O IMPACTO JURÍDICO DOS ERROS DE RECONHECIMENTO FACIAL EM SISTEMAS DE JUSTIÇA: QUANDO A INTELIGÊNCIA ARTIFICIAL ERRA NA IDENTIFICAÇÃO DE SUSPEITOS

Bruno José Meireles Almeida[1]
Luciano Almeida Gomes[2]
Antonio Fernandes Neves Junior[3]
Camila de Mattos Lima Andrade[4]

RESUMO

Este artigo tem como objetivo analisar os impactos jurídicos decorrentes dos erros produzidos por sistemas de reconhecimento facial na identificação de suspeitos no sistema de justiça criminal brasileiro, considerando as implicações sobre garantias constitucionais, seletividade penal e responsabilidade estatal. A metodologia consistiu uma abordagem qualitativa, estruturada por meio de análise documental, estudo de caso e revisão bibliográfica., realizada em bases nacionais e internacionais e critérios de inclusão que abarcaram estudos revisados por pares, documentos oficiais e pesquisas que abordassem vieses algorítmicos, discriminação, direitos fundamentais e uso de tecnologias de vigilância entre 2021 a 2025. Os resultados evidenciaram que o reconhecimento facial opera com taxas elevadas de erro, especialmente na identificação de pessoas negras e mulheres, devido a bases de dados desbalanceadas, ausência de auditoria, opacidade algorítmica e replicação de padrões discriminatórios historicamente presentes no sistema penal. Demonstrou-se que essas falhas geram prisões injustas, constrangimentos ilegais, estigmatização social e violações diretas à presunção de inocência, ao devido processo legal, à igualdade e à dignidade humana. Constatou-se também que a falta de regulamentação específica no Brasil amplia a insegurança jurídica e dificulta o controle institucional e social sobre o uso da tecnologia. Conclui-se que, em sua configuração atual, o reconhecimento facial não apresenta condições técnicas ou jurídicas para ser utilizado como instrumento autônomo de persecução penal, sendo necessária a criação de marcos regulatórios robustos que assegurem transparência, avaliação de impacto, limites de uso e responsabilização estatal, de modo a garantir conformidade com os princípios constitucionais e evitar o aprofundamento de desigualdades estruturais.

Palavras-chave: Inteligência Artificial; Reconhecimento Facial; Discriminação Social; Direitos Humanos; Responsabilidade Legal.

ABSTRACT

[1] Graduando em Direito pela Faculdade de Excelência - UNEX de Jequié, email:bjmeireles8@gmail.com
[2] Graduando em Direito pela Faculdade de Excelência - UNEX de Jequié, email:lucianoalmeidagomes03@gmail,com
[3] Orientador do Curso de Direito pela Faculdade de Excelência - UNEX de Jequié, email:afneves.jeq@ftc.edu.br
[4] Co-Orientadora e docente do Curso de Direito pela Faculdade de Excelência - UNEX de Jequié, email: candrade.jeq@ftc.edu.br

This article aims to analyze the legal impacts resulting from errors produced by facial recognition systems in the identification of suspects within the Brazilian criminal justice system, considering their implications for constitutional guarantees, penal selectivity, and state liability. The methodology employed a qualitative approach structured through documentary analysis, a case study, and a literature review, conducted using national and international databases. The inclusion criteria encompassed peer-reviewed studies, official documents, and research addressing algorithmic bias, discrimination, fundamental rights, and the use of surveillance technologies between 2021 and 2025.The results showed that facial recognition operates with high error rates, especially when identifying Black individuals and women, due to unbalanced datasets, lack of auditing, algorithmic opacity, and the replication of discriminatory patterns historically present in the penal system. These failures lead to wrongful arrests, unlawful constraints, social stigmatization, and direct violations of the presumption of innocence, due process, equality, and human dignity. It was also found that the absence of specific regulation in Brazil increases legal uncertainty and hinders institutional and social control over the use of the technology. It is concluded that, in its current configuration, facial recognition does not present technical or legal conditions to be used as an autonomous investigative tool, requiring the creation of robust regulatory frameworks that ensure transparency, impact assessment, usage limits, and State accountability, in order to guarantee compliance with constitutional principles and prevent the deepening of structural inequalities.

Keywords: Artificial Intelligence; Facial Recognition; Social Discrimination; Human Rights; Liability, Legal.

1. INTRODUÇÃO

O reconhecimento facial, enquanto tecnologia baseada em inteligência artificial, consiste no processamento automatizado de características biométricas para identificar indivíduos por meio de bancos de dados digitais (Negri, 2023). Sua adoção crescente pelo sistema de justiça criminal brasileiro tem sido apresentada como instrumento de modernização e eficiência. No entanto, essa implementação não pode ser compreendida sem reconhecer a herança histórica que estrutura a construção do “suspeito” no país, especialmente no que diz respeito à racialização do crime. Desde o século XIX, autores como Cesare Lombroso contribuíram para consolidar a noção de um “homem delinquente” biologicamente determinado, frequentemente descrito por traços associados às populações negras, consideradas inferiores na escala evolutiva (Lombroso, 1876; Costa, 2023). No Brasil, essas

concepções foram aprofundadas por Nina Rodrigues (1957), médico-legista maranhense que defendia que negros e mestiços possuíam menor capacidade de adaptação civilizatória e maior propensão criminógena, formulando uma criminologia racial que justificava tratamentos penais distintos e reforçava a ideia do homem negro como figura naturalmente suspeita (Rodrigues 1957; Costa, 2023). Essa matriz teórica pseudocientífica estruturou práticas estatais e imaginários sociais que atravessaram séculos e permanecem atuantes nas formas contemporâneas de vigilância.

