

RECONHECIMENTO FACIAL NA INVESTIGAÇÃO CRIMINAL: LIMITES DA PROVA TECNOLÓGICA NO SISTEMA PENAL BRASILEIRO

FACIAL RECOGNITION IN CRIMINAL INVESTIGATIONS: LIMITS OF
TECHNOLOGICAL EVIDENCE IN THE BRAZILIAN CRIMINAL JUSTICE
SYSTEM

Ciências Sociais Aplicadas • 20/10/2026

REGISTRO DOI: [10.70773/revistatopicos/792342253](https://doi.org/10.70773/revistatopicos/792342253)

Mayara Santana Brandão Nolêto¹

Maíla Rocha Feitosa Herênio²

RESUMO

O reconhecimento facial tem ganhado crescente relevância no campo da segurança pública e da investigação criminal, sobretudo diante da incorporação de ferramentas de inteligência artificial aos procedimentos de identificação de indivíduos. O presente estudo analisa os limites da utilização do reconhecimento facial na investigação criminal e como prova tecnológica no sistema penal brasileiro, considerando sua compatibilidade com os direitos e garantias fundamentais. Do ponto de vista metodológico, realizou-se revisão de literatura, de abordagem qualitativa e caráter exploratório-descritivo, fundamentada em produções científicas e jurídicas relacionadas ao reconhecimento facial, à inteligência artificial, ao processo penal, à proteção de dados e aos vieses algorítmicos. Os resultados da análise demonstraram que, embora essa tecnologia possa contribuir para a eficiência das investigações, sua utilização apresenta desafios ligados à possibilidade de erros de identificação, à discriminação algorítmica, ao tratamento de dados biométricos e ao comprometimento de garantias processuais. Constatou-se, ainda, que os resultados produzidos por sistemas automatizados não devem ser utilizados isoladamente como fundamento para responsabilização criminal, sendo indispensável sua confrontação com outros elementos probatórios. Conclui-se que o reconhecimento facial pode atuar como instrumento auxiliar da investigação criminal, desde que submetido a critérios de confiabilidade, transparência, supervisão humana e controle jurídico, de modo a preservar a presunção de inocência, o contraditório, a ampla defesa e o devido processo legal.

Palavras-chave: reconhecimento facial; investigação criminal; prova tecnológica.

ABSTRACT

Facial recognition has gained increasing relevance in public security and criminal investigations, particularly with the incorporation of artificial intelligence tools into procedures for identifying individuals. This study analyzes the limits of using facial recognition in criminal investigations and as technological evidence within the Brazilian criminal justice system, considering its compatibility with fundamental rights and safeguards. Methodologically, a qualitative, exploratory-descriptive literature review was conducted, drawing on scientific and legal publications addressing facial recognition, artificial intelligence, criminal procedure, data protection, and algorithmic bias. The analysis indicated that although this technology may contribute to investigative efficiency, its use raises challenges involving possible identification errors, algorithmic discrimination, biometric data processing, and the impairment of procedural safeguards. It was also found that outputs produced by automated systems should not, on their own, serve as grounds for criminal liability; they must be assessed alongside other evidence. The study concludes that facial recognition may serve as an auxiliary tool in criminal investigations, provided it is subject to reliability and transparency requirements, human oversight, and legal scrutiny, thereby safeguarding the presumption of innocence, adversarial proceedings, the right to a full defense, and due process of law.

Keywords: criminal investigation; facial recognition; technological evidence.

1. INTRODUÇÃO

A intensificação do uso de tecnologias digitais tem reconfigurado as práticas de investigação criminal e a própria produção de elementos informativos e probatórios no âmbito da persecução penal. Dentre

essas inovações, ganha destaque o reconhecimento facial fundamentado em inteligência artificial, tecnologia voltada à identificação ou verificação de indivíduos a partir da análise automatizada de características biométricas extraídas de imagens e vídeos (Machado; Barros, 2024).

Sua adoção por órgãos de segurança pública costuma ser apresentada como mecanismo apto a ampliar a capacidade estatal de identificar suspeitos, localizar pessoas procuradas e processar registros oriundos de sistemas de videomonitoramento. Não obstante, a disseminação dessa tecnologia também levanta questionamentos jurídicos acerca de sua confiabilidade, da proteção aos direitos fundamentais e dos limites que devem balizar sua utilização no processo penal.

