RJI
REVISTA JURÍDICA IVAÍ
IVAÍ JOURNAL OF LAW
ISSN 2965-7075
UniFatecie, Paranavaí/PR, v. 4, n. 1, jan./jun. 2026

RECONHECIMENTO FACIAL COMO PROVA PENAL: ENTRE A EFICIÊNCIA TECNOLÓGICA E A FRAGILIDADE DOS STANDARDS PROBATÓRIOS

FACIAL RECOGNITION AS CRIMINAL EVIDENCE: BETWEEN TECHNOLOGICAL EFFICIENCY AND THE FRAGILITY OF EVIDENTIARY STANDARDS

Maria Fernanda Pires
Mestranda - UENP
Jacarezinho-Paraná-Brasil
https://orcid.org/0009-0002-9631-2828
http://lattes.cnpq.br/5005767614865196
wrtpires@gmail.com

RESUMO: O presente artigo analisa o uso da tecnologia de reconhecimento facial no âmbito da segurança pública brasileira, com o objetivo de compreender seu funcionamento e avaliar sua efetividade no combate à criminalidade. A pesquisa parte da premissa de que tais sistemas, embora apresentados como ferramentas neutras e eficientes, operam por meio de algoritmos de inteligência artificial que podem reproduzir vieses estruturais. Inicialmente, examina-se o funcionamento técnico do reconhecimento facial, destacando suas etapas de coleta, processamento e comparação de dados biométricos. Em seguida, investiga-se sua implementação no Brasil, evidenciando a expansão dessa tecnologia em projetos estatais e sua utilização no cumprimento de mandados de prisão. Diante desse cenário, busca-se analisar em que medida os resultados gerados por essa tecnologia podem ser admitidos como prova no processo penal, bem como se sua utilização observa os parâmetros exigidos pelos standards probatórios. A partir de uma abordagem qualitativa, de caráter exploratório e descritivo, com base em pesquisa bibliográfica e documental, utiliza-se o método dedutivo para examinar a compatibilidade dessa ferramenta com os direitos fundamentais, especialmente no que se refere à proteção de dados pessoais, à presunção de inocência e ao devido processo legal, à luz de referenciais teóricos como o garantismo penal de Luigi Ferrajoli e a teoria dos standards probatórios de Jordi Ferrer Beltrán. Conclui-se que, apesar de seu potencial tecnológico, o uso do reconhecimento facial no contexto brasileiro suscita relevantes preocupações quanto à transparência, à regulação e à possibilidade de reforço de discriminações. Verifica-se, ainda, que os elementos produzidos por essa tecnologia podem, no máximo, ser admitidos como indícios, apresentando limitada força probatória no processo penal, o que exige cautela em sua utilização e maior controle jurídico-institucional.
PALAVRAS-CHAVE: reconhecimento facial; prova penal; standarts.

ABSTRACT: This article analyzes the use of facial recognition technology in the context of Brazilian public security, aiming to understand its operation and evaluate its effectiveness in combating crime. The research starts from the premise that such systems, although presented as neutral and efficient tools, operate through artificial intelligence algorithms that can reproduce their structures. Initially, the technical functioning of facial recognition is examined, highlighting its stages of collection, processing, and comparison of biometric data. Then, its implementation in Brazil is investigated, highlighting the expansion of this technology in state projects and its use in the execution of arrest warrants. Given this scenario, the study seeks to analyze to what extent the results generated by this technology can be admitted as evidence in criminal proceedings, as well as whether its use complies with the requirements of evidentiary standards. From a qualitative, exploratory, and descriptive approach, based on bibliographic and documentary research, the deductive method is used to examine the compatibility of this tool with fundamental rights, especially regarding the protection of personal data, the presumption of innocence, and due process of law, in light of theoretical frameworks such as Luigi Ferrajoli's penal guarantees and Jordi Ferrer Beltrán's theory of evidentiary standards. It is concluded that, despite its technological potential, the use of facial recognition in the Brazilian context raises

relevant questions regarding transparency, regulation, and the possibility of reinforcing discrimination. It is also found that the elements produced by this technology can, at most, be admitted as compromises, presenting limited probative force in criminal proceedings, which requires caution in its use and greater legal-institutional control.
Keywords: facial recognition; criminal evidence; standards.

