



CARLA EUGÊNIA OLIVEIRA FERNANDES

MARCELA DE SOUSA SANTOS

REBECA CELENA DE SOUSA FERREIRA

**O RECONHECIMENTO FACIAL REALIZADO POR MEIOS TECNOLÓGICOS DE
VIGILÂNCIA EM MASSA: ANÁLISE SOB A PERSPECTIVA DOS DIREITOS
FUNDAMENTAIS**

TERESINA-PI

2026

CARLA EUGÊNIA OLIVEIRA FERNANDES
MARCELA DE SOUSA SANTOS
REBECA CELENA DE SOUSA FERREIRA

**O RECONHECIMENTO FACIAL REALIZADO POR MEIOS TECNOLÓGICOS DE
VIGILÂNCIA EM MASSA: ANÁLISE SOB A PERSPECTIVA DOS DIREITOS
FUNDAMENTAIS**

Artigo de Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Afya Centro Universitário Uninovafapi, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientadora: Profa. Dra. Iracema Rebeca de Medeiros Fazio

TERESINA-PI

2026

FICHA CATALOGRÁFICA

F363r Fernandes, Carla Eugênia Oliveira.

O reconhecimento facial realizado por meios tecnológicos de vigilância em massa: análise sob a perspectiva dos direitos fundamentais / Carla Eugênia Oliveira Fernandes; Marcela de Sousa Santos; Rebeca Celena de Sousa Ferreira. – Teresina: UNINOVAFAPI, 2026.

Orientador (a): Profº. Dra. Iracema Rebeca de Medeiros Fazio. – UNINOVAFAPI, 2026.

35.p.; color.; 23cm.

Trabalho de conclusão (Bacharelado em Direito). – UNINOVAFAPI, Teresina, 2026.

1. Direitos fundamentais. 2. Lei geral de proteção de dados. 3. Proteção de dados. 4. Reconhecimento facial. 5. Vigilância em massa. I. Título. II. Santos, Marcela de Sousa. III. Ferreira, Celena de Sousa.

CDD 340

CARLA EUGÊNIA OLIVEIRA FERNANDES

MARCELA DE SOUSA SANTOS

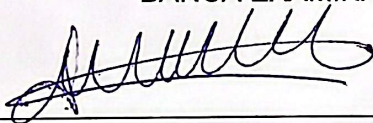
REBECA CELENA DE SOUSA FERREIRA

**O RECONHECIMENTO FACIAL REALIZADO POR MEIOS TECNOLÓGICOS DE
VIGILÂNCIA EM MASSA: ANÁLISE SOB A PERSPECTIVA DOS DIREITOS
FUNDAMENTAIS**

Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do
Afya Centro Universitário Uninovafapi,
como requisito parcial para obtenção do
grau de Bacharel em Direito.

Data de Aprovação: 25 / 06 / 2026

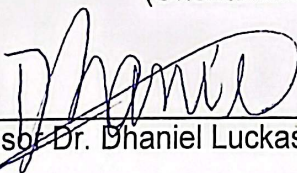
BANCA EXAMINADORA



Professora Dra. Iracema Rebeca de Medeiros Fazio

Afya Centro Universitário Uninovafapi

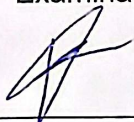
(Orientadora)



Professor Dr. Dhanil Lucas Terto Madeira Ferreira

Afya Centro Universitário Uninovafapi

(1º Examinador)



Professor Dr. Lívio Augusto de Carvalho Santos

Afya Centro Universitário Uninovafapi

(2º Examinador)

AGRADECIMENTOS

Dedicamos este trabalho a Deus, cuja infinita sabedoria já conhecia cada palavra aqui escrita antes mesmo que sonhássemos com este momento, concedendo-nos a graça de viver este propósito.

Dedicamos, com todo amor, esta conquista aos nossos pais e familiares, que, sob muito esforço e dedicação, tornaram possível nossa caminhada até aqui. Agradecemos pelo apoio constante, pelos incentivos, pelos sacrifícios realizados e pelas orações que nos fortaleceram, permitindo que florescêssemos e colhêssemos os sonhos que hoje temos a alegria de concretizar.

