



**UNIVERSIDADE CATÓLICA DO SALVADOR**  
**GRADUAÇÃO EM DIREITO**

**JOANA MORAIS DA PAIXÃO**

**VIGILÂNCIA E RECONHECIMENTO FACIAL: RESPONSABILIDADE DO  
ESTADO NA DISCRIMINAÇÃO ALGORÍTMICA DE PESSOAS NEGRAS E  
PERIFÉRICAS**

**SALVADOR - BAHIA**

**2026**

**JOANA MORAIS DA PAIXÃO**

**VIGILÂNCIA E RECONHECIMENTO FACIAL: RESPONSABILIDADE DO  
ESTADO NA DISCRIMINAÇÃO ALGORÍTMICA DE PESSOAS NEGRAS E  
PERIFÉRICAS**

Trabalho de Conclusão de Curso apresentado  
como requisito para obtenção de título de  
bacharel em Direito da Universidade Católica  
do Salvador, sob a orientação da Profa. Dra.  
Laura Cecília Fagundes dos Santos Braz.

**SALVADOR - BAHIA**

**2026**

**JOANA MORAIS DA PAIXÃO**

**VIGILÂNCIA E RECONHECIMENTO FACIAL: RESPONSABILIDADE DO  
ESTADO NA DISCRIMINAÇÃO ALGORÍTMICA DE PESSOAS NEGRAS E  
PERIFÉRICAS**

Trabalho de Conclusão de Curso apresentado  
como requisito para obtenção de título de  
bacharel em Direito da Universidade Católica  
do Salvador, sob a orientação da Profa. Dra.  
Laura Cecília Fagundes dos Santos Braz.

Salvador, 22 de junho de 2026.

**BANCA EXAMINADORA**

---

Profa. Dra. Laura Cecília Fagundes dos Santos Braz  
Universidade Católica do Salvador

---

Prof. Me. Carlos Alberto José Barbosa Coutinho  
Universidade Católica do Salvador

---

Prof. Esp. Nicholas Moura da Luz  
Universidade Federal da Bahia

## **AGRADECIMENTOS**

Primeiramente, gostaria de agradecer a Deus e a todos que iluminaram o meu caminho até aqui. Agradeço aos meus pais pela dedicação, comprometimento e amor que depositaram em toda a minha vida, especialmente na minha formação educacional. À minha mãe, Darlane, exemplo feminino em minha vida, que sempre esteve ao meu lado com palavras de encorajamento, mostrando-me o quão longe posso chegar e sempre deixando explícito o seu orgulho por mim. Ao meu pai, Ironaldo, que desde sempre se mostrou interessado e orgulhoso de cada conquista minha. O amor e a dedicação de vocês certamente me trouxeram até aqui e, com toda certeza, me levarão a lugares inimagináveis. Gostaria de agradecer também às minhas avós, Amélia e Evani, que, mesmo sem entender, sempre se demonstraram interessadas pelo meu futuro. E ao meu avô, Israel, que, de onde estiver, sei que olha por mim. Por último, mas não menos importante, quero agradecer ao meu pet, Apolo, que genuinamente esteve ao meu lado em todas as madrugadas de estudo desde que entrou em minha vida, sempre me fazendo companhia e, de alguma forma, garantindo que eu não estivesse sozinha ao longo desse período.

## **RESUMO**

Este estudo analisou a responsabilidade civil do Estado decorrente da utilização de sistemas de reconhecimento facial baseados em inteligência artificial no contexto da segurança pública brasileira, sob o prisma do risco de discriminação algorítmica contra a população negra e periférica. O problema de pesquisa centrou-se em investigar a compatibilidade dessas ferramentas com os direitos fundamentais e os limites para a responsabilização estatal em caso de erros operacionais. Para tanto, adotou-se uma metodologia de natureza qualitativa, com caráter exploratório e descritivo, por meio de pesquisa bibliográfica, documental e análise jurisprudencial dos Tribunais Superiores, utilizando-se o método dedutivo. Como resultados, constatou-se que os vieses algorítmicos e os falsos positivos não constituem meras falhas técnicas isoladas, mas sim a reprodução institucional do racismo estrutural na formação da suspeita penal, gerando prisões injustas e violações diretas às garantias constitucionais da igualdade e do devido processo legal. Conclui-se que a responsabilidade do Estado nesses cenários é de natureza objetiva, nos termos do artigo 37, §6º, da Constituição Federal, evidenciando-se a premente necessidade de mecanismos rigorosos de regulação, governança de dados e fiscalização externa para impedir que os aparatos tecnológicos perpetuem e ampliem as desigualdades históricas no Estado Democrático de Direito.

Palavras-chave: Reconhecimento facial; Discriminação algorítmica; Responsabilidade do Estado; Direitos fundamentais; Racismo estrutural.

## **ABSTRACT**

This study analyzed the civil liability of the State arising from the use of facial recognition systems based on artificial intelligence within the context of Brazilian public security, under the perspective of the risk of algorithmic discrimination against the Black and peripheral population. The research problem focused on investigating the compatibility of these tools with fundamental rights and the limits for state accountability in the event of operational errors. To this end, a qualitative research methodology was adopted, with an exploratory and descriptive approach, through bibliographic and documentary research, as well as jurisprudential analysis of the Higher Courts, utilizing the deductive method. As a result, it was found that algorithmic biases and false positives do not constitute mere isolated technical flaws, but rather the institutional reproduction of structural racism in the formation of criminal suspicion, resulting in unjust arrests and direct violations of constitutional guarantees of equality and due process of law. It is concluded that the State's liability in these scenarios is strict, pursuant to Article 37, §6, of the Federal Constitution, highlighting the pressing need for rigorous mechanisms of regulation, data governance, and external oversight to prevent technological apparatuses from perpetuating and amplifying historical inequalities within the Democratic State of Law.

**Keywords:** Facial recognition; Algorithmic discrimination; State liability; Fundamental rights; Structural racism.

## SUMÁRIO

|                                                                                                        |           |
|--------------------------------------------------------------------------------------------------------|-----------|
| <b>1. INTRODUÇÃO.....</b>                                                                              | <b>8</b>  |
| <b>2. METODOLOGIA.....</b>                                                                             | <b>10</b> |
| <b>3. RACISMO E DESIGUALDADE ESTRUTURAL NO BRASIL.....</b>                                             | <b>12</b> |
| 3.1. FORMAÇÃO HISTÓRICA DAS DESIGUALDADES RACIAIS NO<br>BRASIL.....                                    | 13        |
| 3.2. RACISMO ESTRUTURAL E SELETIVIDADE NO SISTEMA DE CONTROLE<br>SOCIAL.....                           | 15        |
| <b>4. TECNOLOGIAS DE VIGILÂNCIA E RECONHECIMENTO FACIAL NO<br/>BRASIL.....</b>                         | <b>17</b> |
| 4.1. CONCEITO E FUNCIONAMENTO DOS SISTEMAS DE RECONHECIMENTO<br>FACIAL.....                            | 18        |
| 4.2. IMPLEMENTAÇÃO DE CÂMERAS DE SEGURANÇA COM IA NA<br>SEGURANÇA PÚBLICA BRASILEIRA.....              | 20        |
| <b>5. DISCRIMINAÇÃO ALGORÍTMICA, ERROS DE IDENTIFICAÇÃO E<br/>VIESES NO RECONHECIMENTO FACIAL.....</b> | <b>22</b> |
| <b>6. DIREITOS FUNDAMENTAIS AFETADOS PELO RECONHECIMENTO<br/>FACIAL.....</b>                           | <b>25</b> |
| <b>7. RESPONSABILIDADE DO ESTADO E LIMITES AO USO DA<br/>TECNOLOGIA.....</b>                           | <b>29</b> |
| 7.1. RESPONSABILIDADE CIVIL DO ESTADO POR ERROS DE<br>IDENTIFICAÇÃO.....                               | 31        |
| 7.2. DEVIDO PROCESSO LEGAL E USO DE TECNOLOGIAS NA PERSECUÇÃO<br>PENAL.....                            | 36        |
| 7.3. NECESSIDADE DE REGULAÇÃO E CONTROLE ESTATAL.....                                                  | 39        |
| 7.4. ANÁLISE JURISPRUDENCIAL E CASOS CONCRETOS.....                                                    | 41        |
| <b>8. CONSIDERAÇÕES FINAIS.....</b>                                                                    | <b>43</b> |
| <b>REFERÊNCIAS.....</b>                                                                                | <b>45</b> |

## 1. INTRODUÇÃO

As ferramentas de inteligência artificial vêm expandindo-se de forma significativa no âmbito da segurança pública e têm promovido profundas transformações nas dinâmicas de vigilância e controle social. Dentre essas inovações, destacam-se os mecanismos de reconhecimento facial aplicados a dispositivos de monitoramento, amplamente empregados com o escopo de identificar indivíduos em espaços públicos, coibir ilícitos e subsidiar investigações. Inseridos em um contexto de vanguarda tecnocientífica e de busca por maior eficiência estatal, referidos recursos vêm sendo progressivamente adotados por órgãos públicos no Brasil. Porém, a despeito dos potenciais benefícios associados à modernização das práticas de policiamento, a instrumentalização dessas tecnologias suscita relevantes questionamentos jurídicos, notadamente no que tange à salvaguarda de direitos fundamentais e à responsabilização estatal por eventuais danos decorrentes de sua aplicação.

No cenário brasileiro, marcado por severas disparidades sociais e raciais, a implementação de tais sistemas não ocorre em um ambiente neutro ou equilibrado. Ao contrário, amolda-se a uma realidade historicamente estruturada por práticas discriminatórias que influenciam a atuação das instituições e os processos de criminalização. Nesse panorama, a população negra e periférica figura como o alvo preferencial de abordagens ostensivas, evidenciando a seletividade penal já operante no aparato de segurança pública. A introdução de tecnologias baseadas em aprendizado de máquina, portanto, descortina a necessidade de investigação acerca da reprodução ou intensificação dessas assimetrias por meio de procedimentos automatizados.

Estudos técnicos demonstram que os softwares de biometria facial apresentam taxas de erro expressivamente maiores na identificação de pessoas negras, em razão, particularmente, do viés algorítmico arraigado nos bancos de dados utilizados para o treinamento dos sistemas. Essas falhas técnicas culminam em falsas correspondências, ensejando abordagens indevidas, constrangimentos ilegais e, em cenários mais gravosos, privações injustas da liberdade. Diante disso, emerge o problema jurídico relativo à responsabilidade civil do Estado pelos prejuízos oriundos da utilização de aparatos que, embora destinados à promoção da ordem pública, operam como vetores de discriminação indireta contra minorias raciais.

Sob a perspectiva jurídica, o emprego de sistemas de identificação facial tange diretamente o núcleo de garantias fundamentais, tais como a igualdade, a dignidade da



pessoa humana, a privacidade e o devido processo legal. A presença de equívocos sistemáticos que atingem desproporcionalmente determinados estratos sociais evidencia o potencial lesivo da discriminação indireta, exigindo escrutínio crítico acerca da legitimidade do uso de tais ferramentas pelo poder público. Ademais, o tratamento de dados biométricos insere a discussão no ecossistema da proteção de dados pessoais, impondo balizamentos à atuação estatal e requerendo mecanismos adequados de controle e fiscalização.