No cenário brasileiro, a inserção do reconhecimento facial nas políticas de segurança pública exige atenção redobrada, na medida em que se torna necessário compatibilizar a inovação tecnológica com as garantias constitucionais vigentes. A adoção de sistemas automatizados não pode ser avaliada apenas sob o prisma da eficiência operacional, uma vez que seus resultados são capazes de interferir diretamente na liberdade e na esfera de direitos dos sujeitos submetidos à persecução penal.

Nessa direção, Araújo, Cardoso e Paula (2021) analisam a necessidade de regulamentação do uso do reconhecimento facial na segurança pública nacional, enquanto Almeida (2022) evidencia as implicações decorrentes do emprego dessas tecnologias na esfera penal.

Um dos pontos centrais dessa discussão refere-se à possibilidade de erros na identificação dos indivíduos por meio de sistemas algorítmicos. Tais sistemas operam a partir de padrões estatísticos e de bancos de dados previamente estruturados, de modo que a qualidade, a representatividade e o tratamento desses dados exercem influência direta sobre os resultados obtidos.

Cani e Nunes (2022) associam essa problemática ao risco de erros judiciais originados do uso de algoritmos de reconhecimento facial. Nessa perspectiva, quando o resultado tecnológico passa a fundamentar abordagens policiais, investigações, prisões ou decisões processuais penais, revela-se imprescindível avaliar com rigor o grau de confiabilidade atribuível a esse elemento.

Nesse contexto, o problema de pesquisa consiste em examinar os limites jurídicos e probatórios que incidem sobre o uso do reconhecimento facial na investigação criminal, bem como sobre sua admissibilidade como meio de prova no processo penal brasileiro, tendo em vista os riscos de identificação equivocada, a presença de vieses algorítmicos e a possibilidade de violação de direitos e garantias fundamentais.

Este estudo analisa os limites da utilização do reconhecimento facial na investigação criminal e como prova tecnológica no sistema penal brasileiro, à luz de sua compatibilidade com os direitos e garantias fundamentais assegurados pelo ordenamento jurídico.

Especificamente, busca compreender a aplicação do reconhecimento facial no âmbito da segurança pública e da investigação criminal; identificar os principais riscos relacionados a erros de identificação e a vieses algorítmicos; examinar as

repercussões da tecnologia sobre princípios e garantias do processo penal; analisar aspectos vinculados à proteção dos dados biométricos; e discutir os limites necessários à utilização dos resultados produzidos pelos sistemas de reconhecimento facial como elementos informativos ou probatórios.

A relevância da pesquisa está demonstrada pela crescente adoção de ferramentas de inteligência artificial e reconhecimento biométrico pelos sistemas de segurança pública, bem como na necessidade de fixar parâmetros que impeçam o avanço tecnológico de resultar em redução das garantias individuais.

No que se refere aos procedimentos metodológicos, trata-se de pesquisa bibliográfica, de abordagem qualitativa e natureza exploratório-descritiva, baseada na análise da produção científica e jurídica sobre reconhecimento facial, inteligência artificial, prova tecnológica, investigação criminal, processo penal, proteção de dados, vieses algorítmicos e direitos fundamentais. O levantamento abrange artigos científicos, trabalhos acadêmicos, livros e outras publicações relacionadas ao tema, com prioridade para materiais que ofereçam sólida fundamentação teórica e jurídica à compreensão do problema.

A análise bibliográfica busca promover diálogo entre as diferentes perspectivas identificadas na literatura, em especial aquelas voltadas à aplicação do reconhecimento facial na segurança pública, aos riscos de erro e discriminação algorítmica, à proteção dos dados biométricos e às implicações processuais decorrentes da utilização dos resultados automatizados. A partir dessa revisão, pretende-se identificar convergências, divergências e lacunas presentes na

produção acadêmica, relacionando-as aos princípios e garantias que estruturam o sistema penal brasileiro.

2. RECONHECIMENTO FACIAL E SUA UTILIZAÇÃO NA INVESTIGAÇÃO CRIMINAL

O avanço das tecnologias digitais tem alterado de forma expressiva as estratégias adotadas pelo Estado na prevenção e na investigação de crimes. Nesse cenário, os sistemas de reconhecimento facial passaram a integrar ferramentas de monitoramento e identificação de indivíduos, sobretudo por meio de câmeras de segurança, bancos de imagens e mecanismos automatizados aptos a comparar características biométricas faciais. A incorporação dessas tecnologias às políticas de segurança pública configura uma das expressões contemporâneas do processo de digitalização das atividades estatais (Almeida, 2022).