Dedicamos também este trabalho à nossa orientadora, Prof.^a Dra. Iracema Fazio, pela dedicação, paciência, acolhimento e valiosas contribuições ao longo desta trajetória. Sua orientação segura, seus ensinamentos e sua confiança foram fundamentais para a construção deste trabalho e para o nosso crescimento acadêmico e pessoal.

Estendemos esta dedicatória a todos os professores da graduação, que compartilharam seus conhecimentos, experiências e valores ao longo de nossa formação. Cada ensinamento contribuiu para a construção da profissionalidade que hoje buscamos exercer com compromisso, responsabilidade e sensibilidade.

"Para que todos vejam, e saibam, e considerem, e juntamente entendam que a mão do Senhor fez isso." - Isaías 41:20

RESUMO

O presente artigo tem como tema o reconhecimento facial realizado por meios tecnológicos de vigilância em massa no contexto da segurança pública e das investigações criminais no Brasil. O avanço da inteligência artificial e a crescente utilização dessas tecnologias pelo Estado têm gerado relevantes debates jurídicos acerca de sua compatibilidade com os direitos e garantias fundamentais assegurados pela Constituição Federal de 1988, especialmente a privacidade, a intimidade, os direitos da personalidade e o direito de não produzir provas contra si mesmo. Nesse contexto, busca-se responder ao seguinte problema de pesquisa: os erros do reconhecimento facial, gerados por meios tecnológicos de vigilância em massa, ocasionam violações aos direitos fundamentais do acusado? A pesquisa tem como objetivo geral analisar como o uso de provas obtidas por reconhecimento facial pelo Estado brasileiro pode violar direitos fundamentais, como a intimidade, a vida privada, os direitos da personalidade e o direito de não produzir prova contra si mesmo. Como objetivos específicos, busca identificar a forma como o ordenamento jurídico brasileiro enfrenta o conflito entre direitos individuais e interesses coletivos na utilização de tecnologias de vigilância; avaliar se a Lei Geral de Proteção de Dados oferece mecanismos suficientes para suprir eventuais lacunas jurídicas relacionadas ao uso do reconhecimento facial em investigações criminais no Brasil; e examinar os direitos fundamentais afetados por erros de identificação decorrentes do uso dessa tecnologia em processos criminais, verificando se essa prática é compatível com os princípios constitucionais. Parte-se da hipótese científica de que os erros no reconhecimento facial, decorrentes de tecnologias de vigilância em massa, podem violar direitos fundamentais do acusado. Metodologicamente, adotou-se o método dedutivo, com abordagem qualitativa de caráter exploratório, desenvolvida por meio de pesquisa bibliográfica e documental, fundamentada na análise da Constituição Federal, da Lei Geral de Proteção de Dados, da doutrina especializada, da jurisprudência e de produções acadêmicas relacionadas ao tema. Os resultados demonstraram que a ausência de regulamentação específica para o uso do reconhecimento facial na segurança pública favorece a ocorrência de violações a direitos fundamentais, especialmente diante da existência de falhas técnicas, vieses algorítmicos, discriminação racial e identificações equivocadas. Verificou-se, ainda, que a LGPD apresenta limitações quanto à proteção dos dados biométricos utilizados em atividades de segurança pública e investigação criminal, em razão da exclusão dessas atividades de seu âmbito de incidência. Conclui-se que a utilização do reconhecimento facial em sistemas de vigilância em massa, sem mecanismos adequados de transparência, fiscalização, controle institucional e regulamentação específica, representa risco concreto à efetivação dos direitos fundamentais. Assim, evidencia-se a necessidade de criação de legislação específica que estabeleça limites claros para o uso dessas tecnologias, assegurando a compatibilização entre segurança pública, inovação tecnológica e proteção dos direitos fundamentais no Estado Democrático de Direito.

Palavras-chave: Direitos fundamentais; Lei Geral de Proteção de Dados; Proteção de dados; Reconhecimento facial; Vigilância em massa.