Mediante os fatos expostos, o presente estudo visa à análise da responsabilidade civil do Estado decorrente da utilização de sistemas de reconhecimento facial baseados em inteligência artificial no contexto da segurança pública brasileira, com foco no viés algorítmico que vulnerabiliza a população negra e periférica. O objetivo geral da pesquisa visa a examinar a compatibilidade dessas práticas com os direitos fundamentais previstos na Constituição Federal de 1988, bem como discutir os limites jurídicos ao uso dessas tecnologias e a necessidade de procedimentos regulatórios capazes de garantir que sua aplicação esteja em perfeita consonância com os princípios do Estado Democrático de Direito.

## 2. METODOLOGIA

O presente trabalho consiste em uma investigação de natureza qualitativa, desenvolvida com o objetivo de analisar a responsabilidade civil do Estado decorrente da implementação de sistemas de reconhecimento facial baseados em inteligência artificial no cenário da segurança pública brasileira, especialmente diante dos riscos de discriminação algorítmica que atingem a população negra e periférica. O estudo possui caráter exploratório e descritivo, buscando compreender os impactos jurídicos e sociais da adoção dessas ferramentas e sua compatibilidade com os direitos fundamentais assegurados pela Constituição Federal de 1988.

Para a realização do estudo, foram utilizados os métodos de pesquisa bibliográfica e documental. O levantamento bibliográfico fundamentou-se no exame de livros, artigos científicos, dissertações, teses e demais produções acadêmicas relacionadas ao racismo estrutural, à inteligência artificial, à discriminação algorítmica, à proteção de dados pessoais e à responsabilidade civil do Estado. Também foram consultados relatórios elaborados por instituições de ensino, organizações da sociedade civil e órgãos públicos que se dedicam à investigação dos impactos produzidos pelas tecnologias de vigilância e monitoramento automatizado.

A vertente documental concentrou-se no exame da legislação aplicável à matéria, especialmente da Carta Magna, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), do Código de Processo Penal e de outras normas relacionadas ao tratamento de dados biométricos e ao manejo de mecanismos tecnológicos no âmbito da segurança pública. Além disso, foram analisados relatórios técnicos, notas institucionais e documentos produzidos por entidades nacionais voltadas ao estudo do aprendizado de máquina e dos direitos fundamentais.

No desenvolvimento do trabalho, adotou-se o método dedutivo, partindo-se da análise de conceitos gerais relacionados ao racismo estrutural, aos direitos fundamentais e à responsabilidade estatal para, posteriormente, examinar sua aplicação específica aos sistemas de identificação facial utilizados pelo poder público. Também foi realizada uma análise da jurisprudência de decisões proferidas pelos tribunais superiores, com destaque para julgados relacionados ao reconhecimento de pessoas, à validade da prova penal e às garantias processuais fundamentais, a fim de compreender o posicionamento do Poder Judiciário diante da crescente expansão dessas tecnologias.

Por fim, o estudo buscou promover uma reflexão crítica acerca dos limites jurídicos do emprego do reconhecimento facial pelo Estado, examinando a necessidade de mecanismos de controle, transparência e fiscalização capazes de assegurar a proteção dos direitos fundamentais e a compatibilidade dessas ferramentas com os princípios que orientam o Estado Democrático de Direito.

### **3. RACISMO E DESIGUALDADE ESTRUTURAL NO BRASIL**

O racismo e a desigualdade estrutural no Brasil estabelecem fenômenos que ultrapassam manifestações individuais de preconceito, integrados na própria organização social, econômica e institucional do país. As desigualdades raciais podem ser vistas no acesso à educação, ao mercado de trabalho, à renda, à moradia e à segurança, demonstrando que determinados grupos sociais estão sujeitos a condições historicamente desiguais de cidadania e acesso a direitos fundamentais.

Ainda que a Constituição Federal de 1988 tenha consolidado o princípio da igualdade e reconhecido o racismo como crime inafiançável e imprescritível, os indicadores sociais apontam que a população negra continua ocupando posições de maior vulnerabilidade social. Dados do Instituto Brasileiro de Geografia e Estatística (IBGE) revelam que pessoas pretas e pardas apresentam menores rendimentos médios, maiores índices de informalidade e menor presença em cargos de liderança quando comparadas à população branca. Essas diferenças demonstram que a desigualdade racial não pode ser entendida apenas sob uma perspectiva econômica, visto que envolve fatores históricos, sociais e institucionais que atuam diretamente na distribuição de oportunidades no país.

Além das desigualdades econômicas, a violência também atinge de maneira distinta determinados grupos sociais. Estudos recentes demonstram que a população negra representa a maior parcela das vítimas de homicídio no Brasil, sobretudo entre jovens moradores de periferias urbanas. Esse cenário indica que raça e condição social continuam exercendo influência significativa sobre o acesso à segurança, à proteção estatal e ao pleno exercício da cidadania.

Nesse contexto, o conceito de racismo estrutural torna-se fundamental para compreender a permanência dessas desigualdades. Conforme asseverou Silvio Almeida (2021), o racismo não se limita a práticas discriminatórias isoladas, mas integra o funcionamento das instituições e das estruturas sociais, produzindo mecanismos contínuos de exclusão e marginalização. Portanto, as desigualdades raciais deixam de ser interpretadas como situações ocasionais ou individuais, passando a ser entendidas como resultado de processos históricos e institucionais firmados ao longo do tempo.

A constância dessas desigualdades também influencia a maneira pela qual determinados grupos sociais são expostos a mecanismos de controle, vigilância e atuação estatal. Mesmo em contextos ligados à modernização institucional e ao avanço

tecnológico, estruturas sociais desiguais podem colaborar para a reprodução de práticas discriminatórias já existentes, principalmente quando determinados indivíduos permanecem historicamente vinculados a espaços de suspeição, marginalização e controle social.

Desta forma, compreender o racismo estrutural no Brasil exige analisar os processos históricos que colaboraram para a consolidação dessas desigualdades e para a manutenção de hierarquias sociais baseadas em critérios raciais. A exclusão econômica e social da população negra não se desenvolveu de forma espontânea, sendo diretamente relacionada à formação histórica da sociedade brasileira, marcada pela escravidão, pela ausência de políticas efetivas de integração após a abolição e pela construção de estruturas sociais excludentes que ainda produzem reflexos na realidade contemporânea (ALMEIDA, 2021; FERNANDES, 2008). Por isso, sob a lente de referidos autores, torna-se necessário compreender a própria formação histórica das desigualdades raciais no Brasil e os mecanismos que permitiram sua permanência ao longo do tempo.

### 3.1. FORMAÇÃO HISTÓRICA DAS DESIGUALDADES RACIAIS NO BRASIL

A formação histórica das desigualdades raciais no Brasil está diretamente ligada ao processo de colonização e à consolidação da escravidão como fator central da organização econômica e social do país. Durante mais de três séculos, o uso da mão de obra escravizada sustentou grande parte da produção agrícola e mineradora brasileira, fixando relações sociais marcadas pela exploração, pela violência e pela exclusão da população negra do acesso a direitos e espaços de poder (FERNANDES, 2008). Nesse cenário, a separação racial passou a ocupar papel importante na construção das hierarquias sociais brasileiras.

O sistema escravista não gerou apenas desigualdades econômicas, como também mecanismos sociais de marginalização que relacionavam a população negra a posições de inferioridade social. A escravidão foi responsável pela normalização de práticas de violência, controle e desumanização que impactaram profundamente a formação da sociedade brasileira. Assim, a exclusão racial deixou de ser apenas efeito da condição jurídica de pessoa escravizada, tornando-se parte da própria estrutura comunitária construída ao longo do período colonial e imperial.

Com a abolição da escravidão em 1888, conforme descortina a literatura sociológica nacional, o Estado brasileiro não realizou políticas efetivas de integração social da população negra recém-liberta. Sem acesso à terra, à educação ou a oportunidades econômicas, grande parte da população negra continuou em condições de pobreza e vulnerabilidade social. Ao mesmo tempo, políticas de incentivo à imigração europeia foram usadas como estratégia de reorganização do mercado de trabalho, reforçando processos de exclusão racial já existentes.

Ao longo do século XX, na esteira das análises de Fernandes (2008), espalhou-se a ideia de democracia racial, segundo a qual o Brasil teria desenvolvido relações harmoniosas entre diferentes grupos raciais em razão da miscigenação. No entanto, essa narrativa ajudou a dificultar o reconhecimento das desigualdades raciais existentes no país. Mesmo diante da ausência de segregação formal semelhante à observada em outros países, a população negra manteve-se submetida a menores oportunidades de acesso à educação, ao mercado de trabalho e à participação em espaços de poder.

A exclusão histórica da população negra ainda determinou a organização dos espaços urbanos brasileiros. O crescimento das cidades aconteceu de maneira desigual, acumulando populações negras e pobres em regiões periféricas marcadas pela precariedade de serviços públicos, ausência de infraestrutura adequada e maiores índices de vulnerabilidade social. Essas condições colaboraram para fortalecer associações históricas entre pobreza, marginalização e população negra, principalmente em contextos relacionados à segurança pública e ao controle social.

Além das desigualdades materiais, a herança escravista gerou impactos institucionais e culturais permanentes. A construção histórica da figura da pessoa negra como sujeito suspeito ou socialmente perigoso influenciou práticas institucionais e formas de atuação estatal ao longo do tempo. Dessa forma, as desigualdades raciais passaram a se reproduzir não apenas por meio da exclusão econômica, mas também por meio de mecanismos sociais e institucionais incorporados à estrutura da sociedade brasileira (FERNANDES, 2008; ALMEIDA, 2021).

Entender a formação histórica das desigualdades raciais no Brasil, portanto, é essencial para avaliar como determinadas práticas de controle e vigilância social evoluíram historicamente no país. As estruturas construídas desde o período escravista influenciaram de forma significativa a forma como determinados grupos sociais passaram a ser alvo preferencial da atuação repressiva estatal, aspecto que auxiliou para

a compreensão do racismo estrutural e da seletividade presentes no sistema de controle social brasileiro.

### 3.2. RACISMO ESTRUTURAL E SELETIVIDADE NO SISTEMA DE CONTROLE SOCIAL

O racismo estrutural influencia diretamente o funcionamento das instituições sociais e a forma como determinados grupos são vistos pelo poder público e pela sociedade. No Brasil, a atuação do sistema de controle social foi historicamente destacada por práticas seletivas que afetam de maneira mais intensa a população negra e periférica, principalmente em contextos ligados à segurança pública, vigilância estatal e repressão penal. Essa seletividade não acontece de forma isolada ou excepcional, mas está incluída em estruturas sociais construídas no decorrer da formação histórica brasileira (ALMEIDA, 2021)

O sistema de controle social compreende mecanismos formais e informais utilizados para regular comportamentos e manter determinada ordem social. Entre esses mecanismos, evidenciam-se a atuação policial, o sistema de justiça criminal, o sistema penitenciário e as políticas de segurança pública. Embora essas instituições tenham como finalidade garantir proteção e ordem social, sua atuação muitas vezes ocorre de maneira desigual, direcionando abordagens, suspeitas e intervenções estatais de forma excessiva sobre determinados grupos sociais.