Na atualidade, pesquisas demonstram que sistemas de reconhecimento facial replicam e ampliam essa lógica discriminatória ao apresentar índices elevados de erro na identificação de pessoas negras. A Defensoria Pública do Rio de Janeiro revelou que mais de 80% das prisões injustas por reconhecimento equivocado no país recaem sobre pessoas negras, evidenciando que os algoritmos apenas traduzem, em linguagem matemática, estereótipos raciais historicamente construídos (Negri; Winter, 2023).

Os impactos dessa tecnologia se materializam em casos concretos amplamente divulgados pela imprensa. Um dos mais emblemáticos ocorreu com uma dentista baiana, presa injustamente em Salvador após ser identificada como autora de um assalto, embora estivesse trabalhando no momento do crime. Situação semelhante ocorreu com um jovem negro no Rio de Janeiro, detido ao sair do trabalho devido a uma falsa correspondência gerada pelo sistema. Em outro episódio, um homem permaneceu preso por 37 dias após a tecnologia associar uma foto 3×4 antiga ao rosto captado por câmeras de segurança, demonstrando falhas técnicas graves e ausência de auditoria humana (Guimarães, 2021). Esses casos revelam que o problema não é isolado, mas estrutural.

Além disso, estudos internacionais reforçam as limitações da tecnologia: Buolamwini e Gebru (2018) demonstraram taxas de erro superiores a 34% na identificação de mulheres negras, contrastando com menos de 1% entre homens brancos, evidenciando vieses demográficos profundos. No Brasil, tais falhas são agravadas pela ausência de regulamentação específica, pela precariedade dos bancos de dados, pela opacidade algorítmica e pela tendência de que operadores do direito atribuam às decisões automatizadas um caráter de autoridade técnica. O

Superior Tribunal de Justiça, no julgamento do HC 598.886/SC (2020), reconheceu que o reconhecimento fotográfico é prova frágil e suscetível a estereótipos raciais, sendo ainda mais arriscado quando automatizado por algoritmos não auditáveis.

As consequências desses erros se propagam em três dimensões: penal, civil e administrativa. Na esfera penal, a utilização da tecnologia como fundamento para prisões e medidas restritivas viola princípios essenciais, como a presunção de inocência, o devido processo legal e a proporcionalidade. Na esfera civil, os danos decorrentes de prisões injustas, como perda de emprego, abalo moral, estigmatização e privação indevida de liberdade configuram responsabilidade objetiva do Estado, conforme o art. 37, §6º da Constituição Federal, impondo dever de indenizar quando falhas algorítmicas ou omissões estatais geram prejuízos. Já na responsabilidade administrativa, a ausência de auditoria, de governança algorítmica, recairá sobre o agente público que autorizou, supervisionou ou deixou de monitorar o sistema, conforme o art. 116, I, da Lei 8.112/90, instaurando-se sindicância ou processo disciplinar para apurar fatos, garantir defesa, aplicar sanções e corrigir falhas institucionais, de modo a assegurar adequada responsabilização administrativa.

Assim, a presente pesquisa pretende contribuir para o debate jurídico ao demonstrar que, em sua configuração atual, o reconhecimento facial não apresenta condições técnicas ou normativas para ser utilizado como instrumento autônomo de persecução penal, exigindo regulamentação robusta, mecanismos de auditoria contínua e limites claros de uso a fim de garantir sua compatibilidade com os princípios constitucionais e com a proteção dos direitos fundamentais.

Diante desse cenário, justifica-se a necessidade de analisar os impactos jurídicos decorrentes dos erros de reconhecimento facial, considerando a interseção entre vieses algorítmicos, discriminação racial e responsabilização estatal. O objetivo geral deste estudo é examinar criticamente como a aplicação dessa tecnologia no processo penal brasileiro tem violado garantias fundamentais. Como objetivos específicos, busca-se compreender os fatores técnicos e sociais que contribuem para esses erros; analisar as repercussões penais, civis e administrativas; avaliar a responsabilidade do Estado diante de prisões injustas; e

investigar a suficiência das propostas legislativas em debate, como o Anteprojeto da LGPD Penal e o Marco Legal da Inteligência Artificial.

2. METODOLOGIA

A presente pesquisa adota uma abordagem qualitativa, estruturada por meio de análise documental, estudo de caso e revisão bibliográfica. A análise documental foi realizada a partir de decisões judiciais, relatórios institucionais, normas jurídicas, boletins informativos e materiais produzidos por órgãos oficiais e entidades de direitos humanos, permitindo identificar e interpretar registros formais relacionados aos erros de reconhecimento facial. O estudo de caso concentrou-se em episódios reais de prisões indevidas no Brasil, possibilitando compreender, em profundidade, as repercussões jurídicas e sociais decorrentes da utilização equivocada dessa tecnologia. Complementarmente, desenvolveu-se uma revisão bibliográfica narrativa envolvendo livros, artigos científicos, dissertações e produções acadêmicas pertinentes ao tema, visando contextualizar o fenômeno, identificar discussões teóricas e ampliar a compreensão crítica sobre o impacto do reconhecimento facial no sistema de justiça criminal. A triangulação desses três procedimentos metodológicos contribuiu para uma análise robusta, integrando fundamentos teóricos, evidências empíricas e documentos oficiais.