O reconhecimento facial pode ser definido como tecnologia biométrica voltada à identificação ou verificação de indivíduos a partir da análise de características específicas da face humana. No campo da segurança pública, sua aplicação permite comparar imagens captadas por sistemas de videomonitoramento com registros já armazenados em bancos de dados. A tecnologia atua, assim, como instrumento auxiliar das autoridades responsáveis pela investigação, ampliando as possibilidades de localização de pessoas procuradas ou vinculadas a determinado fato investigado (Araújo; Cardoso; Paula, 2021).

Almeida (2022), ao examinar o emprego de tecnologias de reconhecimento facial para fins de persecução penal, destaca a relevância de discutir os efeitos decorrentes da incorporação desses

instrumentos à atividade estatal. O reconhecimento facial não deve ser entendido apenas como inovação voltada ao aumento da eficiência da segurança pública, na medida em que sua aplicação está diretamente relacionada ao exercício do poder punitivo estatal e pode gerar consequências relevantes sobre os direitos dos indivíduos.

Essa discussão ganha especial importância diante da expansão dos sistemas de monitoramento em espaços públicos. Silva, Franqueira e Hartmann (2021) examinam o emprego do reconhecimento facial voltado à segurança pública e sua regulação no contexto latino-americano, evidenciando a relevância de se estabelecerem parâmetros claros para o uso dessa tecnologia. A adoção de sistemas automatizados pelo Estado pressupõe a existência de mecanismos jurídicos capazes de delimitar suas finalidades e as formas legítimas de sua utilização.

No cenário brasileiro, o reconhecimento facial já se encontra incorporado a determinadas iniciativas de segurança pública. Andréa, Silva e Gundim (2022), ao investigarem a implementação dessa tecnologia como política pública a partir do caso do Metrô de São Paulo, demonstram de que modo tais sistemas podem ser inseridos em ambientes de grande circulação de pessoas. Esse exemplo evidencia tanto as possibilidades oferecidas pela tecnologia quanto a necessidade de avaliar criteriosamente seus impactos jurídicos e sociais.

A adoção do reconhecimento facial relaciona-se, portanto, diretamente com a busca por maior eficiência na identificação de indivíduos e na obtenção de informações ao longo dos procedimentos investigativos. Contudo, o emprego dessas

ferramentas não dispensa a atuação humana. Os resultados produzidos pelos sistemas devem ser compreendidos como elementos capazes de auxiliar a investigação, e não como conclusões absolutas acerca da identidade de determinada pessoa.

Araújo, Cardoso e Paula (2021) situam essa problemática no debate sobre a regulação do reconhecimento facial na segurança pública brasileira. A expansão de uma tecnologia apta a coletar, analisar e comparar dados biométricos exige a fixação de parâmetros que orientem sua utilização pelo poder público. Nesse sentido, a inovação tecnológica deve caminhar ao lado da construção de mecanismos de controle que permitam compatibilizar segurança pública, eficiência investigativa e proteção dos direitos fundamentais.

Dessa forma, a utilização do reconhecimento facial na investigação criminal deve ser analisada para além de seus potenciais benefícios operacionais. Sua inserção no sistema de justiça criminal demanda avaliação crítica quanto à confiabilidade, à transparência, ao controle e aos limites jurídicos aplicáveis, especialmente diante da possibilidade de que uma identificação produzida por algoritmo repercuta em procedimentos investigativos ou em medidas que afetem diretamente a liberdade do indivíduo.

2.1. Reconhecimento Facial Como Prova e as Garantias do Processo Penal

A utilização do reconhecimento facial adquire maior complexidade jurídica quando seus resultados extrapolam a função meramente investigativa e passam a integrar procedimentos relacionados à formação da prova. No processo penal, a produção e a valoração dos

elementos probatórios devem observar garantias voltadas a proteger o indivíduo contra arbitrariedades e a assegurar a legitimidade da atuação estatal. De acordo com Macedo (2024), torna-se necessário questionar em que medida uma identificação produzida por sistema automatizado pode ser considerada suficientemente confiável para subsidiar decisões no âmbito criminal.