No contexto brasileiro, a população negra ocupa posição central neste cenário de seletividade. Dados relacionados à violência, encarceramento e letalidade policial apontam que pessoas negras são as principais atingidas pela atuação repressiva do Estado (IPEA; FBSP, 2023). Na maioria dos casos, jovens negros moradores de periferias urbanas viram alvo preferencial de abordagens policiais, revistas pessoais, operações de segurança e ações de vigilância. Esse cenário evidencia que critérios raciais e sociais impactam diretamente a maneira como o controle estatal é exercido.

A seletividade do sistema penal também pode ser observada no perfil da população carcerária brasileira. O encarceramento em massa alcançou de maneira desproporcional pessoas negras e socialmente vulneráveis, demonstrando que o sistema de justiça criminal não atua de maneira imparcial em relação às desigualdades existentes na sociedade. Além das condições econômicas, fatores relacionados à raça,

território e posição social influenciam significativamente a maior exposição de certos grupos à criminalização e à repressão estatal.

Sob essa ótica, o racismo estrutural auxilia para a consolidação de padrões institucionais que combinam determinados indivíduos à suspeição e à periculosidade. A construção histórica da figura do indivíduo negro como potencial ameaça social influencia práticas institucionais, discursos de segurança pública e mecanismos de vigilância. Assim, o controle social passa a atuar de maneira seletiva, repetindo desigualdades históricas já presentes na estrutura social brasileira.

Além da atuação repressiva direta, essa seletividade também aparece na distribuição desigual de proteção estatal, aspecto também evidenciado nos dados de vulnerabilidade do IPEA (2023). Regiões periféricas e comunidades majoritariamente negras regularmente convivem com ausência de serviços públicos adequados, precariedade de direitos básicos e maior exposição à violência. Consequentemente, o controle exercido pelo Estado ocorre muitas vezes de maneira predominantemente punitiva, sem que haja proporcional garantia de cidadania, proteção social ou efetivação de direitos fundamentais.

A persistência dessas práticas evidencia que o racismo estrutural não se limita a comportamentos individuais discriminatórios, mas afeta o funcionamento das próprias instituições responsáveis pela manutenção da ordem social. A seletividade existente no sistema de controle social brasileiro demonstra como desigualdades raciais historicamente construídas continuam gerando impactos concretos sobre a vida da população negra, contribuindo para a manutenção de processos de exclusão, marginalização e violência institucional.

Diante disso, o avanço de tecnologias utilizadas para monitoramento, identificação e vigilância da população passa a exigir análise crítica, principalmente diante da possibilidade de reprodução de padrões discriminatórios já presentes na atuação estatal contemporânea. Dessa forma, torna-se essencial examinar o desenvolvimento das tecnologias de vigilância e reconhecimento facial no Brasil e seus impactos sobre grupos historicamente submetidos a processos seletivos de controle social.



#### **4. TECNOLOGIAS DE VIGILÂNCIA E RECONHECIMENTO FACIAL NO BRASIL**

O avanço tecnológico ocorrido nas últimas décadas expandiu significativamente a utilização de mecanismos de vigilância e monitoramento no Brasil, tanto pelo poder público quanto pela iniciativa privada. A expansão de câmeras de segurança em espaços urbanos, transportes públicos, estabelecimentos comerciais e órgãos estatais passou a fazer parte de estratégias voltadas ao controle social, à prevenção da criminalidade e à ampliação da segurança pública. Nesse contexto, o desenvolvimento de tecnologias digitais permitiu maior capacidade de coleta, armazenamento e processamento de dados relacionados à circulação e identificação de indivíduos.

A utilização de sistemas de vigilância ganhou maior relevância no país a partir da intensificação dos processos de urbanização e do avanço das tecnologias de informação. Com o crescimento expressivo dos centros urbanos e o aumento das preocupações relacionadas à violência urbana, políticas públicas começaram a incorporar mecanismos tecnológicos de monitoramento como instrumentos de apoio à atuação estatal. Aos poucos, sistemas de câmeras e centrais integradas de vigilância passaram a ocupar posição estratégica nas políticas de segurança implementadas em diferentes estados brasileiros.

Juntamente ao avanço desses mecanismos, o desenvolvimento da inteligência artificial e da análise automatizada de dados aumentou a capacidade de identificação e rastreamento de indivíduos. Sistemas tecnológicos passaram a operar mediante cruzamento de informações, processamento de imagens e reconhecimento de padrões, possibilitando maior rapidez na identificação de pessoas e no tratamento de grandes volumes de dados. No entanto, a ampliação dessas ferramentas também reforçou debates relacionados à privacidade, à proteção de dados pessoais e aos limites da atuação estatal perante os direitos fundamentais garantidos constitucionalmente.

No Brasil, tais discussões ganharam maior relevância com a consolidação da Lei Geral de Proteção de Dados Pessoais (LGPD), responsável por estabelecer parâmetros para o tratamento de dados pessoais, inclusive por órgãos públicos. A crescente utilização de tecnologias de vigilância começou a exigir reflexões relacionadas à transparência, ao controle do uso de dados biométricos e à necessidade de compatibilização entre segurança pública e garantias fundamentais. Nesse cenário, o uso de mecanismos automatizados de identificação passou a despertar preocupações

ligadas ao monitoramento excessivo da população e à possibilidade de ampliação de práticas discriminatórias já existentes no contexto social brasileiro.

Entre as ferramentas tecnológicas mais utilizadas nesse contexto, destaca-se o reconhecimento facial, sistema que passou a ser gradualmente incorporado em políticas de segurança pública, monitoramento urbano e identificação de indivíduos em espaços públicos. A expansão dessa tecnologia no Brasil aumentou as discussões acerca de sua precisão, funcionamento e impactos sobre direitos fundamentais, especialmente diante da utilização crescente de dados biométricos pelo Estado. Assim, torna-se necessário compreender o conceito e o funcionamento dos sistemas de reconhecimento facial não apenas sob perspectiva tecnológica, mas também a partir de suas repercussões jurídicas. A forma como essas ferramentas realizam processos de identificação, armazenam dados biométricos e produzem resultados automatizados influencia diretamente a atuação estatal, especialmente quando tais informações passam a subsidiar medidas de segurança pública, atividades investigativas e decisões capazes de afetar direitos fundamentais. Por essa razão, a análise dos aspectos técnicos da tecnologia constitui etapa indispensável para a compreensão dos riscos jurídicos e das discussões relativas à responsabilidade do Estado decorrentes de sua utilização.

#### 4.1. CONCEITO E FUNCIONAMENTO DOS SISTEMAS DE RECONHECIMENTO FACIAL

A tecnologia de reconhecimento facial opera por meio de um processo automatizado de análise, processamento e identificação de características biológicas individuais que, longe de configurar um procedimento puramente neutro, constitui o marco zero de potenciais violações de direitos fundamentais no ambiente digital e físico. O ciclo operacional dessa tecnologia se inicia com a captação de imagens em tempo real por meio de câmeras de vigilância ou dispositivos de monitoramento distribuídos pelo espaço público. Uma vez obtida a imagem do transeunte, o software executa a chamada detecção facial, etapa técnica que consiste na localização e no isolamento de um rosto humano dentro do enquadramento da câmera, distinguindo-o de outros elementos do cenário, como veículos, postes e fachadas comerciais (KASPERSKY BRASIL, s.d.).

Na fase subsequente, o sistema avança para o mapeamento facial tridimensional ou bidimensional. O software analisa minuciosamente a geometria da face,

identificando e mensurando os chamados pontos nodais, que englobam a distância entre os olhos, a profundidade das órbitas oculares, o comprimento e largura do nariz, o formato das maçãs do rosto, o contorno da mandíbula e a linha da testa (KASPERSKY BRASIL, s.d.). Esses pontos nodais funcionam como coordenadas geométricas que são processadas por algoritmos de inteligência artificial e convertidas em uma sequência numérica complexa. Esse código matemático final gera a chamada assinatura facial ou vetor biométrico, que serve como a identidade digitalizada daquele indivíduo para o sistema computacional (KASPERSKY BRASIL, s.d.).

Ocorre que essa conversão da identidade humana em vetores matemáticos não constitui um ato puramente objetivo, imune a arbitrariedades. A própria determinação de quais características faciais serão priorizadas pelo código, bem como a calibração dos limiares de assertividade técnicos (thresholds) que definem o quão flexível a máquina será ao considerar duas imagens como sendo da mesma pessoa, derivam de escolhas de programadores e diretrizes políticas e comerciais prévias. Sob a aparente neutralidade da ciência da computação, identificam-se as escolhas técnicas e institucionais que influenciam diretamente os resultados produzidos pelos sistemas: ao delegar a identificação de cidadãos a um padrão estatístico preestabelecido por entes privados, o Estado assume o risco de que inconsistências técnicas sejam incorporadas à atividade policial e influenciam a formação de suspeitas criminais.

Diante disso, constata-se que o processamento dessas características biométricas distancia-se de qualquer ideal de isenção científica ou infalibilidade. Os sistemas de inteligência artificial aplicados à segurança pública brasileira operam sob o fenômeno da opacidade algorítmica, a denominada “caixa preta” (black box), cenário no qual os critérios lógico-dedutivos, os pesos atribuídos às variáveis e as correlações internas que orientaram a decisão da máquina permanecem inacessíveis e inaudíveis pelo próprio poder público contratante e pelo cidadão afetado.

Essa falta de transparência técnica atua como premissa fática indissociável da violação de direitos constitucionais. Quando o aparato estatal adota tecnologia cuja engenharia interna é proprietária e de limitada transparência, cria-se um cenário potencialmente incompatível com garantias processuais fundamentais asseguradas ao cidadão. Fragilizam-se, portanto, garantias fundamentais basilares inscritas no artigo 5º da Constituição Federal de 1988, tais como o devido processo legal, o contraditório, a ampla defesa e o princípio da presunção de inocência, uma vez que se torna virtualmente impossível ao cidadão contestar a lógica de uma máquina que o apontou

como criminoso. Todavia, o risco de lesão a essas garantias não se encerra no mapeamento isolado da face; ele se potencializa drasticamente no momento em que esses dados matemáticos são inseridos na engrenagem de controle do Estado, passando por um processo de emparelhamento com acervos governamentais, fenômeno cuja dinâmica passa a ser descortinada no tópico subsequente.

#### 4.2. IMPLEMENTAÇÃO DE CÂMERAS DE SEGURANÇA COM IA NA SEGURANÇA PÚBLICA BRASILEIRA

Após a modelagem e a geração da assinatura facial pelo sistema de inteligência artificial, a etapa crucial e mais sensível para a persecução penal consiste no cruzamento de dados, momento em que o risco fático de erro tecnológico se transmuta efetivamente em dano jurídico concreto. O vetor numérico recém-gerado a partir da imagem capturada na via pública é transmitido a uma central de processamento e comparado, em frações de segundo, com bancos de dados preexistentes e armazenados pelo Estado. Essas bases governamentais contêm acervos de fotografias de indivíduos com mandados de prisão em aberto, registros de antecedentes criminais ou cadastros civis de ampla escala, como bancos de dados de identificação civil e do Departamento de Trânsito (MARRAFON; SCHIEBERT, 2025).