1 INTRODUÇÃO

O avanço da sociedade contemporânea tem promovido transformações significativas no campo da segurança pública e nas estratégias de combate à criminalidade, destacando-se, nesse contexto, a adoção de tecnologias de autenticação biométrica, especialmente o reconhecimento facial.

Tal ferramenta utiliza algoritmos de inteligência artificial e aprendizado de máquina para identificar e mapear pontos nodais da face humana, como o formato do nariz, dos olhos e da mandíbula, comparando-os com bancos de dados previamente existentes. Trata-se de uma técnica frequentemente apresentada como neutra e objetiva, voltada à efetivação de medidas como o cumprimento de mandados de prisão.

O presente artigo tem como objetivo analisar o funcionamento da tecnologia de reconhecimento facial, bem como problematizar sua efetividade no âmbito da segurança pública, investigando se sua utilização contribui, de fato, para a redução da criminalidade ou se, ao contrário, acaba por automatizar práticas decisórias marcadas por vieses estruturais.

Embora divulgada como uma inovação capaz de facilitar a identificação de indivíduos em diferentes ambientes, sua operacionalização revela elevada complexidade, envolvendo múltiplas etapas de processamento de dados e análise estatística, o que ultrapassa a simples captura de imagens. No cenário brasileiro, observa-se uma rápida expansão dessa tecnologia, com sua adoção por diversos estados e municípios em projetos que potencialmente monitoram milhões de cidadãos.

Entretanto, tal crescimento ocorre em um contexto de fragilidade regulatória e insuficiente transparência institucional, na medida em que muitos órgãos públicos não disponibilizam relatórios de impacto à proteção de dados pessoais. Nesse contexto, a discussão acerca da admissibilidade e do valor probatório dessas ferramentas torna-se ainda mais relevante, sobretudo quando confrontada com as garantias fundamentais do processo penal, conforme delineadas pelo garantismo penal de Luigi Ferrajoli e pela teoria dos standards probatórios desenvolvida por Jordi Ferrer Beltrán.

A presente pesquisa adota abordagem qualitativa, de caráter exploratório e descritivo, desenvolvida por meio de pesquisa bibliográfica e documental. Inicialmente, busca-se compreender o funcionamento técnico da tecnologia de reconhecimento facial, a partir da análise de literatura especializada, legislação e produções acadêmicas sobre inteligência artificial, proteção de dados e segurança pública. Em seguida, procede-se ao exame de dados, relatórios e informações públicas acerca da implementação e utilização dessa tecnologia no Brasil, com o objetivo de identificar seus impactos jurídicos e sociais.

Para tanto, utiliza-se o método dedutivo, partindo de premissas gerais relacionadas aos direitos fundamentais, à proteção de dados pessoais e às garantias do processo penal, conforme delineadas por autores como Luigi Ferrajoli e Ferrer Beltrán para a análise crítica de sua aplicação no contexto da segurança pública brasileira.

2 O RECONHECIMENTO FACIAL

Com o avanço da sociedade, diversas mudanças têm sido implementadas para facilitar a convivência social e ampliar a segurança dos indivíduos: não raro, observa-se, cada vez mais, a presença de câmeras de segurança nas ruas, portas com travas de metal e alarmes para detecção de objetos metálicos, medidas voltadas ao aumento da segurança coletiva.

Nesse contexto, destaca-se a autenticação por reconhecimento biométrico — tecnologia que identifica pessoas com base em características físicas, como impressões digitais, reconhecimento facial, voz, íris ou palma da mão (Rzemyk, 2017, p. 249-254): trata-se de uma forma de autenticação e segurança aplicável a dispositivos eletrônicos, aeroportos, caixas automáticos, entre outros ambientes.

Dentre essas modalidades, o reconhecimento facial merece destaque, pois consiste em uma técnica biométrica de identificação ou verificação de indivíduos a partir de características faciais — utilizando algoritmos avançados de inteligência artificial e aprendizado de máquina para analisar imagens e/ou vídeos, identificando padrões específicos do rosto humano (Marinho, 2025, p. 02-03).