Foram utilizados apenas descritores essenciais e diretamente relacionados ao tema, a saber: “Inteligência Artificial”, “Reconhecimento Facial”, “Erros de Identificação” e “Discriminação Algorítmica”, além de suas correspondentes em inglês. Na etapa inicial da busca, foram identificados 456 artigos na base SciELO, 61.200 artigos no Google Acadêmico e 7.176 artigos no Portal CAPES.

Os critérios de inclusão englobaram: (a) artigos publicados em periódicos científicos revisados por pares; (b) estudos que analisassem aspectos jurídicos, tecnológicos ou sociais do reconhecimento facial; (c) pesquisas que discutissem erros de identificação, vieses algorítmicos ou impactos sobre direitos fundamentais; (d) documentos oficiais e pareceres relevantes sobre a regulamentação da inteligência artificial e segurança pública; e (e) produções que apresentassem dados

empíricos sobre prisões injustas decorrentes de reconhecimento facial. Foram também incluídos artigos de revisão, estudos comparativos internacionais, casos paradigmáticos e jurisprudências que abordassem a temática.

Foram excluídos materiais que: Não apresentassem rigor metodológico; tratassem apenas de aspectos técnicos de software sem interface jurídica; estivessem duplicados nas bases; não disponibilizassem texto integral; ou abordassem tecnologias biométricas distintas do reconhecimento facial sem relação direta com seu uso no processo penal.

Quanto ao idioma, foram considerados trabalhos publicados em português, inglês e espanhol, permitindo maior abrangência e acesso às discussões internacionais sobre vieses algorítmicos e riscos jurídicos da IA. O período temporal adotado para seleção das publicações compreendeu os anos de 2021 a 2025, intervalo definido em razão da consolidação das tecnologias de reconhecimento facial, expansão do machine learning e do surgimento de debates contemporâneos sobre inteligência artificial, privacidade, responsabilização estatal e discriminação algorítmica. Após a aplicação dos critérios de inclusão e exclusão, 30 estudos foram selecionados para leitura completa, resultando na incorporação final de 7 artigos científicos que compuseram o corpus da análise documental.

3. RESULTADOS E DISCUSSÃO

A partir da aplicação dos critérios de busca, filtragem e seleção previamente descritos na metodologia, foram identificados os estudos que compõem o corpus final da análise documental. Para garantir maior clareza e organização dos dados, os artigos selecionados foram sistematizados em uma tabela contendo informações essenciais sobre cada publicação, como autores, tipo de estudo, objetivos, principais resultados e conclusões. Essa sistematização permite visualizar de forma comparativa as evidências encontradas, facilitando a análise crítica e a identificação de convergências, limitações e contribuições relevantes para a compreensão dos impactos jurídicos dos erros de reconhecimento facial no processo penal brasileiro.

Quadro 1 – Distribuição da produção científica

Autor(es)/ Ano	Tipo de Estudo	Objetivos	Principais Resultados	Conclusões
Negri e Winter, 2023	Revisão teórica e análise crítica	Analisar falhas da regulamentação da IA e impactos da discriminação algorítmica no reconhecimento facial.	Identificaram que sistemas de reconhecimento facial apresentam erros elevados contra pessoas negras e ausência de controles regulatórios.	A tecnologia reforça a seletividade penal e viola garantias fundamentais sem estrutura regulatória adequada.
Buolamwini e Gebru, 2018	Estudo experimental empírico	Avaliar precisão de sistemas de reconhecimento facial em diferentes recortes de raça e gênero.	Encontraram taxas de erro superiores a 34% em mulheres negras e inferiores a 1% em homens brancos.	Concluíram que o reconhecimento facial é enviesado e racialmente discriminatório.
Leardini, 2021	Estudo jurídico-tecnológico	Investigar implicações jurídicas da vigilância inteligente e da proteção de dados no uso de reconhecimento facial.	Identificou problemas técnicos como baixa qualidade de imagens, falta de padronização e riscos à privacidade.	A tecnologia não deve ser usada como prova única e exige regulamentação para evitar abusos.
Biondi & Cernev, 2023	Revisão crítica e análise regulatória	Avaliar impactos regulatórios da IA e a ausência de governança no Brasil.	Demonstraram falta de auditoria, transparência e critérios técnicos nos sistemas utilizados pela segurança pública.	A ausência de governança amplia erros estruturais e viola princípios da legalidade e eficiência.
Porto & Rolim, 2022	Estudo analítico sobre seletividade penal	Examinar efeitos sociais e penais do reconhecimento facial no Brasil.	Revelaram que a tecnologia amplia seletividade racial e produz prisões injustas.	Concluíram que o uso atual viola presunção de inocência e reforça o racismo estrutural.

Araujo, Zullo e Torres, 2020	Estudo jurídico-social	Discutir desafios jurídicos, sociais e tecnológicos do reconhecimento facial.	Mostraram que a tecnologia é usada sem controle, estimulando abordagens sem critérios e práticas discriminatórias.	Defendem criação urgente de marcos regulatórios e limites estritos de uso.
Guimarães, 2021	Estudo de casos	Analisar prisões injustas causadas por erros de reconhecimento facial no Brasil.	Casos de pessoas presas por fotos antigas, erros sistemáticos e ausência de auditoria.	O uso da tecnologia causa danos reais, irreversíveis e evidencia falhas graves.