Caso o algoritmo identifique uma correspondência matemática entre a assinatura capturada na rua e alguma imagem arquivada que atinja ou supere o índice de similaridade pré-configurado, o sistema emite um sinal de alerta automático (match). Esse alerta é enviado aos terminais dos agentes de segurança pública em campo, disparando a ordem de abordagem ostensiva, interceptação e, frequentemente, a condução ou prisão do indivíduo identificado pela máquina (MARRAFON; SCHIEBERT, 2025).

É nesse ponto de interseção técnica e procedimental que a tecnologia se materializa como um poderoso vetor de discriminação institucionalizada. O cruzamento automatizado de imagens não opera em um vácuo de neutralidade social; ele depende diretamente do emparelhamento com bancos de dados criminais que foram gerados ao longo de décadas por um sistema de persecução penal historicamente seletivo, desigual e racista. Consequentemente, o match gerado pelo algoritmo não reflete uma verdade jurídica factual ou uma certeza investigativa, mas sim a reprodução e a ampliação automatizada dos vieses estruturais contidos no próprio acervo histórico de dados

coletados pelo Estado.

Dessa forma, a falha técnica de correspondência, tecnicamente denominada falso positivo, deixa de ser um mero erro computacional estatisticamente aceitável e passa a configurar um ato ilícito estatal quando produz restrição indevida de liberdade ou constrangimento ilegal. Esse fenômeno incide de forma desproporcional sobre peles retintas, em razão da sub-representação e da má calibração dos sistemas, frequentemente treinados e testados em bases de dados de populações eurocêtricas (brancas).

Ao transpor essa tecnologia deficitária para a realidade social brasileira, o erro assume recorte de raça e classe: são homens negros e periféricos os alvos preferenciais dos falsos positivos e dos subsequentes constrangimentos legais e prisões indevidas. Essa violência estatal é perpetuada sob a aparência de modernização e eficiência tecnológica, vulnerabilizando corpos negros e periféricos sob o pretexto de otimização da segurança pública.

Desmistificado o fluxo de funcionamento do reconhecimento facial, resta evidente que o isolamento dos aspectos técnicos em detrimento de suas repercussões jurídicas constitui um equívoco conceitual e metodológico. A engenharia dessas ferramentas de inteligência artificial, marcada pela opacidade de suas decisões, pela assimetria de informações e pela contaminação por vieses estruturais, fornece o substrato fático e empírico que justifica e exige a intervenção do Direito.

Não cabe ao jurista debater a suposta eficiência mercadológica da ferramenta, mas sim reconhecer que sua arquitetura atual pode operar como reprodutora de ilegalidades e constrangimentos direcionados a grupos sociais específicos. Configura-se, assim, o nexo de causalidade entre a atividade tecnológica do Estado, ao implantar sistemas com potenciais vícios na segurança pública, e o dano moral, existencial e social infligido aos indivíduos vulnerabilizados. Essa constatação impõe como resposta jurídica o reconhecimento da responsabilidade civil objetiva da Administração Pública, cuja fundamentação teórica e aplicação prática serão detalhadas no capítulo seguinte.

## **5. DISCRIMINAÇÃO ALGORÍTMICA, ERROS DE IDENTIFICAÇÃO E VIESES NO RECONHECIMENTO FACIAL**

A utilização de sistemas de reconhecimento facial pela segurança pública tem intensificado debates acerca dos impactos da inteligência artificial sobre direitos fundamentais, especialmente no âmbito da persecução penal. Embora frequentemente associados à ideia de precisão técnica e neutralidade operacional, estudos contemporâneos demonstram que tais sistemas apresentam falhas relacionadas à discriminação algorítmica, erros de identificação e vieses estruturais, decorrentes da qualidade dos dados e das escolhas metodológicas envolvidas em seu desenvolvimento (ARAÚJO; CARDOSO; PAULA, 2021; SHAH et al., 2024).

Desde logo, essas limitações não se restringem ao plano técnico, pois são incorporadas à atuação estatal. Assim, o reconhecimento facial não funciona apenas como ferramenta auxiliar, mas como elemento que influencia a formação da suspeita penal e a seleção de alvos de investigação, produzindo efeitos diretos sobre direitos fundamentais. Essa transposição do erro técnico para o ato estatal é o que confere relevância jurídica ao tema.

A discriminação algorítmica manifesta-se, sobretudo, por meio de falsos positivos, nos quais o sistema associa incorretamente indivíduos a registros de bancos de dados. Embora tratados como estatisticamente residuais, esses erros possuem alto impacto jurídico, pois podem fundamentar abordagens policiais e restrições de liberdade, conferindo ao dado tecnológico um peso decisório relevante na prática institucional.

O Conselho Nacional de Justiça aponta que os erros de reconhecimento facial não atingem a população de forma uniforme, havendo incidência desproporcional sobre pessoas negras, o que evidencia a relação entre tais sistemas e desigualdades estruturais já presentes no sistema penal brasileiro (CNJ, 2023; ALMEIDA, 2021). Nesse sentido, a tecnologia não apenas reflete essas desigualdades, mas pode reforçá-las. A contribuição da teoria do racismo estrutural para essa discussão revela-se especialmente relevante, uma vez que, conforme sustenta Almeida (2021), as práticas discriminatórias não decorrem exclusivamente de comportamentos individuais, mas estão inseridas no funcionamento regular das instituições e das estruturas sociais. Desse modo, quando sistemas algorítmicos são treinados a partir de bases de dados produzidas em contextos historicamente marcados pela seletividade penal e pela desigualdade racial, existe o

risco de que tais distorções sejam reproduzidas e potencializadas sob a aparência de neutralidade tecnológica.

Os vieses algorítmicos consistem em padrões sistemáticos de erro decorrentes do treinamento dos sistemas. Um dos principais fatores é a composição desigual dos bancos de dados, frequentemente marcados pela predominância de determinados grupos sociais, o que reduz a precisão do reconhecimento para populações sub-representadas (SHAH et al., 2024). Essa assimetria técnica se converte, na prática, em assimetria decisória, na medida em que determinados grupos passam a estar mais expostos a erros de identificação e às consequências jurídicas deles decorrentes.

Além disso, fatores como baixa qualidade das imagens, condições ambientais e limitações operacionais em tempo real ampliam a taxa de erro dos sistemas, especialmente em contextos de vigilância policial, nos quais a verificação humana é reduzida. Nessas circunstâncias, a confiança excessiva nos resultados produzidos pela tecnologia pode contribuir para o enfraquecimento da análise crítica por parte dos agentes públicos, ampliando o risco de que falhas técnicas sejam incorporadas ao processo de tomada de decisões estatais.

Outro ponto relevante é a opacidade dos sistemas, muitas vezes desenvolvidos por empresas privadas que não divulgam integralmente seus critérios de funcionamento. Essa falta de transparência compromete a auditabilidade e limita o controle externo sobre a confiabilidade dos resultados (MARRAFON; SCHIEBERT, 2025).

Essa opacidade também impacta o plano jurídico, pois dificulta a reconstrução da cadeia causal do erro e limita a capacidade de fiscalização dos critérios utilizados pelos algoritmos. Ainda assim, não afasta a responsabilidade estatal por danos decorrentes da atuação administrativa, nos termos do art. 37, §6º, da Constituição Federal. Ao contrário, a utilização de tecnologias potencialmente lesivas aos direitos fundamentais reforça a necessidade de mecanismos institucionais capazes de assegurar transparência, auditabilidade, supervisão humana e controle permanente dos sistemas empregados pelo poder público.

Diante disso, constata-se que os riscos do reconhecimento facial ultrapassam o plano técnico e alcançam o exercício do poder punitivo estatal. A falha algorítmica, quando incorporada à atuação policial, deixa de ser uma falha puramente computacional e se converte em questão jurídico-constitucional, por afetar a formação da suspeita penal, a confiabilidade da prova e a legitimidade das decisões estatais.

Por essa razão, os vieses, erros de identificação e a opacidade dos sistemas não apenas comprometem a precisão tecnológica, mas tensionam diretamente direitos fundamentais, ao introduzirem incerteza estrutural em decisões que afetam a liberdade individual. Diante desse cenário, torna-se indispensável a construção de parâmetros normativos e mecanismos de controle capazes de compatibilizar a utilização da inteligência artificial com as garantias constitucionais que limitam o exercício do poder estatal. É a partir dessa perspectiva que se impõe a análise, no capítulo seguinte, dos direitos fundamentais impactados pelo uso do reconhecimento facial.



## **6. DIREITOS FUNDAMENTAIS AFETADOS PELO RECONHECIMENTO FACIAL**

Os impactos do uso de sistemas de reconhecimento facial na segurança pública ultrapassam o plano estritamente técnico e alcançam diretamente a esfera de proteção dos direitos fundamentais. Isso ocorre porque a incorporação de inferências algorítmicas à atuação estatal interfere na forma como se constroem suspeitas, se direcionam investigações e se fundamentam decisões que podem restringir a liberdade individual, especialmente no âmbito da persecução penal.

Nesse cenário, o direito à liberdade é um dos primeiros a ser afetado, uma vez que erros de identificação podem resultar em abordagens policiais, conduções e até prisões indevidas. Os chamados falsos positivos evidenciam que a correspondência algorítmica não possui caráter absoluto de precisão, podendo vincular equivocadamente indivíduos a registros constantes em bancos de dados biométricos ou criminais (SHAH et al., 2024). Quando incorporados pela atuação estatal, esses resultados deixam de ser meramente probabilísticos e passam a produzir efeitos concretos sobre a restrição de direitos.

Associada a essa questão, a presunção de inocência também é tensionada, na medida em que o indivíduo passa a ser submetido a intervenções estatais com base em inferências tecnológicas que não equivalem, por si só, a prova robusta de autoria ou materialidade. Essa dinâmica altera, na prática, a lógica tradicional do processo penal, pois antecipa a formação da suspeita a partir de um juízo automatizado, enfraquecendo a exigência constitucional de fundamentação concreta para restrições de liberdade. Sob essa ótica, a utilização de resultados algorítmicos como elemento central para justificar intervenções estatais exige cautela redobrada, uma vez que a presunção de inocência impõe ao Estado o dever de demonstrar a responsabilidade do investigado por meio de elementos probatórios idôneos, não sendo compatível com a atribuição de presunção de veracidade absoluta a inferências produzidas por sistemas automatizados.

A preocupação assume especial relevância diante do disposto no artigo 5º, inciso LVII, da Constituição Federal, segundo o qual ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória. Embora o reconhecimento facial não produza, por si só, uma declaração de culpabilidade, sua utilização como elemento determinante para a formação da suspeita criminal pode gerar efeitos práticos incompatíveis com a lógica protetiva da presunção de inocência. Isso ocorre porque a

correspondência biométrica produzida pelo algoritmo tende a ser percebida pelos agentes responsáveis pela persecução penal como indicativo objetivo de autoria (SHAH et al., 2024). Nessas circunstâncias, o risco não reside apenas na possibilidade de identificações equivocadas, mas também na atribuição de excessiva confiança a resultados tecnológicos que demandam constante verificação e contextualização por parte dos agentes públicos responsáveis pela persecução penal.