ABSTRACT

This article addresses facial recognition performed by mass surveillance technologies in the context of public security and criminal investigations in Brazil. The advancement of artificial intelligence and the increasing use of these technologies by the State have generated relevant legal debates regarding their compatibility with the fundamental rights and guarantees ensured by the 1988 Federal Constitution, especially privacy, intimacy, personality rights, and the right not to produce evidence against oneself. In this context, this research seeks to answer the following question: do errors in facial recognition, generated by mass surveillance technologies, cause violations of the fundamental rights of the accused? The general objective of this research is to analyze how the use of evidence obtained through facial recognition by the Brazilian State can violate fundamental rights, such as intimacy, private life, personality rights, and the right not to produce evidence against oneself. Specifically, it seeks to identify how the Brazilian legal system addresses the conflict between individual rights and collective interests in the use of surveillance technologies; This study aims to assess whether the General Data Protection Law (LGPD) offers sufficient mechanisms to address potential legal gaps related to the use of facial recognition in criminal investigations in Brazil; and to examine the fundamental rights affected by identification errors resulting from the use of this technology in criminal proceedings, verifying whether this practice is compatible with constitutional principles. It starts from the scientific hypothesis that errors in facial recognition, resulting from mass surveillance technologies, can violate the fundamental rights of the accused. Methodologically, a deductive method was adopted, with a qualitative exploratory approach, developed through bibliographic and documentary research, based on the analysis of the Federal Constitution, the General Data Protection Law, specialized doctrine, jurisprudence, and academic productions related to the topic. The results demonstrated that the absence of specific regulations for the use of facial recognition in public security favors the occurrence of violations of fundamental rights, especially given the existence of technical flaws, algorithmic biases, racial discrimination, and mistaken identifications. It was also found that the LGPD (Brazilian General Data Protection Law) has limitations regarding the protection of biometric data used in public security and criminal investigation activities, due to the exclusion of these activities from its scope. It is concluded that the use of facial recognition in mass surveillance systems, without adequate mechanisms for transparency, oversight, institutional control, and specific regulation, represents a concrete risk to the realization of fundamental rights. Thus, the need for specific legislation that establishes clear limits for the use of these technologies is evident, ensuring compatibility between public security, technological innovation, and the protection of fundamental rights in a democratic state governed by the rule of law.

Keywords: Fundamental rights; General Data Protection Law; Data protection; Facial recognition; Mass surveillance.

SUMÁRIO

1 INTRODUÇÃO	11
2 ARTIGO	14
3 CONSIDERAÇÕES FINAIS	36
REFERÊNCIAS.....	38

1 INTRODUÇÃO

O avanço da inteligência artificial e o uso do reconhecimento facial no Brasil têm gerado debates jurídicos acerca da utilização dessas tecnologias em investigações criminais, especialmente quanto ao risco de violação de direitos fundamentais, como a privacidade, a intimidade, os direitos da personalidade e o direito de não produzir provas contra si mesmo.

Nesse sentido, diante da ausência de regulamentação específica sobre a matéria, o presente estudo busca verificar se a utilização dessas provas pelo Estado é compatível com o ordenamento jurídico brasileiro e com a Lei Geral de Proteção de Dados (LGPD), considerando o necessário equilíbrio entre segurança pública e direitos individuais. O problema central da pesquisa consiste em examinar se os erros do reconhecimento facial, gerados por meios tecnológicos de vigilância em massa, ocasionam violações aos direitos fundamentais do acusado?

Além disso, a relevância do tema justifica-se pelo crescente uso de tecnologias de inteligência artificial no âmbito da segurança pública, bem como pelos impactos jurídicos e sociais decorrentes de falhas nos sistemas de reconhecimento facial, que podem resultar em prisões injustas, discriminação racial e violações de garantias constitucionais. Soma-se a isso o fato de que ainda são escassos os estudos jurídicos aprofundados e a regulamentação específica acerca da utilização dessas tecnologias em investigações criminais no Brasil, evidenciando a necessidade de maior debate acadêmico e legislativo sobre a temática.