A tecnologia de reconhecimento facial opera mediante comparações fundamentadas em dados e parâmetros previamente estabelecidos. Seu resultado, portanto, decorre de um procedimento tecnológico que pode não ser plenamente compreendido pelo investigado, pelos operadores jurídicos ou mesmo pelos agentes responsáveis pela utilização do sistema. Essa característica gera desafios relacionados à transparência e à possibilidade efetiva de questionamento dos procedimentos empregados até se chegar à identificação (Andréa; Silva; Gundim, 2022).

Machado e Barros (2024) associam diretamente o reconhecimento facial por inteligência artificial ao princípio da inocência, inserindo essa discussão no contexto dos processos penais brasileiro e comparado. Tal relação assume particular relevância porque a identificação algorítmica de uma pessoa não deve gerar presunção automática de participação em determinada prática criminosa. O resultado fornecido pelo sistema constitui produto de uma operação tecnológica e, justamente por isso, sua utilização deve ser submetida a análise crítica dentro do conjunto de elementos disponíveis na investigação ou no processo.

A presunção de inocência representa garantia essencial para impedir que suspeitas ou indícios sejam tratados como

comprovação antecipada de responsabilidade penal. Nessa direção, a utilização do reconhecimento facial deve ser acompanhada de cautela, de modo que a correspondência apontada pelo algoritmo não seja convertida automaticamente em certeza quanto à identidade ou à responsabilidade do indivíduo (Baptista; Martins; Ferreira, 2025).

A utilização de resultados automatizados apresenta desafios ao contraditório e à ampla defesa. Para que determinado elemento tecnológico possa ser adequadamente contestado, é indispensável compreender os procedimentos empregados em sua produção. Fatores como a origem das imagens analisadas, a qualidade do material, o banco de dados utilizado e as características do sistema podem se tornar decisivos na avaliação da confiabilidade do resultado.

Macedo (2024) trata do direito à revisão das decisões automatizadas de reconhecimento facial, aspecto que reforça a importância da supervisão humana sobre os resultados produzidos por algoritmos. Essa possibilidade de revisão ganha relevância particular no campo penal, no qual as decisões podem repercutir diretamente sobre direitos fundamentais. O emprego da inteligência artificial, portanto, não deve afastar a responsabilidade dos agentes humanos pela análise e pela validação das informações produzidas.

2.2. Erros de Identificação, Vieses Algorítmicos e Discriminação

Um dos principais problemas associados aos sistemas de reconhecimento facial reside na possibilidade de erros de identificação. Ainda que se costume atribuir aos recursos tecnológicos uma percepção de objetividade, os algoritmos não

estão necessariamente livres de limitações. Seu desempenho depende de diversos fatores, entre os quais se destacam a qualidade das imagens processadas, os bancos de dados utilizados e os critérios adotados no desenvolvimento e no funcionamento dos sistemas (Baptista; Martins; Ferreira, 2025).

No âmbito penal, eventuais falhas assumem gravidade especial, pois uma identificação incorreta pode direcionar a investigação para pessoa sem qualquer relação com o fato apurado. Cani e Nunes (2022) discutem os erros judiciais no contexto da vigilância digital e colocam em questão os algoritmos de reconhecimento facial. Essa problemática evidencia que a incorporação de novas tecnologias à persecução penal deve ser acompanhada de análise criteriosa dos riscos que tais instrumentos produzem.

Os erros vinculados ao reconhecimento facial relacionam-se, ainda, à discussão sobre vieses algorítmicos. Sistemas automatizados são desenvolvidos e treinados a partir de conjuntos de dados, de modo que a composição dessas bases pode interferir diretamente na capacidade do algoritmo de realizar comparações adequadas. A representatividade dos dados utilizados constitui, portanto, aspecto relevante para a avaliação da qualidade e dos impactos da tecnologia (Andréa; Silva; Gundim, 2022).

Nóbrega e Zaidan (2023) sustentam a necessidade de construção de um reconhecimento facial antidiscriminatório, ressaltando o imperativo de assegurar bancos de rostos diversos e de combater vieses. A perspectiva apresentada pelos autores demonstra que a diversidade das bases de dados não configura questão meramente técnica, mas possui também dimensão jurídica e social, sobretudo quando os sistemas são empregados por instituições estatais.