O devido processo legal também sofre impactos relevantes, especialmente em sua dimensão substancial. A utilização de sistemas opacos compromete a racionalidade das decisões estatais, na medida em que os critérios de funcionamento dos algoritmos não são plenamente acessíveis às partes envolvidas. A doutrina aponta que essa ausência de transparência limita o controle jurisdicional e dificulta a verificação da confiabilidade dos resultados utilizados na persecução penal (MARRAFON; SCHIEBERT, 2025).

Sob essa perspectiva, o devido processo legal não se limita à observância formal de procedimentos previamente estabelecidos, abrangendo também a exigência de racionalidade, transparência e controle dos atos praticados pelo Estado. A utilização de mecanismos decisórios cuja lógica de funcionamento permanece inacessível ou insuficientemente compreendida dificulta a fiscalização da legalidade das medidas adotadas e compromete a legitimidade das intervenções fundamentadas em resultados algorítmicos. Em um Estado Democrático de Direito, a restrição de direitos fundamentais exige não apenas fundamento jurídico válido, mas também a possibilidade de controle e verificação dos elementos utilizados para justificar a atuação estatal.

Nesse mesmo sentido, o contraditório e a ampla defesa são enfraquecidos pela assimetria informacional entre acusação e defesa. A ausência de acesso aos dados de treinamento, aos critérios de validação e às taxas de erro dos sistemas impede a contestação técnica efetiva da prova algorítmica, comprometendo a paridade de armas no processo penal.

A efetividade do contraditório pressupõe que a defesa tenha acesso aos elementos necessários para compreender e impugnar os fundamentos da acusação. Entretanto, a opacidade que caracteriza muitos sistemas de reconhecimento facial dificulta a identificação dos critérios empregados para a produção dos resultados apresentados como elemento probatório. Conforme observam Marrafon e Schiebert (2024), a limitação da auditabilidade algorítmica compromete a transparência necessária

ao controle dos dados e processos utilizados por essas tecnologias. Como consequência, a defesa pode encontrar obstáculos significativos para contestar a confiabilidade da identificação realizada, situação que enfraquece a concretização material das garantias previstas no artigo 5º, inciso LV, da Constituição Federal.

Outro direito fundamental diretamente afetado é a dignidade da pessoa humana. A exposição indevida a abordagens, investigações e outras intervenções promovidas pelo Estado com fundamento em identificações equivocadas pode gerar estigmatização, constrangimento e reforço de estereótipos sociais. Nessa hipótese, a lesão aos direitos fundamentais não decorre do funcionamento isolado da tecnologia, mas da incorporação de seus resultados à atuação estatal sem mecanismos adequados de verificação, supervisão e controle (CNJ, 2023; ALMEIDA, 2021).

A relevância da dignidade da pessoa humana nesse contexto decorre do fato de que ela constitui fundamento da República Federativa do Brasil, nos termos do artigo 1º, inciso III, da Constituição Federal. Por essa razão, a atuação estatal não pode reduzir o indivíduo à condição de mero objeto de classificação tecnológica ou de tratamento automatizado de dados. Ainda que empregados com a finalidade legítima de promoção da segurança pública, os sistemas de reconhecimento facial devem permanecer compatíveis com a proteção da autonomia individual, da igualdade material e do respeito à condição humana, evitando a reprodução de padrões discriminatórios historicamente presentes nas estruturas sociais e institucionais brasileiras (ALMEIDA, 2021).

Além disso, a utilização dessas tecnologias impacta a própria exigência de controle e motivação das decisões estatais. A chamada “autoridade técnica” do algoritmo tende a ser incorporada como justificativa implícita de veracidade, reduzindo o grau de escrutínio humano sobre atos de persecução penal e enfraquecendo o dever de fundamentação das intervenções estatais. Nessas circunstâncias, o risco jurídico não decorre apenas da falibilidade tecnológica, mas da possibilidade de que o Estado transfira, ainda que parcialmente, a fundamentação de suas decisões para mecanismos cuja lógica de funcionamento não se encontra plenamente sujeita ao escrutínio democrático e jurisdicional.

Dessa forma, verifica-se que os efeitos do reconhecimento facial não se limitam à esfera operacional da segurança pública, mas atingem diretamente o núcleo de proteção dos direitos fundamentais. A tecnologia, quando utilizada sem transparência adequada e sem mecanismos efetivos de controle, passa a integrar a própria estrutura de

tomada de decisão estatal, influenciando concretamente a forma como a liberdade é restringida e como as garantias processuais são asseguradas.

A análise conjunta dessas garantias demonstra que os riscos associados ao reconhecimento facial não decorrem exclusivamente da possibilidade de erros técnicos isolados. O problema constitucional revela-se mais amplo e está relacionado à crescente incorporação de processos automatizados ao exercício do poder punitivo estatal. Quando sistemas algorítmicos passam a influenciar a seleção de suspeitos, a produção de elementos informativos e a adoção de medidas potencialmente restritivas de direitos, torna-se indispensável verificar sua compatibilidade com os limites impostos pela Constituição Federal. Os direitos fundamentais analisados atuam, como verdadeiros mecanismos de contenção do poder estatal, impedindo que a busca por eficiência tecnológica resulte na relativização das garantias que estruturam o processo penal democrático. A observância dessas garantias mostra-se ainda mais necessária quando os resultados produzidos pelos sistemas são incorporados à atividade estatal e utilizados como fundamento para intervenções potencialmente restritivas de direitos fundamentais.

Nesse sentido, a análise dos direitos fundamentais afetados evidencia que o problema não se esgota na identificação de falhas técnicas ou vieses algorítmicos. Sob a perspectiva jurídica, a principal preocupação não reside na mera existência da tecnologia, mas na decisão estatal de incorporá-la à persecução penal e utilizar seus resultados como fundamento para intervenções potencialmente restritivas de direitos sem mecanismos suficientes de transparência, controle e supervisão. Por essa razão, torna-se necessário avançar para a discussão acerca da responsabilidade do Estado e dos limites jurídicos ao uso dessas tecnologias, a fim de delimitar em que medida o poder público pode empregar sistemas automatizados na persecução penal sem violar os parâmetros constitucionais de proteção aos direitos fundamentais.

## **7. RESPONSABILIDADE DO ESTADO E LIMITES AO USO DA TECNOLOGIA**

A ampliação do uso de tecnologias de reconhecimento facial na segurança pública brasileira intensificou debates relacionados aos limites jurídicos da atuação estatal diante da incorporação de sistemas automatizados de vigilância, identificação e monitoramento populacional. O avanço dessas ferramentas demonstrou que a utilização de inteligência artificial pelo poder público não pode ser analisada exclusivamente sob perspectiva operacional ou administrativa, sobretudo porque o exercício da atividade estatal permanece submetido aos princípios constitucionais que limitam o poder de intervenção do Estado sobre os indivíduos.

No contexto da segurança pública, a utilização de mecanismos automatizados de identificação produz impactos que ultrapassam questões relacionadas à eficiência tecnológica. O reconhecimento facial passou a integrar atividades de policiamento, monitoramento urbano e persecução penal, influenciando procedimentos investigativos e medidas de controle social exercidas pelo Estado. Diante disso, o debate jurídico relacionado a essas tecnologias passou a envolver não apenas a legitimidade de sua utilização, mas também os parâmetros necessários para limitar abusos e assegurar compatibilidade entre inovação tecnológica e garantias constitucionais.

Embora o ordenamento jurídico brasileiro não possua legislação específica destinada exclusivamente à regulamentação do reconhecimento facial, a atuação estatal permanece condicionada aos princípios constitucionais da legalidade, proporcionalidade, finalidade administrativa e proteção dos direitos fundamentais. Isso significa que a utilização de ferramentas biométricas pelo poder público exige observância de limites jurídicos relacionados à transparência, necessidade, adequação e controle da atividade estatal.

A ausência de regulamentação específica sobre sistemas de reconhecimento facial intensifica parte dessas discussões. Atualmente, não existem critérios nacionais uniformes acerca da implementação dessas ferramentas, dos parâmetros mínimos de confiabilidade tecnológica, dos mecanismos obrigatórios de auditoria independente ou dos limites relacionados ao armazenamento e compartilhamento de dados biométricos pela administração pública. Como consequência, diferentes órgãos estatais passaram a utilizar tecnologias automatizadas de identificação sem padronização normativa suficiente acerca dos mecanismos de fiscalização e controle externo.

Nesse cenário, a utilização de sistemas algorítmicos pela administração pública exige reflexão acerca da própria delegação de decisões potencialmente sensíveis a mecanismos automatizados. Ainda que o reconhecimento facial seja frequentemente apresentado como ferramenta auxiliar de segurança pública, a influência produzida pelos resultados algorítmicos sobre abordagens policiais, procedimentos investigatórios e medidas de vigilância demonstra que essas tecnologias passaram a exercer papel relevante na formação de decisões estatais capazes de impactar diretamente direitos individuais.

A problemática torna-se mais complexa diante da limitada transparência dos sistemas utilizados pelo poder público. Grande parte das tecnologias biométricas empregadas em atividades de segurança pública é desenvolvida por empresas privadas que não divulgam integralmente os critérios internos utilizados pelos algoritmos para realização das correspondências faciais. Essa limitação reduz a possibilidade de fiscalização independente acerca da confiabilidade dos sistemas, dificultando a verificação dos parâmetros utilizados durante os processos automatizados de identificação.

Conforme aponta o CNJ (2023), a opacidade algorítmica interfere diretamente no controle democrático da atividade estatal. A ausência de informações claras sobre funcionamento, treinamento e margem de erro dos sistemas biométricos compromete a possibilidade de acompanhamento social acerca da forma como essas tecnologias são utilizadas pelo poder público. Em um cenário de expansão da vigilância digital, a inexistência de mecanismos adequados de controle institucional amplia riscos relacionados à utilização desproporcional ou inadequada dessas ferramentas.

Além disso, a utilização de tecnologias automatizadas na segurança pública exige observância de critérios relacionados à necessidade e proporcionalidade da intervenção estatal. O simples avanço tecnológico não autoriza ampliação irrestrita da capacidade de monitoramento do Estado sobre a população. Conforme observam Araújo, Cardoso e Paula (2021), a implementação de sistemas biométricos deve ser acompanhada de justificativas legítimas relacionadas à finalidade da medida, aos limites de utilização das informações coletadas e à existência de mecanismos capazes de reduzir riscos de abusos e violações de direitos fundamentais.

A discussão relacionada aos limites jurídicos do reconhecimento facial também envolve a necessidade de fortalecimento de mecanismos institucionais de fiscalização e responsabilização estatal. A utilização de inteligência artificial pela administração

pública exige controle contínuo acerca da confiabilidade dos sistemas empregados, da segurança dos bancos de dados utilizados e da compatibilidade entre os mecanismos tecnológicos de vigilância e os parâmetros constitucionais aplicáveis à atuação estatal.