3.1 Erros de Reconhecimento Facial e Seus Impactos na Identificação de Suspeitos

Os resultados obtidos a partir da análise dos estudos indicam que o reconhecimento facial, quando utilizado para identificar suspeitos no sistema de justiça criminal, apresenta um índice significativo de falhas, especialmente nas populações racialmente vulnerabilizadas. Segundo dados apresentados por Negri e Winter (2023), tais erros decorrem da insuficiência de diversidade nos bancos de dados utilizados para treinar algoritmos, que acabam por gerar correspondências equivocadas e conduzir a prisões injustas. O problema se intensifica em contextos nos quais a tecnologia é tratada como infalível, apesar das evidências científicas demonstrarem suas limitações técnicas e discriminatórias.

De acordo com Leardini (2021), a precisão dos algoritmos pode variar drasticamente conforme a qualidade das imagens, o ambiente de captação e as condições faciais dos indivíduos. Isso significa que fatores como iluminação, ângulo de câmera, envelhecimento e até elementos como barba ou maquiagem interferem no resultado, produzindo identificações equivocadas. O autor ressalta que, justamente por tais limitações, o reconhecimento facial não pode ser utilizado como prova única, sob pena de violar o devido processo legal.

Casos concretos relatados pela imprensa reforçam a gravidade dos erros. No Brasil, conforme relatado por Guimarães (2021), diversos cidadãos foram presos

devido a falhas em sistemas de reconhecimento facial, incluindo casos nos quais fotos antigas de documentos, como RGs desatualizados, foram equivocadamente associadas a autores de crimes. Em um dos episódios analisados, um homem permaneceu preso por 37 dias em razão de uma foto 3×4 antiga vinculada à base de dados policial. Esses casos demonstram que a tecnologia, sem controle e auditoria eficaz, agrava desigualdades.

Os estudos também revelam que, além da imprecisão técnica, existe grande falta de padronização procedimental no uso da ferramenta. Segundo Biondi e Cernev (2023), muitos sistemas utilizados pelos órgãos de segurança pública não passam por avaliação de impacto ou verificação de qualidade, o que torna o uso ainda mais arriscado. Esses autores alertam que a adoção indiscriminada da tecnologia pode gerar um cenário de insegurança jurídica, especialmente em países como o Brasil, que não possuem uma regulamentação robusta.

O Superior Tribunal de Justiça, no julgamento do HC 598.886/SC, reconheceu que o reconhecimento fotográfico tecnologia considerada precursora do reconhecimento facial automatizado é uma prova frágil, sujeita a indução por vieses raciais e falhas cognitivas humanas (STJ, 2020). Essa constatação, integrada às evidências científicas sobre falhas algorítmicas, demonstra que a automatização não corrige erros já conhecidos, mas os amplia em escala preocupante.

Esse entendimento jurisprudencial se torna ainda mais evidente quando analisamos o teor literal do acórdão. No HC 598.886/SC, o ministro Rogério Schietti afirmou expressamente que: “*O reconhecimento de pessoa, presencialmente ou por fotografia, realizado na fase do inquérito policial, apenas é apto para identificar o réu e fixar a autoria delitiva quando observadas as formalidades previstas no art. 226 do Código de Processo Penal e quando corroborado por outras provas colhidas na fase judicial, sob o crivo do contraditório e da ampla defesa*” (STJ, HC 598.886/SC, 2020). O acórdão também advertiu que “*o reconhecimento por meio fotográfico é ainda mais problemático, máxime quando se realiza por simples exibição de fotos previamente selecionadas pela autoridade policial*”, esclarecendo que essa prática pode induzir a erros graves de identificação e reforçar estereótipos. A inserção desse entendimento demonstra que, se até o reconhecimento humano é considerado frágil e insuficiente quando não observadas as garantias legais, a

versão automatizada que herda e amplia vulnerabilidades cognitivas, raciais e procedimentais apresenta risco ainda maior de produzir falsos positivos e violações de direitos fundamentais.

Negri (2023) destaca que softwares de IA treinados em bases inadequadas replicam decisões humanas enviesadas, produzindo resultados que reforçam a seletividade penal. Assim, quando esses sistemas são aplicados para identificar suspeitos, mesmo pequenas discrepâncias visuais podem ser interpretadas como “compatíveis”, gerando falsos positivos. Tais efeitos são agravados pela opacidade dos algoritmos, que impede a compreensão das etapas de decisão.

Outro dado relevante encontrado nos resultados refere-se ao aumento das detenções cautelares injustas. Porto e Rolim (2022) argumentam que os erros de correspondência, mesmo quando identificados posteriormente, deixam marcas profundas na vida dos acusados, que enfrentam não apenas o encarceramento temporário, mas também danos morais, estigmatização social e prejuízos laborais. Esse conjunto de impactos demonstra que o erro algorítmico possui repercussões longas e irreversíveis.

Araujo, Zullo e Torres (2020) observam que a tecnologia tem sido empregada no Brasil principalmente para fins de investigação criminal e localização de suspeitos, embora ainda careça de mecanismos legais de controle. Os autores apontam que a confiabilidade excessiva depositada nesses sistemas pelos operadores da segurança pública contribui para abordagens sem critérios e ações policiais que se justificam exclusivamente por alertas algorítmicos.

A falta de regulamentação, conforme apontado por Biondi e Cernev (2023), contribui diretamente para o aumento desses erros, já que não há critérios legais mínimos para a aquisição, auditoria ou implementação de sistemas de reconhecimento facial. Os autores afirmam que, enquanto não houver diretrizes claras sobre responsabilidade e limites de uso, os riscos continuarão a recair sobre a parcela mais vulnerável da população.