O funcionamento ocorre em três estágios sequenciais: a captura de imagens por dispositivos óticos, processamento biométrico mediante mapeamento de pontos nodais faciais – como a distância entre os olhos, o formato do nariz e da mandíbula, criando um modelo

matemático único para cada indivíduo, e comparação com banco de dados preexistentes (Oliveira, 2025, p.10167).

Figura 1: Fluxo de Trabalho de Reconhecimento facial



Fonte: autoral;

Após a identificação de um rosto humano, inicia-se a etapa propriamente dita de reconhecimento. Nessa fase, algoritmos e softwares específicos do sistema são empregados para analisar e comparar o rosto detectado com os registros constantes em um banco de dados de imagens, que funciona como base operacional da ferramenta de identificação. O objetivo dessa etapa é estabelecer a identidade dos indivíduos capturados em imagens ou vídeos, por meio da comparação das características faciais.

> Essa caminhada histórica demonstra que a tecnologia de reconhecimento facial está diretamente vinculada a dois fatores técnicos primordiais: a capacidade de identificação de padrões de imagens em diferentes cenários ambientais; e ao banco de dados que alimenta o algoritmo de identificação que opera a ferramenta de identificação (Freitas; Souza; Nora, p.571. 2025).

Considerando essa forma de operação, é possível afirmar que os sistemas de reconhecimento facial adotados no cenário da segurança pública brasileira funcionam a partir de um processo composto por quatro fases que, embora distintas, atuam de maneira complementar.

A primeira dessas fases é caracterizada pela geração de imagens, realizada por meio do monitoramento ostensivo de locais estratégicos, com o objetivo de coletar dados visuais. Essa etapa, ainda que não diretamente vinculada a uma técnica específica de reconhecimento, é fundamental para a obtenção das imagens. Nesse sentido, pode-se afirmar que ela atua como uma fase de ativação do processo, pois insere os indivíduos no alcance da tecnologia e assegura que o sistema disponha dos insumos visuais necessários para o início da fase de identificação (Barbosa; Yamaguchi; Teodoro, p.73. 2025).

Produzidas as imagens, inicia-se a fase de detecção. Após essa identificação, segue-se a terceira etapa, a do reconhecimento, momento em que, uma vez identificado o rosto, o sistema gera uma representação numérica única, construída a partir da posição, do tamanho, do contorno e de outras características faciais (Barbosa; Yamaguchi; Teodoro, p.73. 2025).

Concluída essa etapa, tem início a quarta e última fase: a comparação. Nela, a representação numérica gerada anteriormente é confrontada com outras representações faciais constantes em um banco de dados, geralmente alimentado pelas forças policiais.

Embora o funcionamento da tecnologia de reconhecimento facial possa aparentar simplicidade, inovação e aplicabilidade imediata — razões pelas quais vem sendo adotada por governos estaduais como uma das principais ferramentas de combate à criminalidade, seu uso no Brasil é marcado por diversas preocupações e críticas. Essa resistência se manifesta de forma mais intensa entre entidades defensoras dos direitos humanos e organizações da sociedade civil.

Um elemento central da propagação dessas tecnologias é o risco. As câmeras são estruturadas por modelos algorítmicos (O'Neil, 2020, p. 19) para, a partir de comportamentos, identificar a existência de um risco ou, ainda, associar faces a bancos de suspeitos policiais. A opacidade de sua operacionalidade técnica levou estudiosos do tema a classificarem esses algoritmos como verdadeiras "caixas pretas" (Pasquale, 2015).

O Centro de Privacidade e Tecnologia da Georgetown Law, em estudo realizado em 2016, sustenta que o reconhecimento facial possui natureza inerentemente probabilística — isto é, não fornece respostas binárias, mas sim correspondências baseadas em graus de probabilidade. O referido estudo também destaca que determinadas características faciais funcionam como indicadores mais confiáveis de similaridade do que outras, razão pela qual muitos algoritmos são calibrados para atribuir maior peso a traços mais consistentes e discriminativos

Nesse contexto, conclui-se que a operação dessa tecnologia não é neutra, sendo influenciada por múltiplos fatores — tanto técnicos quanto ambientais, geográficos e sociais. Entre os fatores internos, destacam-se os bancos de dados utilizados no treinamento e na execução dos sistemas de identificação. Já entre os fatores externos, incluem-se o ambiente em que a tecnologia foi desenvolvida e testada, bem como os equipamentos empregados em sua utilização, todos com impacto direto em seu desempenho.