A utilização do reconhecimento facial pelo poder público demonstra que o avanço tecnológico precisa ser acompanhado por mecanismos jurídicos capazes de limitar arbitrariedades, assegurar transparência institucional e compatibilizar inovação tecnológica com garantias fundamentais asseguradas pelo Estado Democrático de Direito. A incorporação dessas ferramentas às atividades de segurança pública também amplia discussões acerca das consequências produzidas por falhas decorrentes da atuação estatal mediada por sistemas automatizados, especialmente quando erros de identificação resultam em constrangimentos, abordagens indevidas ou restrições injustificadas de direitos individuais. Nesse contexto, a incorporação de tecnologias de reconhecimento facial à atividade estatal demonstra que o avanço tecnológico não elimina a necessidade de observância dos limites constitucionais impostos ao exercício do poder público. Ao contrário, quanto maior a capacidade de intervenção proporcionada pelas ferramentas tecnológicas, maior deve ser o nível de controle jurídico destinado à proteção dos direitos individuais.

#### 7.1. RESPONSABILIDADE CIVIL DO ESTADO POR ERROS DE IDENTIFICAÇÃO

A utilização de sistemas de reconhecimento facial pelo poder público passou a ampliar discussões relacionadas à responsabilidade estatal pelos danos decorrentes de falhas produzidas durante processos automatizados de identificação. No contexto da segurança pública, a incorporação dessas tecnologias às atividades de vigilância e persecução penal fez surgir situações em que indivíduos passaram a ser submetidos a abordagens policiais, constrangimentos e investigações motivadas por correspondências biométricas posteriormente consideradas equivocadas. Diante disso, o debate jurídico deixou de envolver apenas a legitimidade do uso da tecnologia e passou a alcançar as consequências produzidas pelos erros decorrentes da atuação estatal mediada por sistemas algorítmicos.

A responsabilidade civil do Estado encontra fundamento no artigo 37, §6º, da Constituição Federal (BRASIL, 1988), segundo o qual as pessoas jurídicas de direito público respondem pelos danos que seus agentes causarem a terceiros no exercício da

função administrativa. No âmbito da utilização do reconhecimento facial, essa responsabilização assume relevância diante da possibilidade de falhas produzidas por mecanismos tecnológicos empregados diretamente pelo poder público em atividades relacionadas à segurança e controle social.

A aplicação desse dispositivo constitucional ao contexto do reconhecimento facial demonstra que a adoção de sistemas tecnológicos não afasta os deveres jurídicos impostos à Administração Pública. A conclusão decorre da própria lógica do regime constitucional de responsabilidade objetiva. O artigo 37, §6º, da Constituição Federal não condiciona o dever de indenizar à demonstração de culpa administrativa, bastando a comprovação da conduta estatal, do dano e do nexo causal. Assim, quando a utilização de sistemas de reconhecimento facial resultar em abordagens indevidas, constrangimentos ilegais, prisões equivocadas ou outras formas de lesão a direitos fundamentais, a circunstância de o dano ter sido produzido por mecanismos automatizados não possui aptidão para romper a imputação jurídica ao Estado. A tecnologia não substitui a atuação administrativa; ao contrário, constitui instrumento por ela escolhido e incorporado ao exercício da função pública.

A análise da responsabilidade estatal nesse contexto, contudo, não pode ser dissociada da realidade social na qual essas tecnologias são implementadas. Conforme sustenta Almeida (2021), o racismo estrutural não se manifesta apenas por meio de condutas individuais discriminatórias, mas integra o funcionamento regular das instituições e das estruturas de poder da sociedade. Essa compreensão possui relevância direta para o debate acerca da discriminação algorítmica, sobretudo quando observada em conjunto com os dados apresentados pelo Conselho Nacional de Justiça (2023), que apontam a incidência desproporcional de erros de reconhecimento facial sobre pessoas negras. Desse modo, quando o Estado utiliza tecnologias potencialmente capazes de reproduzir ou intensificar desigualdades já presentes na dinâmica institucional, a discussão sobre responsabilidade civil deixa de envolver exclusivamente falhas técnicas isoladas e passa a abranger os riscos decorrentes da própria utilização de ferramentas que podem reforçar padrões discriminatórios historicamente consolidados. Sob essa perspectiva, a discriminação algorítmica não pode ser compreendida como fenômeno exclusivamente tecnológico. Quando o poder público incorpora sistemas capazes de reproduzir padrões discriminatórios historicamente presentes na estrutura social brasileira, assume igualmente o dever jurídico de prevenir, fiscalizar e reparar os danos decorrentes de sua utilização. A omissão estatal diante dos riscos conhecidos



relacionados à incidência desproporcional de erros sobre determinados grupos sociais reforça a necessidade de responsabilização compatível com os princípios constitucionais da igualdade, da dignidade da pessoa humana e da proteção dos direitos fundamentais.

Embora os sistemas biométricos sejam frequentemente apresentados como instrumentos de apoio técnico às atividades policiais, a utilização dessas ferramentas integra a própria atuação administrativa estatal. Isso significa que os danos decorrentes de erros de identificação realizados por mecanismos automatizados não podem ser tratados como falhas exclusivamente tecnológicas ou desvinculadas da responsabilidade do poder público. A adoção de sistemas de inteligência artificial pela administração pública pressupõe dever de cautela relacionado à escolha das ferramentas utilizadas, à fiscalização de sua confiabilidade e ao acompanhamento dos riscos produzidos por sua aplicação prática. A circunstância de a identificação inicial ser produzida por mecanismo automatizado não altera a natureza estatal da atividade desempenhada, nem afasta os deveres constitucionais de proteção dos direitos fundamentais que recaem sobre a Administração Pública.

Os erros de identificação decorrentes do reconhecimento facial podem produzir consequências significativas sobre a esfera jurídica dos indivíduos afetados. Nessas hipóteses, a ocorrência do dano não decorre de atuação exclusivamente individual dos agentes públicos, mas da própria estrutura tecnológica incorporada à atividade estatal. Por essa razão, os prejuízos causados por identificações equivocadas devem ser analisados à luz do regime constitucional de responsabilidade objetiva, considerando que a atividade administrativa permanece sendo exercida pelo Estado, ainda que mediada por sistemas de inteligência artificial.

A problemática torna-se ainda mais complexa diante da dificuldade de compreensão técnica dos próprios sistemas utilizados pelo Estado. A existência de limitações relacionadas à transparência dos algoritmos não pode servir como fundamento para afastar ou reduzir a responsabilidade estatal. Ao decidir incorporar sistemas tecnológicos à sua atuação administrativa, cabe ao poder público assegurar níveis adequados de auditabilidade, fiscalização e controle capazes de garantir a identificação das causas dos eventuais erros produzidos pelos mecanismos automatizados.

Além disso, a responsabilidade do Estado não se limita aos casos de falha direta do sistema tecnológico. A utilização inadequada dos resultados produzidos pelos

algoritmos também pode contribuir para violações de direitos individuais. Correspondências biométricas realizadas por sistemas automatizados não representam prova absoluta de identidade e exigem verificação humana adequada antes da adoção de medidas restritivas de direitos. A ausência de protocolos rigorosos de conferência e validação das informações produzidas pelos sistemas de reconhecimento facial pode intensificar riscos relacionados à atuação estatal arbitrária ou desproporcional. Essa circunstância demonstra que a responsabilidade estatal não está relacionada apenas à existência de falhas tecnológicas, mas também à forma como os resultados produzidos pelos sistemas são utilizados pelos agentes públicos. A supervisão humana adequada constitui requisito indispensável para reduzir riscos de violações a direitos fundamentais e preservar a legitimidade da atuação administrativa.

No âmbito da administração pública, a incorporação de tecnologias automatizadas exige observância de deveres relacionados à prevenção de danos e à adoção de mecanismos de controle compatíveis com os riscos produzidos pelas ferramentas utilizadas. Isso envolve não apenas avaliação prévia acerca da confiabilidade dos sistemas biométricos empregados, mas também monitoramento contínuo de sua utilização prática, treinamento adequado dos agentes responsáveis pela operação das tecnologias e implementação de procedimentos destinados à redução de falhas de identificação.

Sob essa perspectiva, a responsabilidade civil do Estado não deve ser compreendida apenas como mecanismo de reparação posterior ao dano. No contexto da incorporação da inteligência artificial às atividades de segurança pública, ela também assume função preventiva, impondo ao poder público o dever de adotar medidas destinadas à redução dos riscos inerentes à utilização dessas tecnologias. Isso envolve a adoção de mecanismos de transparência, fiscalização e controle compatíveis com a complexidade dos sistemas empregados, bem como a realização de avaliações permanentes acerca de sua confiabilidade e dos riscos produzidos por sua aplicação prática. Tais medidas mostram-se especialmente relevantes diante das limitações relacionadas à opacidade algorítmica e à possibilidade de ocorrência de erros capazes de afetar direitos fundamentais dos indivíduos submetidos a esses mecanismos de identificação (MARRAFON; SCHIEBERT, 2025).

As discussões relacionadas à responsabilidade estatal também envolvem a necessidade de definição de parâmetros jurídicos acerca da utilização de inteligência artificial em atividades de segurança pública. A ausência de regulamentação específica

sobre reconhecimento facial no Brasil contribui para insegurança relacionada aos critérios de fiscalização, controle e responsabilização aplicáveis aos danos decorrentes da utilização dessas ferramentas. Como consequência, o debate jurídico passou a exigir maior atenção acerca dos limites da delegação de funções potencialmente sensíveis a mecanismos automatizados de tomada de decisão.

Nesse contexto, a responsabilização civil do Estado assume função relevante não apenas na reparação dos danos causados aos indivíduos afetados, mas também como instrumento de controle da própria atuação administrativa. A possibilidade de responsabilização estatal contribui para reforçar a necessidade de maior cautela na implementação de sistemas biométricos e incentiva o desenvolvimento de mecanismos institucionais voltados à fiscalização da atividade tecnológica exercida pelo poder público.

A responsabilidade estatal discutida neste trabalho não decorre da simples existência de sistemas de reconhecimento facial, mas da decisão administrativa de incorporá-los à atividade de segurança pública, mesmo diante de riscos conhecidos relacionados a erros de identificação, opacidade algorítmica e reprodução de padrões discriminatórios. Ao optar pela utilização dessas ferramentas como instrumento de apoio à persecução penal, o Estado assume o dever de garantir que sua aplicação ocorra em conformidade com os parâmetros constitucionais de proteção aos direitos fundamentais. Dessa forma, eventuais danos decorrentes da utilização inadequada ou insuficientemente controlada desses sistemas permanecem juridicamente imputáveis ao poder público, que não pode transferir à tecnologia a responsabilidade pelas consequências de sua própria atuação administrativa.