Em perspectiva internacional, Negri (2023) observa que países europeus têm avançado na criação de restrições à tecnologia, justamente porque os erros são considerados incompatíveis com princípios fundamentais como igualdade, privacidade e dignidade humana. Essa tendência sugere que a eficácia da

ferramenta não pode ser tratada como valor absoluto quando viola direitos essenciais. Portanto, os resultados evidenciam que o reconhecimento facial, embora avançado do ponto de vista tecnológico, não possui confiabilidade suficiente para ser utilizado como mecanismo autônomo de identificação no processo penal. Sua aplicação, sem rigor metodológico e sem controle estatal adequado, intensifica erros, amplia desigualdades e viola princípios constitucionais essenciais (Porto; Rolim, 2022).

Além dos impactos diretamente observáveis nas prisões injustas, os estudos analisados evidenciam que parte significativa das falhas decorre de omissões administrativas relacionadas à ausência de fiscalização, testes prévios e auditorias contínuas. Biondi e Cernev (2023) destacam que muitos dos sistemas utilizados por órgãos de segurança pública no Brasil foram adquiridos sem critérios claros de conformidade técnica, sem avaliação de impacto regulatório e sem supervisão institucional mínima. Tal prática viola princípios administrativos como legalidade, eficiência e transparência, previstos no art. 37 da Constituição Federal, ao permitir que tecnologias de alto risco sejam implementadas sem protocolos de controle adequados. Assim, a esfera administrativa não apenas condiciona o desempenho da tecnologia, como também contribui diretamente para a incidência de erros estruturais.

3.2 Vieses Algorítmicos, Racismo Estrutural e Seletividade Penal

A análise dos estudos demonstra que os sistemas de reconhecimento facial não operam em neutralidade técnica, mas sim reproduzem vieses estruturais presentes na sociedade. Negri e Winter (2023) explicam que o machine learning depende de bases de dados massivas formadas por decisões e registros humanos, o que significa que preconceitos raciais e desigualdades históricas são incorporados ao processo de treinamento das inteligências artificiais. Assim, longe de corrigir as falhas humanas, os algoritmos acabam por replicá-las em escala ampliada, reforçando padrões discriminatórios já consolidados no sistema penal brasileiro.

Buolamwini e Gebru (2018) realizaram um dos estudos mais expressivos sobre viés racial em sistemas de reconhecimento facial, revelando índices de erro

extremamente elevados na identificação de mulheres negras chegando a 34,7% em contraste com apenas 0,8% em homens brancos. Esses dados evidenciam que a tecnologia é significativamente mais falha quando aplicada a determinados grupos raciais e de gênero. O impacto dessa disparidade, quando transposto para a esfera penal, é potencialmente devastador, pois significa que pessoas negras têm probabilidade muito maior de serem falsamente acusadas e detidas.

No Brasil, os efeitos desse viés são ainda mais acentuados devido à forte presença do racismo estrutural nas práticas de segurança pública. Porto e Rolim (2022) observam que o sistema penal brasileiro já opera historicamente com uma lógica de seletividade que recai desproporcionalmente sobre pessoas negras e pobres. Quando tecnologias enviesadas são inseridas nesse contexto, o resultado é a amplificação dessa seletividade, reforçando uma gestão penal da pobreza e naturalizando a vigilância concentrada sobre corpos negros.

Os dados apresentados pela Defensoria Pública do Rio de Janeiro reforçam essa tendência: entre 2011 e 2020, 81% das prisões injustas baseadas em reconhecimento fotográfico tecnologia precursora do reconhecimento facial automatizado envolveram pessoas negras (Negri; Winter, 2023). Esses números revelam que a seletividade racial não é uma hipótese abstrata, mas um dado empírico consistente e preocupante. Se a identificação manual já produzia tamanha distorção, os sistemas automatizados tendem a expandi-la devido à autoridade atribuída às máquinas.

Outro ponto fundamental evidenciado por Negri (2023) é a opacidade dos algoritmos, que impede a verificação pública dos critérios de decisão utilizados pelos softwares. Tal opacidade inviabiliza auditorias independentes e dificulta a identificação de vieses internos. Quando não é possível compreender como um sistema chega a determinada correspondência facial, torna-se impossível contestá-la juridicamente. Assim, a opacidade tecnológica cria um ciclo no qual o algoritmo é tratado como “perito infalível”, mesmo que produza resultados racistas.

A presença de vieses também é observada em outros países, o que reforça que o problema não se limita ao contexto brasileiro. No Reino Unido, o grupo Big Brother Watch verificou que mais de 89% dos alertas emitidos por sistemas de reconhecimento facial foram falsos positivos, com maior incidência entre pessoas

negras, pardas, mulheres e até crianças negras (Negri; Winter, 2023). Esses achados internacionais corroboram a tese de que o reconhecimento facial é estruturalmente racializado, independentemente do país que o utiliza.

Conforme destaca Araujo, Zullo e Torres (2020), o uso indiscriminado da tecnologia sem padrões legais de transparência e controle reforça formas de policiamento baseado em perfis, prática historicamente associada ao racismo institucional. Assim, a IA não apenas replica o racismo existente, mas também o legitima ao revesti-lo de um verniz tecnológico, transformando discriminação em suposta “eficiência algorítmica”. O risco é que agentes de segurança interpretem alertas como verdade objetiva, sem questionar as limitações técnicas dos sistemas. Outro aspecto crucial é o fenômeno da “hiperidentificação”, no qual indivíduos que já foram registrados equivocadamente em sistemas policiais passam a ser constantemente reconhecidos como suspeitos em diferentes câmeras e contextos.