Ademais, um dos principais desafios relacionados ao uso desses algoritmos reside no fato de que eles são otimizados a partir dos dados com os quais são alimentados. Em outras palavras, sua capacidade de funcionamento está diretamente condicionada às informações previamente armazenadas, o que pode resultar na reprodução — e até no agravamento — de vieses existentes nesses próprios dados.

Portanto, conclui-se que a confiabilidade dessa tecnologia encontra limites em diversos fatores-chave, dentre os quais se destacam a qualidade das imagens capturadas, a precisão na extração das características faciais e a eficiência dos algoritmos empregados. Nesse sentido, a existência de uma base de dados robusta e bem estruturada revela-se fundamental, na medida em que possibilita maior acurácia na identificação dos indivíduos e reduz a margem de erro nos resultados obtidos.

3 APLICAÇÃO DO RECONHECIMENTO FACIAL NA LEGISLAÇÃO BRASILEIRA

No contexto da segurança pública brasileira, desde 2011, essa tecnologia vem ganhando terreno significativo, tanto em iniciativas do Governo Federal quanto, sobretudo, nas administrações estaduais, como nos Estados de São Paulo, Rio de Janeiro, Bahia, Ceará, Amazonas, Amapá, Paraná, Santa Catarina e no Distrito Federal (INSTITUTO IGARAPÉ, 2026).

Até janeiro de 2025, o Brasil registrava 364 projetos de reconhecimento facial em funcionamento no país, o que significa uma estimativa de mais de 82 milhões de pessoas potencialmente vigiadas pelo mecanismo biométrico (O Panóptico, 2025).

O projeto O Panóptico, que realiza o monitoramento das tecnologias de reconhecimento facial no Brasil, aponta que em 72,5 % dos casos as entidades não apresentaram informações sobre a elaboração de relatórios de impacto à proteção de dados pessoais (Lima et al, 2024). De acordo com a equipe de pesquisa, os projetos operam sem

atender os padrões mínimos de transparência ativa e passiva, o que fragiliza o controle social, abre espaços para abusos, desvios, usos desproporcionais e práticas discriminatórias.

Essa expansão ocorre em múltiplas frentes e em diferentes cenários, mas converge para objetivos comuns: (i) a melhoria dos processos de identificação e detenção de indivíduos suspeitos; (ii) a prevenção e o combate a atividades criminosas; e (iii) o aprimoramento do monitoramento e da segurança em espaços públicos.

Alguns defensores da tecnologia, como Dal Magro, destacam que a adoção do reconhecimento facial pelos estados brasileiros é promovida como estratégia relevante para aumentar a eficácia na prevenção e no combate ao crime, especialmente em regiões extensas, resultando em maior eficiência das ações de segurança pública. Entre os benefícios apontados, destaca-se o uso integrado com bases de dados governamentais e sistemas de monitoramento, permitindo a identificação ágil de pessoas de interesse — como indivíduos com mandados de prisão ou desaparecidos — sem a necessidade de ampliação do efetivo policial.

Considerando a ausência de uma definição precisa, no Brasil, acerca do modo e do contexto de utilização da tecnologia de reconhecimento facial, e tendo em vista que o artigo 144 da Constituição Federal estabelece a segurança pública como dever do Estado e responsabilidade de todos, além de recentes decisões do Supremo Tribunal Federal que ampliaram as competências dos municípios em matéria de segurança pública, diversas administrações municipais têm adotado esses sistemas. Esse cenário tem dificultado sobremaneira o mapeamento e a definição das formas de emprego dessa tecnologia pelos órgãos estatais.