Diante do exposto, verifica-se que a utilização de sistemas de reconhecimento facial pelo poder público não afasta os deveres constitucionais de proteção dos direitos fundamentais nem reduz a incidência do regime de responsabilidade civil do Estado previsto no artigo 37, §6º, da Constituição Federal. Ao contrário, a possibilidade de ocorrência de danos decorrentes de erros de identificação, falhas algorítmicas e utilização inadequada dos resultados produzidos pelos sistemas automatizados reforça a necessidade de controle rigoroso da atividade tecnológica estatal. Mais do que responder a falhas pontuais, a responsabilidade estatal deve ser compreendida como instrumento de proteção dos cidadãos diante dos riscos produzidos pela utilização de tecnologias que, em determinados contextos, podem contribuir para a reprodução de desigualdades já existentes. Nesse cenário, a responsabilização civil assume função não

apenas reparatória, mas também preventiva, contribuindo para a adoção de práticas administrativas mais transparentes, seguras e compatíveis com os princípios do Estado Democrático de Direito.

## 7.2. DEVIDO PROCESSO LEGAL E USO DE TECNOLOGIAS NA PERSECUÇÃO PENAL

A incorporação de tecnologias de reconhecimento facial às atividades de persecução penal ampliou discussões relacionadas à compatibilidade entre mecanismos automatizados de identificação e as garantias processuais asseguradas pelo ordenamento jurídico brasileiro. A utilização de sistemas biométricos em investigações criminais e atividades de segurança pública passou a levantar questionamentos acerca da forma como informações produzidas por algoritmos podem influenciar procedimentos investigativos, medidas restritivas de direitos e formação de elementos probatórios no âmbito penal.

O devido processo legal, previsto no artigo 5º, inciso LIV, da Constituição Federal, constitui uma das principais garantias limitadoras da atuação estatal no exercício do poder punitivo. Sua aplicação exige que procedimentos investigativos e processuais observem parâmetros relacionados à legalidade, transparência, contraditório, ampla defesa e preservação da presunção de inocência. Nesse contexto, a utilização de tecnologias automatizadas pelo Estado não afasta a necessidade de observância dessas garantias constitucionais, ainda que os sistemas empregados sejam apresentados como instrumentos de apoio técnico às atividades investigativas.

A crescente utilização do reconhecimento facial em atividades de persecução penal intensificou debates acerca da confiabilidade das informações produzidas pelos sistemas biométricos. Embora essas ferramentas sejam frequentemente utilizadas para auxiliar processos de identificação de suspeitos e localização de indivíduos, os resultados produzidos pelos algoritmos não possuem caráter absoluto e dependem de múltiplos fatores relacionados à qualidade das imagens, atualização dos bancos de dados e critérios estatísticos utilizados durante as correspondências faciais.

Nesse cenário, um dos principais debates jurídicos envolve o valor probatório atribuído ao reconhecimento facial no âmbito penal. A utilização de correspondências biométricas como fundamento para medidas investigativas ou decisões estatais exige cautela, sobretudo porque os sistemas automatizados operam a partir de probabilidades

estatísticas e não de mecanismos infalíveis de identificação. A transformação de resultados algorítmicos em elementos probatórios sem verificação adequada pode comprometer garantias fundamentais relacionadas à segurança jurídica e à presunção de inocência. Sob a perspectiva constitucional, o problema não reside na mera utilização de ferramentas tecnológicas como instrumentos auxiliares de investigação, mas na possibilidade de que resultados produzidos por sistemas automatizados sejam incorporados à atividade estatal sem o nível de controle exigido pelas garantias processuais. Quando correspondências biométricas passam a fundamentar abordagens, investigações ou medidas potencialmente restritivas de direitos sem adequada validação, surge o risco de violação ao devido processo legal e de comprometimento da legitimidade da atuação estatal no exercício do poder punitivo.

A problemática torna-se ainda mais relevante diante da tendência de atribuição de elevada credibilidade às informações produzidas por sistemas tecnológicos. Em muitos casos, a aparência de neutralidade técnica dos algoritmos contribui para fortalecimento da confiança institucional nos resultados automatizados, reduzindo questionamentos acerca das limitações dos sistemas utilizados. No entanto, a utilização de ferramentas de inteligência artificial no processo penal exige análise crítica permanente acerca da confiabilidade das informações produzidas e dos riscos decorrentes da adoção acrítica de mecanismos tecnológicos de identificação.

Além disso, a utilização do reconhecimento facial na persecução penal produz impactos relevantes sobre o exercício do contraditório e da ampla defesa. A possibilidade de contestação efetiva da prova depende do acesso às informações relacionadas ao funcionamento dos sistemas utilizados, aos critérios empregados durante as correspondências biométricas e às condições em que ocorreu a coleta das imagens analisadas. Sem acesso adequado a esses elementos, torna-se limitada a capacidade defensiva de questionar a confiabilidade técnica dos resultados produzidos pelos algoritmos. Essa limitação assume relevância ainda maior quando se considera que o contraditório e a ampla defesa constituem garantias dirigidas precisamente à contenção do poder estatal. A impossibilidade de contestação efetiva dos elementos utilizados para justificar intervenções investigativas ou processuais cria cenário de desequilíbrio incompatível com a lógica constitucional do processo penal democrático, na medida em que dificulta o controle da própria atuação estatal.

A opacidade presente em muitos sistemas de reconhecimento facial intensifica essa dificuldade. Grande parte das tecnologias utilizadas pelo poder público é

desenvolvida por empresas privadas que não divulgam integralmente os parâmetros internos de funcionamento dos algoritmos. Essa limitação compromete a transparência da atividade probatória e dificulta o exercício pleno do contraditório, especialmente quando a defesa não possui acesso aos dados necessários para verificação da confiabilidade das correspondências biométricas utilizadas na investigação ou no processo penal.

Outro aspecto relevante refere-se à necessidade de preservação da cadeia de custódia digital das informações utilizadas pelos sistemas biométricos. A utilização de imagens faciais em atividades investigativas exige controle rigoroso acerca da origem, armazenamento, manipulação e tratamento dos dados analisados durante os processos automatizados de identificação. A ausência de mecanismos adequados de rastreabilidade compromete a confiabilidade da prova digital e amplia riscos relacionados à utilização indevida ou alteração das informações processadas pelos sistemas tecnológicos.

A preservação da cadeia de custódia assume importância ainda maior diante da natureza sensível dos dados biométricos utilizados pelo reconhecimento facial. A integridade das imagens analisadas, a autenticidade das informações armazenadas e a segurança dos bancos de dados utilizados constituem elementos fundamentais para garantir confiabilidade mínima aos procedimentos de identificação realizados por mecanismos automatizados.

Além disso, a utilização dessas tecnologias na persecução penal exige supervisão humana efetiva durante a interpretação dos resultados produzidos pelos sistemas biométricos. O reconhecimento facial não pode substituir integralmente a atividade investigativa ou a análise crítica realizada pelas autoridades responsáveis pela persecução penal. Correspondências algorítmicas devem ser tratadas como elementos auxiliares de investigação, submetidos à verificação posterior e à análise contextualizada das circunstâncias do caso concreto. A exigência de supervisão humana não representa mera cautela operacional, mas verdadeiro imperativo jurídico decorrente das garantias constitucionais que limitam o exercício do poder punitivo. A transferência irrestrita da formação de juízos investigativos para sistemas automatizados enfraqueceria a responsabilidade dos agentes públicos pela fundamentação de seus atos e comprometeria o dever estatal de assegurar decisões compatíveis com os direitos fundamentais.

A centralidade da supervisão humana decorre justamente da necessidade de impedir que decisões potencialmente restritivas de direitos sejam fundamentadas exclusivamente em resultados automatizados produzidos por sistemas cuja confiabilidade não pode ser considerada absoluta. O exercício do poder punitivo estatal exige fundamentação compatível com as garantias processuais constitucionais, circunstância que impede transferência irrestrita de decisões relevantes para mecanismos algorítmicos de identificação.

As discussões relacionadas ao devido processo legal no contexto da utilização de inteligência artificial demonstram que a modernização tecnológica da persecução penal não elimina a necessidade de fortalecimento das garantias jurídicas aplicáveis à atuação estatal. Ao contrário, a ampliação do uso de tecnologias automatizadas exige desenvolvimento de parâmetros normativos capazes de disciplinar os limites da utilização dessas ferramentas, os critérios de controle institucional e os mecanismos de fiscalização necessários à preservação das garantias processuais fundamentais no âmbito penal. Nessa perspectiva, a observância do devido processo legal no contexto da utilização de tecnologias de reconhecimento facial não constitui obstáculo à modernização da segurança pública, mas condição indispensável para que a atuação estatal permaneça compatível com os limites constitucionais impostos ao exercício do poder punitivo.

### 7.3. NECESSIDADE DE REGULAÇÃO E CONTROLE ESTATAL

A crescente utilização de sistemas de reconhecimento facial pelo poder público evidencia a necessidade de estabelecimento de parâmetros jurídicos específicos capazes de compatibilizar a inovação tecnológica com a proteção dos direitos fundamentais. A discussão acerca da regulação dessas ferramentas não decorre apenas do avanço tecnológico observado na segurança pública, mas principalmente dos riscos jurídicos associados à utilização de mecanismos automatizados em atividades potencialmente restritivas de direitos.

Em um Estado Democrático de Direito, a atuação administrativa encontra limites impostos pela Constituição Federal e não pode ser orientada exclusivamente por critérios de eficiência ou conveniência tecnológica. A incorporação de sistemas de reconhecimento facial à persecução penal exige observância dos princípios da legalidade, proporcionalidade, transparência, motivação e proteção dos direitos

fundamentais, especialmente porque os resultados produzidos por essas ferramentas podem influenciar decisões capazes de afetar diretamente a liberdade dos indivíduos.

A necessidade de regulação revela-se ainda mais relevante diante da possibilidade de ocorrência de erros de identificação, opacidade algorítmica e reprodução de padrões discriminatórios já presentes na estrutura social brasileira. Conforme discutido nos capítulos anteriores, tais riscos não permanecem restritos ao plano tecnológico, mas podem resultar em violações concretas de direitos fundamentais quando os resultados produzidos pelos sistemas são incorporados à atuação estatal sem mecanismos adequados de fiscalização e controle.

Nesse contexto, a regulação deve ser compreendida como instrumento de contenção do poder estatal. A definição de critérios jurídicos claros para utilização do reconhecimento facial permite delimitar os deveres impostos à Administração Pública e estabelecer parâmetros para a aferição da legalidade de sua atuação. Mais do que disciplinar aspectos técnicos da tecnologia, a regulamentação busca assegurar que a atividade estatal permaneça submetida aos limites constitucionais que regem o exercício do poder público.

A observância do devido processo legal, do contraditório, da ampla defesa, da presunção de inocência e da dignidade da pessoa humana exige que informações produzidas por sistemas automatizados não sejam tratadas como elementos dotados de presunção absoluta de veracidade. A utilização dessas ferramentas deve permanecer sujeita à supervisão humana, à possibilidade de contestação e ao controle jurisdicional, de modo a impedir que decisões potencialmente restritivas de direitos sejam fundamentadas exclusivamente em resultados algorítmicos.

Além disso, a existência de mecanismos de controle institucional mostra-se indispensável para garantir transparência, rastreabilidade e fiscalização da atividade tecnológica exercida pelo Estado. A ausência de instrumentos capazes de verificar a confiabilidade dos sistemas utilizados dificulta a identificação de falhas, compromete a proteção dos direitos fundamentais e enfraquece os mecanismos de responsabilização aplicáveis aos danos eventualmente causados aos cidadãos.