Negri e Winter (2023) explicam que esse efeito se torna um ciclo de criminalização automática, pois a tecnologia não corrige seus erros anteriores, ao contrário, tende a repeti-los. Isso gera um cenário em que uma vítima de erro inicial pode continuar sendo perseguida pelo sistema indefinidamente.

Biondi e Cernev (2023) afirmam que, no Brasil, a ausência de regulamentação e de padrões de auditoria técnica amplifica drasticamente esses riscos. Os autores relatam que grande parte dos sistemas utilizados no país foi adquirida sem critérios claros de qualidade, sem avaliação de impacto regulatório e sem mecanismos de mensuração de vieses. Assim, não há garantias de que os algoritmos utilizados atendam minimamente aos princípios da igualdade, proporcionalidade e transparência previstos na Constituição Federal.

Os estudos analisados apontam que a combinação entre tecnologia enviesada e sistema penal seletivo cria uma forma de “racismo algorítmico”, expressão utilizada por Negri e Winter (2023) para descrever a atualização digital do racismo estrutural. Nesse modelo, a discriminação não é fruto apenas de intenção humana, mas emerge de padrões matemáticos construídos a partir de dados contaminados por desigualdades históricas. Trata-se, portanto, de um fenômeno complexo, que exige respostas jurídicas igualmente sofisticadas.

Dessa forma, fica evidente que os sistemas de reconhecimento facial, ao invés de reduzirem desigualdades, contribuem para sua manutenção e agravamento. A automatização da vigilância e da identificação de suspeitos, quando realizada com algoritmos enviesados, viola diretamente os princípios da igualdade, da dignidade da pessoa humana e da não discriminação (Negri; Winter, 2023). Assim, o uso da tecnologia em sua forma atual não pode ser considerado compatível com o Estado Democrático de Direito, especialmente em um país marcado por profundas desigualdades raciais como o Brasil.

3.3 Consequências Jurídicas: Violações de Garantias Fundamentais e Responsabilidade do Estado

A análise jurídica dos impactos do reconhecimento facial evidencia que os erros de identificação produzidos pelos algoritmos representam graves violações a garantias fundamentais previstas na Constituição Federal. A presunção de inocência, princípio estruturante do processo penal brasileiro, torna-se fragilizada quando decisões judiciais são baseadas em alertas automatizados que possuem margens significativas de imprecisão. Negri e Winter (2023) enfatizam que, ao atribuir autoridade epistêmica aos sistemas de IA, operadores do Direito tendem a inverter o ônus argumentativo, tratando o algoritmo como “verdade objetiva”, ainda que sua lógica interna seja opaca. Essa prática subverte o devido processo legal e compromete a exigência de prova robusta para legitimar medidas restritivas de liberdade.

Além disso, o uso da tecnologia sem critérios normativos claros desafia diretamente o princípio da dignidade da pessoa humana, uma vez que permite que indivíduos sejam submetidos a abordagens, detenções e até prisões com base em inferências probabilísticas. De acordo com Porto e Rolim (2022), a dignidade é violada quando pessoas são expostas a constrangimentos ilegais, estigmatização social e perda de liberdade por erros algorítmicos que poderiam ter sido evitados mediante auditoria adequada. A submissão do corpo negro a vigilância intensificada reforça uma lógica de desumanização, incompatível com o Estado Democrático de Direito.

Outro aspecto jurídico crucial refere-se à violação do direito à imagem e à privacidade. O reconhecimento facial, por sua própria natureza, opera mediante extração de dados biométricos sensíveis, classificados pela LGPD como informações de alta proteção jurídica. Leardini (2021) destaca que o uso indiscriminado de câmeras integradas a sistemas de IA permite a formação de bancos de dados massivos, muitas vezes sem consentimento ou transparência, tornando possível o rastreamento contínuo de cidadãos inocentes. A ausência de regulamentação aprofundada sobre o tema agrava esse problema e torna o tratamento desses dados uma zona de insegurança jurídica.

O uso da tecnologia com fins de persecução penal também colide com o princípio da proporcionalidade, especialmente quando os erros são previsíveis pela literatura técnica. Buolamwini e Gebru (2018) demonstram que a taxa de erro nas identificações aumenta de forma desproporcional em grupos já historicamente marginalizados, o que significa que o Estado utiliza uma ferramenta cuja probabilidade de prejudicar inocentes é amplamente conhecida. Sendo assim, a escolha estatal por adotar tais sistemas deve ser avaliada à luz da proibição do excesso, sob pena de violação direta às garantias constitucionais.

No campo da responsabilidade civil do Estado, inúmeros autores defendem que os danos decorrentes de identificação equivocada geram dever de reparação, uma vez que se trata de atividade estatal de risco. Segundo Negri (2023), quando o Estado utiliza algoritmos discriminatórios ou não auditados e, com isso, causa prejuízos materiais, morais ou sociais a um indivíduo, não pode se eximir da responsabilidade alegando falhas tecnológicas. A responsabilidade objetiva, prevista no art. 37, §6º da Constituição Federal, exige que o poder público indenize sempre que houver dano decorrente de sua atuação, e isso inclui danos produzidos por sistemas automatizados que substituem ou complementam decisões humanas.

No âmbito administrativo, a responsabilidade estatal também se manifesta quando agentes públicos ou instituições deixam de cumprir deveres de controle, supervisão e auditoria sobre tecnologias sensíveis. Araujo, Zullo e Torres (2020) ressaltam que a adoção de sistemas automatizados sem regulamentação específica caracteriza falha administrativa, pois descumpre obrigações funcionais mínimas relacionadas à governança da informação, à gestão de riscos e à proteção de dados

sensíveis. A ausência de protocolos administrativos de verificação e correção de vieses constitui violação ao princípio da eficiência administrativa e pode resultar em responsabilização disciplinar, além de comprometer a legitimidade institucional. Assim, o erro algorítmico não é apenas problema técnico, mas também fruto de decisões administrativas inadequadas.