No plano jurídico, a utilização do reconhecimento facial enfrenta desafios particularmente complexos no ordenamento brasileiro. Embora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabeleça princípios como finalidade, adequação e necessidade para o tratamento de dados biométricos (art. 6º), a ausência de regulamentação específica cria lacunas preocupantes, especialmente quando a tecnologia é empregada por órgãos de segurança pública. Como observa Hermes (2025, p. 09-12), a combinação entre sistemas imprecisos e estruturas institucionais com histórico de discriminação racial potencializa riscos à liberdade individual e à igualdade material.

No entanto, não se pode desconsiderar a questão da confiabilidade dessa tecnologia como meio de prova no processo penal. Nesse sentido, surgem: (i) incertezas quanto à precisão na identificação de suspeitos, o que compromete a confiabilidade da ferramenta —

aspecto crítico, já que erros podem gerar graves consequências para indivíduos erroneamente identificados; (ii) o viés algorítmico presente nos sistemas, frequentemente associado ao chamado racismo algorítmico, evidenciando uma possível discriminação estrutural que afeta desproporcionalmente determinados grupos raciais, especialmente a população negra; e (iii) o impacto sobre os direitos fundamentais, marcado por uma vigilância intensiva e contínua, que suscita preocupações relacionadas à privacidade e à liberdade individual.

Na Bahia, mais de 1.750 pessoas foram presas nos últimos seis anos a partir do reconhecimento facial, em geral em virtude de delitos de menor potencial ofensivo ou de natureza cível, como furtos e inadimplência de pensão alimentícia. Contudo, não são apresentados registros dos falsos positivos identificados nessas operações. Estudos apontam que a taxa de falso positivo dos equipamentos de reconhecimento facial pode alcançar aproximadamente 72% dos alertas

> A parte do corpo utilizada na biometria, seja a digital ou a face, nunca é analisada por completo. Isto quer dizer que são escolhidos alguns pontos do rosto ou do dedo e, com base nas distâncias entre esses pontos, é calculada a probabilidade de aquela digital ou de aquela face ser da pessoa cadastrada no banco de dados. No caso do rosto humano, as possibilidades de haver diferenças ou modificações nessas distâncias são bem maiores do que numa digital, já que uma pessoa envelhece e perde colágeno, pode estar bocejando, piscando etc (NUNES, 2019, p. 67-68).

Um exemplo disso é o caso do jovem negro Daniel Félix, o qual foi preso em abril de 2023 após ser indiciado em inquéritos no qual sua foto foi reconhecida equivocadamente como autor de um crime que não cometeu, sendo a terceira vez que teve que provar sua inocência perante o judiciário por fatos semelhantes (Brasil de Fato, 2023).

> O fato narrado demonstra a ocorrência de um resultado “falso positivo”. Isso ocorre quando o Reconhecimento Facial confunde o rosto analisado com outro rosto em sua base de dados, identificando erroneamente a pessoa em questão como outra. Tal ocorrência gera um constrangimento para a pessoa identificada pelo “falso positivo”, pois, identificada equivocadamente a pessoa pelo RF, o resultado é presumido como correto e um inocente é preso sem maiores questionamentos (Barbosa; Yamaguchi; Teodoro, p.77. 2025).

No caso, fica demonstrado que com o reconhecimento facial quando erra torna uma pessoa inocente culpada, negando-lhe a possibilidade de recorrer de imediato. Sua única

salvação é provar sua inocência perante a justiça, após a violação de sua liberdade fundamental (Barbosa; Yamaguchi; Teodoro, p.77.2025).

Com isso, observa-se que, no Brasil, há uma rápida expansão dessa tecnologia, porém sem a devida regulamentação legal e sem a definição de parâmetros claros por parte do Estado e dos municípios que a utilizam.

Conforme os dados apontam, é inegável que, em um primeiro momento, a tecnologia aparenta representar um grande avanço, contribuindo para a agilidade na identificação de indivíduos foragidos ou com mandado de prisão. Contudo, a legislação não deve se preocupar apenas com a celeridade, mas, sobretudo, com a efetividade e a segurança jurídica dessa política.