Sob a perspectiva da responsabilidade civil do Estado, a regulação assume função preventiva de especial relevância. Ao estabelecer critérios objetivos para implementação, utilização e fiscalização dessas tecnologias, o ordenamento jurídico contribui para redução dos riscos inerentes à atividade estatal e fortalece a proteção dos indivíduos submetidos aos mecanismos de identificação biométrica. Dessa forma, a



regulamentação não se destina apenas à organização da atividade administrativa, mas também à prevenção de violações de direitos fundamentais e à redução da ocorrência de danos juridicamente indenizáveis.

Portanto, a necessidade de regulação do reconhecimento facial decorre da própria exigência constitucional de limitação e controle do poder estatal. Em um cenário marcado pela crescente incorporação de tecnologias automatizadas à segurança pública, a proteção dos direitos fundamentais exige que a utilização dessas ferramentas ocorra dentro de parâmetros jurídicos claros, capazes de assegurar transparência, fiscalização, supervisão humana e responsabilização adequada diante de eventuais violações. Somente por meio desse controle é possível compatibilizar o emprego da inovação tecnológica com os valores constitucionais que estruturam o Estado Democrático de Direito.

#### 7.4. ANÁLISE JURISPRUDENCIAL E CASOS CONCRETOS

As discussões relacionadas ao reconhecimento facial na segurança pública brasileira deixaram de possuir caráter exclusivamente teórico e passaram a produzir consequências concretas no âmbito do sistema de justiça criminal. A ocorrência de erros de identificação e a utilização inadequada de procedimentos de reconhecimento evidenciam os riscos jurídicos decorrentes da incorporação de mecanismos tecnológicos à persecução penal sem observância adequada das garantias constitucionais e processuais.

No âmbito jurisprudencial, o Superior Tribunal de Justiça consolidou entendimento restritivo acerca da utilização do reconhecimento pessoal e fotográfico como elemento probatório. Marco relevante dessa construção foi o julgamento do Habeas Corpus n.º 598.886/SC, em que a Sexta Turma reconheceu que a inobservância do procedimento previsto no artigo 226 do Código de Processo Penal compromete a confiabilidade do reconhecimento de pessoas e impede que esse meio de prova, isoladamente considerado, sustente uma condenação criminal.

Posteriormente, o Tribunal reafirmou esse posicionamento em decisões mais recentes, consolidando a compreensão de que reconhecimentos realizados sem observância das formalidades legais não podem servir como fundamento autônomo para decretação de prisão, recebimento de denúncia ou condenação penal. Em 2024, o STJ voltou a destacar a necessidade de observância rigorosa dos critérios legais aplicáveis

ao reconhecimento de pessoas, ressaltando que a apresentação de indivíduos com características semelhantes constitui garantia indispensável para redução dos riscos de erro e preservação da confiabilidade da prova.

A preocupação demonstrada pela Corte assume especial relevância quando analisada sob a perspectiva do racismo estrutural. Conforme sustenta Almeida (2021), as desigualdades raciais não decorrem apenas de comportamentos discriminatórios individuais, mas de estruturas institucionais historicamente consolidadas que produzem resultados desiguais para determinados grupos sociais. Nesse contexto, os erros de identificação envolvendo pessoas negras não podem ser compreendidos apenas como falhas isoladas, mas como manifestações de padrões discriminatórios que podem ser reproduzidos por mecanismos de controle social aparentemente neutros.

Além da evolução jurisprudencial, episódios recentes demonstram que os riscos associados ao reconhecimento facial permanecem presentes na prática da segurança pública brasileira. Em 2024, ganhou repercussão nacional o caso de Ailton Alves de Sousa, morador da periferia de São Paulo conduzido à delegacia diversas vezes após ser equivocadamente associado a um foragido por sistema vinculado ao programa Smart Sampa. O episódio evidenciou falhas relacionadas tanto à confiabilidade das informações utilizadas quanto aos mecanismos de verificação adotados pelo poder público, resultando em sucessivas intervenções indevidas na esfera de direitos do cidadão afetado.

A relevância jurídica desses casos não decorre apenas da existência de falhas tecnológicas, mas da utilização de seus resultados como fundamento para atos estatais potencialmente restritivos de direitos. Quando erros de identificação resultam em abordagens, investigações ou restrições indevidas à liberdade, evidencia-se a necessidade de observância rigorosa das garantias constitucionais e dos deveres de cautela impostos à Administração Pública.

Os precedentes recentes do Superior Tribunal de Justiça e os casos concretos analisados demonstram que a busca por eficiência tecnológica não pode justificar a flexibilização das garantias fundamentais que estruturam o processo penal democrático. Ao contrário, quanto maior a utilização de sistemas automatizados pelo poder público, maior deve ser a exigência de controle, transparência e observância dos direitos fundamentais, especialmente quando estão em jogo a liberdade, a igualdade e a presunção de inocência.

## 8. CONSIDERAÇÕES FINAIS

A utilização do reconhecimento facial na segurança pública brasileira evidencia que o avanço tecnológico aplicado às atividades estatais de vigilância e persecução penal produz impactos que ultrapassam questões relacionadas à eficiência administrativa e ao fortalecimento das políticas de segurança. A incorporação de sistemas automatizados de identificação envolve debates diretamente ligados à proteção de direitos fundamentais, à legitimidade da atuação estatal e aos limites jurídicos do uso da inteligência artificial pelo poder público.

Ao longo da pesquisa, verificou-se que o reconhecimento facial não opera de forma absolutamente neutra, estando sujeito a falhas técnicas, erros de identificação e limitações decorrentes do próprio funcionamento dos sistemas algorítmicos. Em um contexto historicamente marcado pelo racismo estrutural e pela seletividade do sistema de controle social brasileiro, tais falhas assumem consequências ainda mais sensíveis, sobretudo diante da possibilidade de reforço de práticas discriminatórias já existentes na atuação estatal.

A análise desenvolvida também demonstrou que a expansão dessas tecnologias ocorreu em velocidade superior à consolidação de mecanismos normativos e institucionais capazes de regulamentar adequadamente sua utilização. A ausência de critérios específicos relacionados à transparência algorítmica, fiscalização independente, controle dos bancos de dados biométricos e supervisão da atividade tecnológica amplia preocupações relacionadas à segurança jurídica e à proteção das garantias constitucionais.

No âmbito da persecução penal, observou-se que a utilização de sistemas automatizados de reconhecimento exige compatibilização permanente com o devido processo legal, especialmente no que se refere à preservação do contraditório, da ampla defesa, da presunção de inocência e da confiabilidade da prova penal. A atribuição de elevado grau de credibilidade aos resultados produzidos pelos algoritmos não afasta a necessidade de supervisão humana e de controle rigoroso acerca da validade das informações utilizadas em procedimentos investigativos e judiciais.

Além disso, os casos concretos e entendimentos jurisprudenciais analisados demonstram que os riscos relacionados ao reconhecimento facial já produzem consequências práticas relevantes no contexto brasileiro. As discussões recentes desenvolvidas pelo Poder Judiciário reforçam a necessidade de cautela na utilização

dessas ferramentas, principalmente diante da possibilidade de violações de direitos decorrentes de erros de identificação e da utilização inadequada de mecanismos tecnológicos de vigilância.

Dessa forma, conclui-se que o reconhecimento facial não pode ser tratado apenas como instrumento técnico de modernização da segurança pública. A utilização dessas tecnologias exige limites jurídicos claros, mecanismos efetivos de controle estatal e compatibilização constante com os princípios constitucionais que orientam o Estado Democrático de Direito. O avanço tecnológico, por si só, não legitima flexibilização de garantias fundamentais nem autoriza ampliação irrestrita da capacidade estatal de vigilância sobre a população.

## REFERÊNCIAS

Alma Preta. **Homem negro é detido 4 vezes em 7 meses após erro do Smart Sampa.**

Alma Preta, 2024. Disponível em:

<https://almapreta.com.br/sessao/cotidiano/smart-sampa-erro-homem-negro-detido/>.

Acesso em: 12 maio 2026.

Almeida, Silvio. **Racismo estrutural**. São Paulo: Jandaíra, 2021.

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, 2021. Disponível em:

<https://revistajuridica.tjdft.jus.br/index.php/rdj/article/view/734>. Acesso em: 22 abr. 2026.

Brasil. Superior Tribunal de Justiça. Reconhecimento criminal exige que suspeito seja posto ao lado de pessoas parecidas. **Portal STJ**, Brasília, DF, 10 maio 2024. Disponível em:

<https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/10052024-Reconhecimento-criminal-exige-que-suspeito-seja-posto-ao-lado-de-pessoas-parecidas.aspx>. Acesso em: 17 maio 2026.

Brasil. Superior Tribunal de Justiça. STJ traz novos avanços no entendimento sobre o reconhecimento de pessoas. **Portal STJ**, Brasília, DF, 17 mar. 2022. Disponível em:

<https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/17032022-STJ-traz-novos-avancos-no-entendimento-sobre-o-reconhecimento-de-pessoas.aspx>. Acesso em: 17 maio 2026.

Conselho Nacional de Justiça (Brasil). Reconhecimento facial e suas implicações no sistema de justiça criminal. **Revista CNJ**, Brasília, DF, v. 7, n. 1, 2023. Disponível em: <https://www.cnj.jus.br/ojs/revista-cnj/article/view/458>. Acesso em: 27 abr. 2026.

Fernandes, Florestan. **A integração do negro na sociedade de classes**. 5. ed. São Paulo: Globo, 2008.

Instituto Brasileiro de Geografia e Estatística. **Desigualdades sociais por cor ou raça no Brasil**. Rio de Janeiro: IBGE, 2024. Disponível em: <https://educa.ibge.gov.br/jovens/materias-especiais/21039-desigualdades-sociais-por-cor-ou-raca-no-brasil.html>. Acesso em: 11 abr. 2026.

Instituto de Pesquisa Econômica e Aplicada; FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Atlas da violência 2023**. Brasília, DF: IPEA; FBSP, 2023. Disponível em: <https://www.ipea.gov.br/atlasviolencia/>. Acesso em: 13 abr. 2026.

Jota. STJ absolve homem negro que foi condenado com base só em reconhecimento facial. **JOTA**, 2024. Disponível em: <https://www.jota.info/justica/stj-absolve-homem-negro-que-foi-condenado-com-base-so-em-reconhecimento-facial>. Acesso em: 12 maio 2026.

Kaspersky Brasil. O que é reconhecimento facial e como ele funciona? **Kaspersky**, [s.d]. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-facial-recognition>. Acesso em: 24 abr. 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**, [S. l.], 2025. Disponível em: <https://revista.unisal.br/lo/index.php/direitoepaz/article/view/1751>. Acesso em: 2 maio 2026.

Shah, Jay *et al.* Surveying racial bias in facial recognition: balancing datasets and algorithmic enhancements. **Electronics**, v. 13, n. 12, 2024. Disponível em: <https://www.mdpi.com/2079-9292/13/12/2317>. Acesso em: 27 abr. 2026.