** Curitiba: Gazeta do Povo, 2025. Disponível em: https://www.gazetadopovo.com.br/brasil/reconhecimento-facial-videomonitoramento-avanca-brasil/. Acesso em: 4 ago 2025.

REZENDE, Guilherme. **Reconhecimento facial: Segurança Pública e Direitos Fundamentais**. São Paulo: Estratégia Concursos, 2025. Disponível em: https://cj.estrategia.com/portal/reconhecimento-facial-seguranca-publica-direitos/. Acesso em: 4 ago 2025.

REVISTA SEGURANÇA ELETRÔNICA. **Reconhecimento facial na segurança pública:** SAFR se torna grande aliado no combate ao crime. São Paulo: Revista Segurança Eletrônica, 2024. Disponível em: https://revistasegurancaeletronica.com.br/reconhecimento-facial-na-seguranca-publica-safr-se-torna-grande-aliado-no-combate-ao-crime/. Acesso em: 4 ago 2025.

RIBEIRO, Eliéser de Freitas. **Decifrando a tecnologia do reconhecimento facial.** 2023. Disponível em: https://medium.com/@elieser_ribeiro/decifrando-a-tecnologia-do-reconhecimento-facial-27ee45eb6ada. Acesso em: 4 ago 2025.

RAMBE, R.; ABDURRAHMAN, L. **Implikasi Etika dan Hukum dalam Penggunaan Teknologi Pengenalan Wajah: Perlindungan Privasi versus Keamanan Publik (Kajian Literatur**). Jurnal Hukum Caraka Justitia, v. 4, n. 2, p. 90-104, 2024. Disponível em: https://ejournal.up45.ac.id/index.php/JHCJ/article/view/1828. Acessado em 13 ago. 2025.

SANTOS, Jéssica Guedes. **Reconhecimento facial: entre a criminologia, a mídia e a LGPD penal.** Brasília: Universidade de Brasília, 2021. Disponível em: https://revista.internetlab.org.br/wp-content/uploads/2021/07/Reconhecimento-facial-entre-a-criminologia-a-midia-e-a-LGPD-penal.pdf. Acesso em: 3 ago 2025.

SARAIVA, Mariana. **Reconhecimento facial é um aliado da segurança pública do DF.** Brasília: Correio Braziliense, 2025. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2025/06/7159781-reconhecimento-facial-e-um-aliado-da-seguranca-publica-do-df.html. Acesso em: 4 ago 2025.

SERASA EXPERIAN. **Reconhecimento facial: transformação nas estratégias de prevenção à fraude.** 2024. Disponível em: https://www.serasaexperian.com.br/conteudos/reconhecimento-facial-transformacao-nas-estrategias-de-prevencao-a-fraude/. Acesso em: 4 ago 2025.

SILVA, Claudecir Freitas *et al*. **O uso do reconhecimento facial na segurança pública:** divergência entre o combate à criminalidade e o direito à privacidade. Revista Ft, 2024. Disponível em: https://revistaft.com.br/o-uso-do-

reconhecimento-facial-na-seguranca-publica-divergencia-entre-o-combate-a-criminalidade-e-o-direito-a-privacidade/. Acesso em: 4 ago 2025.

SILVA. Francilene. **Reconhecimento facial com tecnologia do CIASC auxilia na prisão de foragido durante a Festa do Pinhão.** Florianópolis: CIASC, 2025. Disponível em: https://www.ciasc.sc.gov.br/reconhecimento-facial-com-tecnologia-do-ciasc-auxilia-na-prisao-de-foragido-durante-a-festa-do-pinhao/.Acesso em: 4 ago 2025.

SOUZA, Marcos. **Aposta contra o crime, reconhecimento facial se espalha pelo país.** São Paulo: Valor Econômico, 2024. Disponível em: https://valor.globo.com/brasil/noticia/2024/03/19/aposta-contra-o-crime-reconhecimento-facial-se-espalha-pelo-pais.ghtml. Acesso em: 4 ago 2025.