4 DIREITO PROBATÓRIO PENAL

No processo penal, por envolver relações jurídicas especialmente sensíveis, como a vida e a liberdade, é imprescindível que o legislador e o aplicador do Direito se preocupem em estabelecer critérios mais rigorosos para a admissibilidade das provas.

Nesse contexto, há doutrinadores que se dedicam ao estudo de parâmetros de aceitabilidade probatória, buscando delimitar quais elementos podem, legitimamente, fundamentar a formação da convicção judicial.

Posto que um dos principais desafios da prova penal reside na formação da convicção judicial, observa-se, por vezes, uma compreensão deturpada de que o objetivo do processo seria “convencer o juiz”, atribuindo-lhe, indevidamente, o papel de agente da justiça em sentido subjetivo. Contudo, a função do magistrado não é a de atuar como justiceiro, mas sim a de apreciar, de forma técnica e imparcial, o conjunto probatório produzido nos autos.

Nesse contexto, cabe ao juiz verificar se as provas apresentadas são suficientes para sustentar um decreto condenatório. Ausente tal suficiência, impõe-se a absolvição, em observância ao princípio do in dubio pro reo. Assim, o magistrado deve decidir com base no que lhe foi efetivamente apresentado, procedendo a uma análise criteriosa e fundamentada das provas, sem extrapolar os limites de sua função jurisdicional.

Infelizmente, em determinados casos, em razão da discricionariedade judicial, observa-se que o magistrado, antes mesmo de proceder à validação da prova, já se encontra imbuído de uma convicção prévia. A partir dessa certeza antecipada, passa a avaliar as

consequências da admissão ou não do elemento probatório, decidindo por aceitá-lo ou rejeitá-lo de modo a confirmar a verdade que previamente formou, em momento anterior ao regular desenvolvimento do processo penal.

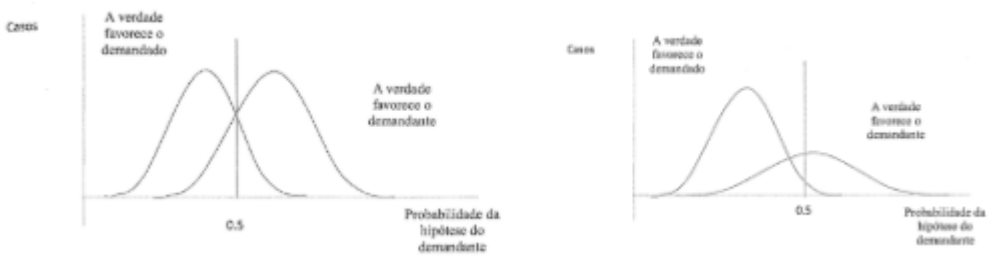
Na busca de uma suposta verdade absoluta, não aquela construída a partir do devido processo legal, mas sim a que melhor satisfaz suas próprias convicções e as expectativas sociais, corre-se o risco de afastamento dos parâmetros de imparcialidade e da verdade processualmente demonstrada.

> No entanto, a tentação de proclamar a obtenção de uma verdade absoluta no processo persiste [...] A abordagem inquisitória atual é fruto de uma epistemologia muito mais grave, autorreferente e monológica, que continua a moldar a mentalidade de muitos magistrados, conscientemente ou não [...] (Ferrajoli, p.183, 2025).

Diante disso, surgiu a figura dos standards probatórios, conforme sustenta Jordi Ferrer-Beltrán, em sua obra Prova sem Convicção, ao analisar as características centrais dos standards probatórios, são estabelecidas regras que determinam o nível de suficiência probatória necessário para que uma hipótese seja considerada provada (Beltrán, 2023, p. 131).

O autor observa que, embora alguns defendam a desnecessidade desses standards, também aponta falhas nas posições que os sustentam. Em especial, critica a utilização de critérios puramente probabilísticos para aferir a robustez da prova, argumentando que, no âmbito do processo penal, não é adequado adotar esse paradigma, ilustrando tal problemática por meio de representações gráficas.

Figura 2: Representações gráficas



Fonte: (Beltrán, p.213,2023).