Porto e Rolim (2022), por sua vez, examinam especificamente o reconhecimento facial e o viés algorítmico de caráter racial. A discussão proposta pelos autores reforça a necessidade de considerar que desigualdades presentes no funcionamento dos algoritmos podem produzir efeitos discriminatórios quando aplicadas no contexto da segurança pública e da investigação criminal.

A problemática dos vieses torna-se particularmente sensível diante da possibilidade de que resultados tecnológicos sejam percebidos como neutros pelo simples fato de terem sido produzidos por sistemas computacionais (Marrafon; Schiebert, 2024). A automatização de uma análise não implica, necessariamente, ausência de falhas ou de desigualdades. Por essa razão, a utilização responsável do reconhecimento facial pressupõe que os resultados obtidos sejam passíveis de verificação e de questionamento.

Essa discussão também repercute sobre a legitimidade da prova tecnológica. Caso o sistema apresente limitações significativas em relação a determinados grupos populacionais, sua utilização desacompanhada de mecanismos adequados de controle pode comprometer a confiabilidade das identificações realizadas. Transparência, diversidade dos bancos de dados, avaliação periódica dos sistemas e supervisão humana constituem, assim, elementos essenciais para reduzir o risco de que a tecnologia contribua para identificações equivocadas ou para práticas discriminatórias.

2.3. Proteção de Dados, Regulação e Limites Jurídicos do Reconhecimento Facial

A utilização do reconhecimento facial também guarda relação direta com a proteção de dados pessoais, uma vez que o funcionamento desses sistemas pressupõe a coleta, o armazenamento e o tratamento de informações biométricas. Ao contrário de determinados dados pessoais passíveis de alteração, as características biométricas mantêm vínculo particularmente estreito com a identidade do indivíduo, circunstância que amplia a exigência de proteção jurídica sobre esse tipo de informação (Silva; Franqueira; Hartmann, 2021).

Marrafon e Schiebert (2024) examinam juridicamente a proteção dos dados obtidos por meio do reconhecimento facial, estabelecendo comparação entre o Regulamento Geral sobre a Proteção de Dados europeu e a Lei Geral de Proteção de Dados brasileira. A análise desenvolvida pelos autores demonstra que a utilização dessas tecnologias não pode ser dissociada das normas voltadas à proteção das informações pessoais, tampouco da necessidade de fixar limites claros para o seu tratamento.

No contexto da segurança pública, a questão ganha complexidade adicional em razão da finalidade estatal atribuída à coleta e à utilização das informações. O interesse público relacionado à prevenção e à repressão de crimes precisa ser compatibilizado com a preservação dos direitos individuais. Nesse sentido, a legitimidade da finalidade estatal não dispensa a discussão sobre proporcionalidade, segurança, transparência e controle no tratamento dos dados biométricos.

Araújo, Cardoso e Paula (2021) destacam a importância da regulação do uso do reconhecimento facial na segurança pública brasileira, evidenciando a necessidade de estrutura normativa apta a

acompanhar o desenvolvimento e a aplicação dessas tecnologias. A regulação assume relevância na medida em que a utilização de sistemas automatizados sem parâmetros suficientemente definidos pode gerar incertezas quanto a responsabilidades, formas de controle e limites aplicáveis ao tratamento das informações obtidas.

Silva, Franqueira e Hartmann (2021), ao tratarem do reconhecimento facial voltado à segurança pública e de sua regulação no contexto latino-americano, também situam a questão regulatória como componente central da discussão. O desenvolvimento tecnológico avança em ritmo acelerado, ao passo que a construção de respostas jurídicas costuma demandar processos mais demorados. Essa assimetria reforça a necessidade de análise contínua quanto à adequação das normas existentes diante das novas formas de vigilância e identificação automatizada.

A proteção de dados relaciona-se, ainda, à exigência de transparência quanto aos sistemas empregados. Para que se torne possível exercer controle jurídico sobre determinada identificação automatizada, é relevante conhecer aspectos ligados à origem dos dados, aos procedimentos de comparação adotados e às condições em que o resultado foi produzido. Essa transparência ganha importância adicional quando as informações obtidas passam a integrar investigação ou procedimento criminal.

A discussão regulatória, contudo, não se limita à proteção dos bancos de dados, alcançando também a definição dos limites de utilização dos resultados produzidos pelos sistemas. Macedo (2024), ao tratar do direito à revisão das decisões automatizadas de reconhecimento facial, contribui para a compreensão da importância da intervenção e do controle humano diante do

emprego de mecanismos automatizados capazes de repercutir sobre direitos individuais.