Ademais, a presente pesquisa tem como objetivo geral analisar como o uso de provas obtidas por reconhecimento facial pelo Estado brasileiro pode violar direitos fundamentais, como a intimidade, a vida privada, os direitos da personalidade e o direito de não produzir prova contra si mesmo.

No que se refere aos objetivos específicos, pretende-se identificar a forma como o ordenamento jurídico brasileiro enfrenta o conflito entre direitos individuais e interesses coletivos na utilização de tecnologias de vigilância; avaliar se a LGPD oferece mecanismos suficientes para suprir eventuais lacunas jurídicas relacionadas ao uso do reconhecimento facial em investigações criminais no Brasil; e examinar os direitos fundamentais afetados por erros de identificação decorrentes do uso dessa tecnologia em processos criminais, verificando se essa prática é compatível com os princípios constitucionais.

Diante disso, parte-se da hipótese científica de que os erros no

reconhecimento facial, decorrentes de tecnologias de vigilância em massa, podem violar direitos fundamentais do acusado. No contexto contemporâneo brasileiro, a expansão das tecnologias avançadas, especialmente da inteligência artificial e dos sistemas de reconhecimento facial, tem sido impulsionada pela promessa de maior eficiência na segurança pública e nas investigações criminais. Contudo, essa inovação levanta sérias preocupações jurídicas, pois pode comprometer garantias constitucionais asseguradas pela Constituição Federal.

Dessa forma, o estudo busca examinar como o ordenamento jurídico brasileiro trata o conflito entre interesses coletivos e direitos individuais, avaliando o papel da LGPD e suas limitações, especialmente diante da ausência de regulamentação específica para o uso do reconhecimento facial na segurança pública.

Além disso, analisa os impactos de identificações equivocadas, os riscos de vieses algorítmicos e as consequências jurídicas e sociais dessas falhas, que podem resultar em graves violações de direitos fundamentais. Assim, o presente trabalho defende a necessidade de criação de legislação específica que regule o uso dessas tecnologias, estabelecendo limites claros, mecanismos de controle e garantias de proteção aos direitos fundamentais, assegurando que o avanço tecnológico ocorra em conformidade com os princípios do Estado Democrático de Direito.

Metodologicamente, devido à natureza do tema abordado, adota-se o método dedutivo e a abordagem qualitativa de caráter exploratório, considerando que o objeto de estudo demanda análise jurídica e social de questões complexas. Parte-se de premissas gerais estabelecidas na Constituição Federal e na LGPD para examinar situações específicas e, a partir delas, formular conclusões acerca da validade e dos limites do uso de provas obtidas por reconhecimento facial no ordenamento jurídico brasileiro.

A pesquisa possui enfoque na interpretação de textos normativos, da doutrina e de produções acadêmicas relacionadas ao tema, bem como na compreensão dos impactos da tecnologia, especialmente no que se refere aos vieses algorítmicos e à possível violação de direitos fundamentais. Para tanto, o trabalho desenvolve-se por meio de pesquisa bibliográfica e documental, com análise da legislação pertinente, obras acadêmicas e consultas a portais oficiais.

Por fim, o presente trabalho encontra-se estruturado em cinco seções, sendo

uma destinada à introdução, outra às considerações finais e três voltadas ao desenvolvimento da pesquisa. Nessas seções serão abordados os seguintes temas: os meios tecnológicos de vigilância em massa e a colisão de direitos fundamentais; a LGPD e o reconhecimento facial na investigação criminal; e os erros do reconhecimento facial decorrentes do uso de tecnologias de vigilância em massa.

2 ARTIGO

O RECONHECIMENTO FACIAL REALIZADO POR MEIOS TECNOLÓGICOS DE VIGILÂNCIA EM MASSA: ANÁLISE SOB A PERSPECTIVA DOS DIREITOS FUNDAMENTAIS

FACIAL RECOGNITION PERFORMED BY TECHNOLOGICAL MEANS OF MASS SURVEILLANCE: ANALYSIS FROM THE PERSPECTIVE OF FUNDAMENTAL RIGHTS