Como demonstrado nos gráficos analisados pelo autor, a aplicação de um mesmo nível de standard probatório a um mesmo caso pode conduzir a resultados distintos. Isso ocorre porque a probabilidade pode, no máximo, auxiliar na construção de cenários acerca do fato delituoso, funcionando como ferramenta de apoio à compreensão do contexto.

Nesse contexto, embora o uso da tecnologia de reconhecimento facial possa contribuir para o aumento da probabilidade de identificação do acusado, sua adoção como verdade absoluta para fundamentar a convicção judicial não se revela confiável.

Isso se deve, sobretudo, às limitações técnicas e aos riscos de erro inerentes a esse tipo de ferramenta, bem como aos vieses presentes nos algoritmos que a sustentam. Tais sistemas ainda não foram plenamente aperfeiçoados a ponto de reduzir significativamente as margens de erro, especialmente no que se refere à diversidade de características faciais da população.

No âmbito da segurança pública, o modelo mais utilizado é o denominado reconhecimento "um para N", cujo objetivo consiste em comparar uma imagem com um amplo banco de dados, muitas vezes composto por milhões de fotografias, a fim de identificar determinado indivíduo.

Essa tecnologia baseia-se na análise de atributos faciais, como formato do rosto, nariz, olhos e queixo; por meio de algoritmos de aprendizado de máquina (machine learning), os quais permitem estabelecer uma probabilidade de correspondência entre a imagem capturada e os registros existentes (Universidade de São Paulo, 2024).

Conforme destaca o professor Fernando Osório, ainda que tais sistemas sejam considerados seguros, não oferecem certeza absoluta. Segundo o autor, "o reconhecimento feito por uma máquina não tem uma garantia de 100% de certeza", o que pode gerar problemas relevantes, sobretudo quando utilizado como fundamento para medidas gravosas, como a prisão. Nessa perspectiva, o reconhecimento facial não pode ser equiparado a prova suficiente para imputação penal, devendo ser corroborado por outros elementos probatórios, à semelhança do que ocorre com o retrato falado, que, isoladamente, não se mostra adequado para sustentar uma acusação (Universidade de São Paulo, 2024).

5 CONSIDERAÇÕES FINAIS

O reconhecimento facial, embora promovido como uma ferramenta inovadora para a segurança pública e autenticação biométrica, apresenta limitações técnicas significativas que impedem sua aceitação como prova absoluta.

O sistema opera de forma inerentemente probabilística, utilizando algoritmos de inteligência artificial que comparam padrões faciais com bancos de dados, mas sem oferecer uma garantia. Essa natureza de "caixa preta" e a dependência da qualidade das imagens e dos dados de treinamento tornam a tecnologia vulnerável a erros, funcionando mais como um auxílio na construção de cenários de probabilidade do que como uma identificação definitiva e inquestionável.

No cenário brasileiro, a expansão acelerada dessa tecnologia ocorre em um contexto de baixa regulamentação e falta de transparência, o que potencializa riscos aos direitos fundamentais. A ausência de relatórios de impacto e de parâmetros claros para o uso policial favorece a reprodução de vieses. Casos documentados de "falsos positivos", que podem alcançar taxas alarmantes de até 72%, demonstram que a confiança cega no sistema pode levar à prisão injusta de inocentes, violando a liberdade individual antes mesmo de qualquer possibilidade de defesa.

Diante disso, é fundamental que o reconhecimento facial seja tratado no processo penal apenas como um elemento informativo que deve ser corroborado por outras provas, de forma semelhante ao que ocorre com o retrato falado.

O Poder Judiciário deve aplicar standards probatórios rigorosos para evitar que a convicção do magistrado seja baseada em certezas tecnológicas ilusórias ou em preconceitos prévios.

6 REFERÊNCIAS

BARBOSA, Bibiana Paschoalino; YAMAGUCHI, Anderson Akira; TEODORO, Ruan Ricardo Bernardo. Reconhecimento facial e a violação de direitos fundamentais: discriminação algorítmica, vigilância em massa e a necessidade de regulação no Brasil. In: ENCONTRO NACIONAL DO CONPEDI, 2025. Direito, Governança e Novas Tecnologias II. CONPEDI, 2025.