Diante disso, o estabelecimento de limites jurídicos ao reconhecimento facial deve considerar diferentes dimensões: a finalidade de utilização da tecnologia, a proteção das informações biométricas, a confiabilidade dos sistemas empregados, a prevenção de discriminações, a transparência dos procedimentos, a possibilidade de contestação dos resultados e a necessidade de supervisão humana. Tais elementos revelam-se essenciais para impedir que a inovação tecnológica seja utilizada de maneira incompatível com as garantias fundamentais.

3. CONCLUSÃO

O desenvolvimento deste estudo permitiu analisar a utilização do reconhecimento facial na investigação criminal, com atenção especial aos limites de sua aplicação como prova tecnológica no sistema penal brasileiro. A crescente incorporação de ferramentas de inteligência artificial às atividades de segurança pública demonstra que o avanço tecnológico pode contribuir para a identificação de indivíduos e para a obtenção de informações relevantes ao longo dos procedimentos investigativos.

Verificou-se, contudo, que a utilização dessas ferramentas deve estar condicionada a critérios jurídicos e técnicos rigorosos, uma vez que seus resultados são capazes de produzir consequências diretas sobre direitos fundamentais e sobre a liberdade das pessoas submetidas à persecução penal.

Em relação ao problema de pesquisa proposto, constatou-se que os limites jurídicos e probatórios aplicáveis ao reconhecimento facial

relacionam-se, sobretudo, à necessidade de assegurar confiabilidade, transparência, possibilidade de contestação e supervisão humana sobre os resultados produzidos pelos sistemas automatizados.

A identificação realizada por algoritmo não deve ser compreendida, isoladamente, como elemento suficiente para comprovar a participação de determinado indivíduo em prática criminosa. O reconhecimento facial deve, assim, assumir caráter auxiliar dentro da investigação, com seus resultados confrontados a outros elementos capazes de confirmar ou de afastar a hipótese inicialmente indicada pela tecnologia.

A análise evidenciou, ainda, que erros de identificação e vieses algorítmicos representam desafios relevantes à utilização do reconhecimento facial no sistema penal. A qualidade das imagens processadas, a composição dos bancos de dados e as características dos sistemas empregados podem interferir diretamente nos resultados obtidos.

Quando tais limitações não são devidamente consideradas, surge o risco de identificações equivocadas e de tratamento desigual entre diferentes grupos populacionais. A busca por maior eficiência investigativa, portanto, não pode justificar a utilização acrítica de tecnologias capazes de reproduzir desigualdades ou de provocar consequências injustas a indivíduos identificados de forma incorreta.

Outro aspecto identificado refere-se à necessidade de proteção dos dados biométricos empregados pelos sistemas de reconhecimento facial. A coleta, o armazenamento, o compartilhamento e o

tratamento dessas informações devem ocorrer de maneira compatível com a proteção da privacidade e dos direitos individuais.

Da mesma forma, a utilização de resultados automatizados no processo penal precisa respeitar garantias como a presunção de inocência, o contraditório, a ampla defesa e o devido processo legal. Revela-se fundamental, assim, estabelecer mecanismos que permitam conhecer, verificar e questionar os procedimentos tecnológicos empregados, de modo a impedir que a aparente objetividade dos sistemas automatizados substitua a análise jurídica e humana indispensável à adequada produção e valoração da prova.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. *Revista Brasileira de Segurança Pública*, São Paulo, v. 16, n. 2, p. 264-283, 2022. DOI: 10.31060/rbsp.2022.v16.n2.1377. Disponível em: [Revista Brasileira de Segurança Pública](#). Acesso em: 8 set. 2026.

ANDRÉA, Gianfranco Faggin Mastro; SILVA, Denis Cortiz da; GUNDIM, Wagner Wilson Deiró. Tecnologia de reconhecimento facial como política de segurança pública: o caso do Metrô de São Paulo. *Revista da Faculdade de Direito do Sul de Minas*, Pouso Alegre, v. 38, n. 2, p. 279-298, 2022. Disponível em: [Revista da Faculdade de Direito do Sul de Minas](#). Acesso em: 8 set. 2026.