Casos concretos reforçam essa compreensão. No Brasil, como relatado por Guimarães (2021), pessoas foram presas indevidamente devido a alertas automáticos e passaram dias encarceradas, perdendo emprego, reputação e enfrentando humilhações públicas. Esses episódios mostram que o dano causado pelo reconhecimento facial não é abstrato ou meramente estatístico, é material, concreto e devastador. A análise jurídica desses casos demonstra que o Estado falhou duplamente: Ao utilizar tecnologia incapaz de garantir precisão mínima e ao expandir seu uso sem parâmetros normativos.

Outro ponto relevante refere-se à ausência de transparência na tomada de decisão algorítmica. Araujo, Zullo e Torres (2020) afirmam que a falta de explicabilidade dos algoritmos impossibilita a ampla defesa e o contraditório, já que o cidadão não pode contestar adequadamente um resultado cuja lógica interna é inacessível. A violação desses princípios processuais compromete a legitimidade do processo penal e cria um sistema no qual o acusado enfrenta uma “prova técnica” impossível de refutar, mesmo quando incorreta.

Em países europeus, como demonstram Negri e Winter (2023), a preocupação com essas violações levou a União Europeia a classificar o reconhecimento facial em tempo real como tecnologia de “alto risco” no EU AI Act, o que implica exigências rigorosas de transparência, avaliação de impacto e limites de uso. A comparação internacional evidencia que, enquanto outros países avançam para restringir ou mesmo banir o uso dessa tecnologia, o Brasil ainda carece de um marco regulatório coerente que impeça abusos e discriminações.

O uso indiscriminado do reconhecimento facial também cria rupturas institucionais, pois altera profundamente a forma como o Estado exerce vigilância. Biondi e Cernev (2023) destacam que, em contextos sem regulamentação, há expansão descontrolada do monitoramento automatizado, o que pode resultar em um cenário de vigilância massiva incompatível com princípios democráticos. A falta

de limites normativos claros permite que câmeras integradas a sistemas de IA sejam utilizadas de formas não previstas, ampliando o poder policial e reduzindo a supervisão estatal.

Além disso, há impactos diretos na confiança pública no sistema de justiça. Estudos apresentados por Negri (2023) indicam que erros sucessivos de identificação minam a percepção de legitimidade das instituições, sobretudo entre grupos que historicamente já enfrentam abordagens policiais excessivas. A manutenção de um sistema penal enviesado por algoritmos reforça a crença social de que o Estado seleciona seus suspeitos com base em estereótipos e não em critérios jurídicos objetivos.

A própria jurisprudência brasileira começa a reconhecer essa problemática. No HC 598.886/SC, o STJ afirmou que o reconhecimento fotográfico mesmo feito manualmente é instrumento frágil e sujeito a indução por estereótipos raciais. Quando essa fragilidade é automatizada, o risco jurídico se multiplica. O Tribunal deixou claro que não se pode admitir que pessoas sejam privadas de liberdade com base em métodos cujo erro é estatisticamente provável (STJ, 2020). Essa diretriz jurisprudencial aponta um caminho para a futura regulamentação do tema.

Portanto, as consequências jurídicas dos erros produzidos pelo reconhecimento facial são profundas e multifacetadas. A tecnologia, em sua forma atual, viola direitos fundamentais, compromete princípios basilares do processo penal e expõe o Estado a responsabilidade civil ampla. Como afirmam Porto e Rolim (2022), insistir no uso dessa ferramenta sem regulamentação adequada equivale a institucionalizar práticas discriminatórias sob a aparência de modernização. Assim, do ponto de vista jurídico e constitucional, torna-se evidente que o reconhecimento facial exige limites rígidos, auditoria contínua e controle social efetivo, sob pena de aprofundar injustiças estruturais.

A literatura também aponta que a mitigação de erros depende diretamente da criação de modelos robustos de governança algorítmica, o que inclui auditorias independentes, relatórios de impacto regulatório, supervisão contínua e mecanismos de transparência administrativa (Negri; Winter, 2023). Países europeus, por exemplo, exigem registros claros sobre o funcionamento dos algoritmos, protocolos de explicabilidade e limites estritos para seu uso, justamente para evitar omissões

administrativas que gerem riscos à população. No contexto brasileiro, a inexistência de tais mecanismos torna o reconhecimento facial incompatível com os deveres administrativos de prevenção, controle e prestação de contas. Assim, a esfera administrativa é decisiva para determinar se a tecnologia reforçará desigualdades ou atuará em conformidade com princípios constitucionais.

4 CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo analisar os impactos jurídicos decorrentes dos erros de reconhecimento facial na identificação de suspeitos, especialmente no contexto do sistema de justiça criminal brasileiro. A partir da revisão de literatura realizada, foi possível constatar que a utilização dessa tecnologia, embora frequentemente apresentada como instrumento de modernização e eficiência, opera com limitações técnicas relevantes e produz consequências que comprometem garantias fundamentais. Os resultados evidenciaram que os equívocos gerados pelos algoritmos não constituem falhas isoladas, mas um padrão recorrente associado a vieses estruturais que atravessam tanto as bases de dados quanto às práticas institucionais da segurança pública.