CASTRO, Bruna Azevedo de; ARGUELLO, Katie Silene Cáceres; COSATE, Tatiana Moraes. Capitalismo de vigilância e racismo: o reconhecimento facial automatizado como técnica de controle sobre o corpo negro. Revista Jurídica Direito & Paz, São Paulo/Lorena, ano XVI, n. 47, p. 79–101, 2º sem. 2022.

FERRER BELTRÁN, Jordi. Prova sem convicção: standards de prova e devido processo. Tradução de Vitor de Paula Ramos. 2. Ed. Rev. Atual. E ampl. São Paulo: Editora juspodivm, 2023.

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento fácil e policiamento no Brasil, p. 67 – 70. In: Retratos da Violência: cinco meses de monitoramento, análises e descobertas. Jun. – Out., 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em 02 maio 2026.

PINHO, Ana Cláudia. Apresentação. In: ABELLÁN, Marina Gascón; MATIDA, Janaina (org.). Ferrajoli e a prova. Tradução de Ana Cláudia Pinho (coord.) Et al. 1. Ed. São Paulo: Marcial Pons, 2025. P. 5-8. (Coleção Devido Processo).
Redação. RJ: Jovem negro acusado por reconhecimento facial é inocentado pela terceira vez. Brasil de Fato. 2023. Disponível em: https://www.brasildefato.com.br/2023/10/06/rj-jovem negro-acusado-por-reconhecimento-facial-e-inocentado-pela-terceira-vez. Acesso em: 20 mar. 2026.

RZEMYK, Thomas J. Biometrics in the Criminal Justice System and Society Today. In: FENNELLY, Lawrence J (Edit.). Effective Physical Security. 2ªed. Oxford: Butterworth Heinemann, 2017, p. 249-254. DOI: https://doi.org/10.1016/B978-0-12-804462-9.00010-5. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/B9780128044629000105. Acesso em: 02 abr. 2026.

SCHNEIDER, C. B.; MIRANDA, P. F. M. Vigilância Digital como instrumento de promoção da segurança pública. Publicatio UEPG – Ciências Sociais Aplicadas, Ponta Grossa/RS, v. 28, p. 1-14, 2020. Disponível https://revistas.uepg.br/index.php/sociais/article/view/14435. Acesso em: 31 mar. 2026.

Secretaria de Segurança Pública da Bahia. Reconhecimento Facial da SSP alcança 3 mil foragidos da Justiça na Bahia. Secretaria de Segurança Pública da Bahia. 2025. Disponível em: https://ssp.ba.gov.br/2025/04/04/reconhecimento-facial-da-ssp-alcanca-3-mil-foragidos da-justica-na-bahia/. Acesso em: 04 abr. 2026.

SELINGER, Evan; LEONG, Brenda. The ethics of facial recognition technology, in The Oxford Handbook of Digital Ethics ed. Carissa Véliz. Oxford Handbooks, 2021. Disponível em: https://doi.org/10.1093/oxfordhb/9780198857815.013.32. Acesso em: 25 mar. 2026.

SILVA, Tarcízio. Racismo algorítmico: inteligência artificial e discriminação nas redes digitais. Edições Sesc SP, 2022.

UNIVERSIDADE DE SÃO PAULO. Avanços e desafios da implantação da tecnologia de reconhecimento facial. São Carlos: Portal USP, 12 nov. 2024. Disponível em: https://saocarlos.usp.br/avancos-e-desafios-da-implantacao-da-tecnologia-de-reconhecimento-facial/ . Acesso em: 25 abr. 2026.

VÉLIZ, Carissa. Privacidade é poder. Editora Contracorrente, 2021.

ZMOGINSKI, Felipe. A sociedade mais vigiada do mundo: como a China usa o reconhecimento facial. Uol. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/01/19/a-sociedade-mais-vigiada-do mundo-como-a-china-usa-o-reconhecimento-facial.htm?cmpid=copiaecola. Acesso em: 22 mar. 2026.

ZUBOFF, Shoshana. The age of surveillance capitalism. The Fight for a Human Future at the New Frontier of Power. Public Affairs: New York. 2019.