ARAÚJO, Romulo de Aguiar; CARDOSO, Naiara Deperon; PAULA, Amanda Marcélia de. Regulação e uso do reconhecimento facial na segurança pública do Brasil. *Revista de Doutrina Jurídica*, Brasília, DF, v. 112, e021009, 2021. DOI: 10.22477/rdj.v112i00.734. Disponível em: [Revista de Doutrina Jurídica – TJDF](#). Acesso em: 8 set. 2026.

BAPTISTA, Bárbara Gomes Lupetti; MARTINS, Luciane Patrício Barbosa; FERREIRA, Marco Aurélio Gonçalves. *As problemáticas do reconhecimento facial como prova no processo penal: estudo do caso Luiz Justino e das modificações jurisprudenciais e legislativas posteriores*. 2025. Trabalho de Conclusão de Curso. Universidade Federal Fluminense, Niterói, 2025. Disponível em: [Portal eduCAPES/CAPES](#). Acesso em: 8 set. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 8 set. 2026.

CANI, Luiz Eduardo; NUNES, João Alcantara. Erros judiciais em tempos de *digital surveillance*: os algoritmos de reconhecimento facial em questão. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 8, n. 2, p. 679-712, maio/ago. 2022. DOI: 10.22197/rbdpp.v8i2.720. Disponível em: [SciELO Brasil](#). Acesso em: 8 set. 2026.

MACEDO, Caio Sperandeo de. O direito à revisão das decisões automatizadas de reconhecimento facial e o princípio antropocêntrico. *Revista de Direito Brasileira*, Florianópolis, v. 36, n. 13, p. 226-246, 2024. DOI: 10.26668/IndexLawJournals/2358-1352/2023.v36i13.8569. Disponível em: [Revista de Direito Brasileira](#). Acesso em: 8 set. 2026.

MACHADO, Gabriela Mendes; BARROS, Vinícius Diniz Monteiro de. Reconhecimento facial por inteligência artificial e princípio da inocência: investigações em torno dos processos penais brasileiro e comparado. *Revista EJEJF*, Belo Horizonte, v. 1, n. 1, 2024. DOI:

10.70982/rejef.v1i4.47. Disponível em: [Revista EJEJ – TJMG](#). Acesso em: 8 set. 2026.

MARRAFON, Marco Aurélio; SCHIEBERT, Ani Karini Muniz. Proteção de dados obtidos por reconhecimento facial: uma análise jurídica comparativa entre o Regulamento Geral sobre a Proteção de Dados (GDPR) europeu e a Lei Geral de Proteção de Dados (LGPD) brasileira. *Revista Direito & Paz*, v. 2, n. 51, 2024. Disponível em: [Revista Direito & Paz](#). Acesso em: 8 set. 2026.

NÓBREGA, Flavianne Fernanda Bitencourt; ZAIDAN, João Vitor Sales. Por um reconhecimento facial antidiscriminatório: o imperativo de assegurar bancos de rostos diversos e combater vieses. *Revista CNJ*, Brasília, DF, v. 7, n. 1, p. 139-150, 2023. DOI: 10.54829/revistacnj.v7i1.458. Disponível em: [Revista CNJ](#). Acesso em: 8 set. 2026.

PORTO, Victor Benigno; ROLIM, Emiliana Cavalcante. O reconhecimento facial e o viés algorítmico racista. *Brazilian Journal of Development*, Curitiba, v. 8, n. 5, p. 33349-33371, 2022. DOI: 10.34117/bjdv8n5-049. Disponível em: [Registro do artigo](#). Acesso em: 8 set. 2026.

SILVA, Lorena Abbas da; FRANQUEIRA, Bruna Diniz; HARTMANN, Ivar A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. *Revista Digital de Direito Administrativo*, Ribeirão Preto, v. 8, n. 1, p. 171-204, 2021. DOI: 10.11606/issn.2319-0558.v8i1p171-204. Disponível em: [Revista Digital de Direito Administrativo – USP](#). Acesso em: 8 set. 2026.

¹ Acadêmico do 9º período do curso de Direito - Faculdade de Educação Santa Terezinha - FEST. E-mail: [acesse o artigo original para visualizar o e-mail](#).

² Advogada. Professora. Bacharel em Direito pela Universidade Federal do Maranhão (UFMA). Licenciada em Filosofia (UniBF). Especialista em Direito Tributário (UniBF). Pós-graduanda em Direito Penal. E-mail: [acesse o artigo original para visualizar o e-mail](#).