O objetivo geral foi plenamente alcançado ao demonstrar que tais erros configuram violações diretas à presunção de inocência, ao devido processo legal, à dignidade da pessoa humana e ao direito à igualdade. Do mesmo modo, os objetivos específicos foram atendidos à medida que se identificaram os fatores tecnológicos e sociais que contribuem para os erros de correspondência, analisaram-se as repercussões desses equívocos sobre direitos fundamentais e discutiu-se a responsabilidade do Estado diante de prisões e constrangimentos derivados da adoção da tecnologia.

A discussão desenvolvida permitiu compreender que os sistemas de reconhecimento facial, em sua configuração atual, não apresentam condições de funcionamento que assegurem confiabilidade, neutralidade ou segurança jurídica. Ao contrário, reforçam padrões de seletividade penal e aprofundam desigualdades já existentes, sobretudo em relação a grupos racialmente vulnerabilizados. Observou-se, ainda, que a ausência de regulamentação específica, aliada à

opacidade dos algoritmos, dificulta a fiscalização social, fragiliza a proteção de dados sensíveis e aumenta o risco de danos irreversíveis para as pessoas injustamente identificadas como suspeitas.

De modo geral, constatou-se que a tecnologia não pode ser utilizada como ferramenta autônoma de persecução penal, tampouco como fundamento único para medidas restritivas de liberdade. Sua adoção sem critérios técnicos rigorosos, sem parâmetros normativos e sem mecanismos de auditoria contínua traduz-se em violação de direitos e na ampliação de injustiças estruturais. Assim, verifica-se a necessidade urgente de elaboração de marcos regulatórios sólidos, capazes de estabelecer limites claros, garantir transparência, prever responsabilização estatal e assegurar que qualquer uso da inteligência artificial esteja alinhado aos princípios constitucionais.

Conclui-se, portanto, que o reconhecimento facial deve ser adotado com extrema cautela no âmbito jurídico, sobretudo no processo penal. Enquanto não houver garantias técnicas, normativas e institucionais capazes de mitigar os riscos identificados, sua utilização permanece incompatível com a efetividade dos direitos fundamentais e com os pressupostos do Estado Democrático de Direito. O estudo evidencia a necessidade de aprofundar pesquisas e promover debates interdisciplinares que permitam construir alternativas tecnológicas e jurídicas alinhadas à proteção da liberdade, da igualdade e da justiça. Reconhece-se, ainda, que a revisão integrativa apresenta limitações decorrentes da dependência de estudos já publicados, da diversidade metodológica das fontes e da falta de dados empíricos nacionais consolidados sobre a acurácia dos sistemas atualmente utilizados. Assim, permanecem lacunas relevantes para investigações futuras, especialmente análises empíricas sobre o desempenho real dos algoritmos no Brasil, estudos sobre governança algorítmica na esfera penal, impactos psicossociais das prisões injustas e pesquisas que integrem Direito, Tecnologia e Direitos Humanos na formulação de modelos regulatórios mais eficientes.

REFERÊNCIAS

ARAUJO, A. L.; ZULLO, D.; TORRES, M. Reconhecimento facial: desafios jurídicos, tecnológicos e sociais. 2020.

BIONDI, P.; CERNEV, A. Inteligência artificial, vieses e impactos regulatórios no Brasil. 2023.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus n. 598.886/SC. Rel. Min. Rogério Schietti Cruz. Sexta Turma. Julgado em 27 out. 2020.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, v. 1, p. 1-15, 2018.

COSTA, Iraneidson Santos. Europa, Itália e Roma Negra. In: A Bahia já deu régua e compasso: medicina legal, raça e criminalidade na Bahia (1890–1940). Salvador: EDUFBA, 2023. p. 65–75. Disponível em: https://doi.org/10.7476/9786556305011.0004. Acesso em: 10 nov. 2025.

G1 BAHIA. Dentista é presa após erro de reconhecimento facial em Salvador. G1, Salvador, 2023. Disponível em: https://g1.globo.com. Acesso em: 20 nov. 2025.

G1 RIO. Jovem é preso por engano após ser confundido por sistema de reconhecimento facial. G1, Rio de Janeiro, 2022. Disponível em: https://g1.globo.com. Acesso em: 20 nov. 2025.

GUIMARÃES, T. Prisões injustas e reconhecimento facial: estudo de casos no Brasil. 2021.

LEARDINI, A. Privacidade, proteção de dados e tecnologias de vigilância: implicações jurídicas do uso de sistemas inteligentes. 2021.

LOMBROSO, Cesare. O homem delinquente. 5. ed. Rio de Janeiro: Forense, 2001.

NEGRI, A. L. Discriminação algorítmica e regulação da inteligência artificial: riscos, limites e perspectivas. 2023.

NEGRI, A. L.; WINTER, L. A. C. Falhas da regulamentação da inteligência artificial no combate à discriminação algorítmica realizada pelo reconhecimento facial. RRDDIS – Revista Rede de Direito Digital, Intelectual & Sociedade, Curitiba, v. 3, n. 6, p. 243-266, 2023.

PORTO, T.; ROLIM, M. Reconhecimento facial, seletividade penal e impactos sociais no sistema de justiça criminal. 2022.

RODRIGUES, Raimundo Nina. As raças humanas e a responsabilidade penal no Brasil. 4. ed. São Paulo: Companhia Editora Nacional, 1957.

UOL NOTÍCIAS. Homem fica preso 37 dias após reconhecimento equivocado por foto antiga. UOL, São Paulo, 2021. Disponível em: https://www.uol.com.br. Acesso em: 20 nov. 2025.