RESUMO

O presente artigo tem como tema o reconhecimento facial realizado por meios tecnológicos de vigilância em massa no contexto da segurança pública e das investigações criminais no Brasil. O avanço da inteligência artificial e a utilização dessas tecnologias pelo Estado têm gerado debates acerca de sua compatibilidade com os direitos e garantias fundamentais assegurados pela Constituição Federal de 1988, especialmente a privacidade, a intimidade, os direitos da personalidade e o direito de não produzir provas contra si mesmo. A pesquisa busca responder se os erros do reconhecimento facial, gerados por meios tecnológicos de vigilância em massa, ocasionam violações aos direitos fundamentais do acusado. O objetivo geral consiste em analisar como o uso de provas obtidas por reconhecimento facial pelo Estado brasileiro pode violar direitos fundamentais, como a intimidade, a vida privada, os direitos da personalidade e o direito de não produzir prova contra si mesmo. Utilizou-se o método dedutivo, com abordagem qualitativa e caráter exploratório, mediante pesquisa bibliográfica e documental fundamentada na Constituição Federal, na Lei Geral de Proteção de Dados, na doutrina, na jurisprudência e em produções acadêmicas relacionadas ao tema. Os resultados demonstraram que a ausência de regulamentação específica para o uso do reconhecimento facial na segurança pública favorece violações a direitos fundamentais, especialmente em razão de falhas técnicas, vieses algorítmicos, discriminação racial e identificações equivocadas. Conclui-se que a utilização dessa tecnologia exige regulamentação específica, transparência, fiscalização e controle institucional, a fim de assegurar a compatibilização entre segurança pública, inovação tecnológica e proteção dos direitos fundamentais.

Palavras-chave: Direitos fundamentais; Lei Geral de Proteção de Dados; Proteção de dados; Reconhecimento facial; Vigilância em massa.

ABSTRACT

This article addresses facial recognition performed by mass surveillance technologies in the context of public security and criminal investigations in Brazil. The advancement of artificial intelligence and the use of these technologies by the State

have generated debates about their compatibility with the fundamental rights and guarantees ensured by the 1988 Federal Constitution, especially privacy, intimacy, personality rights, and the right not to produce evidence against oneself. This research seeks to answer whether errors in facial recognition, generated by mass surveillance technologies, cause violations of the fundamental rights of the accused. The general objective is to analyze how the use of evidence obtained through facial recognition by the Brazilian State can violate fundamental rights, such as intimacy, private life, personality rights, and the right not to produce evidence against oneself. The deductive method was used, with a qualitative and exploratory approach, through bibliographic and documentary research based on the Federal Constitution, the General Data Protection Law, doctrine, jurisprudence, and academic productions related to the topic. The results demonstrated that the absence of specific regulations for the use of facial recognition in public security favors violations of fundamental rights, especially due to technical flaws, algorithmic biases, racial discrimination, and mistaken identifications. It is concluded that the use of this technology requires specific regulation, transparency, oversight, and institutional control in order to ensure compatibility between public security, technological innovation, and the protection of fundamental rights.

Keywords: Fundamental rights; General Data Protection Law; Data protection; Facial recognition; Mass surveillance.

1 INTRODUÇÃO

O avanço da inteligência artificial e o uso do reconhecimento facial no Brasil têm gerado debates jurídicos acerca da utilização dessas tecnologias em investigações criminais, especialmente quanto ao risco de violação de direitos fundamentais, como a privacidade, a intimidade, os direitos da personalidade e o direito de não produzir provas contra si mesmo.

Nesse sentido, diante da ausência de regulamentação específica sobre a matéria, o presente estudo busca verificar se a utilização dessas provas pelo Estado é compatível com o ordenamento jurídico brasileiro e com a Lei Geral de Proteção de Dados (LGPD), considerando o necessário equilíbrio entre segurança pública e direitos individuais. O problema central da pesquisa consiste em examinar se os erros do reconhecimento facial, gerados por meios tecnológicos de vigilância em massa, ocasionam violações aos direitos fundamentais do acusado?

Além disso, a relevância do tema justifica-se pelo crescente uso de tecnologias de inteligência artificial no âmbito da segurança pública, bem como pelos impactos jurídicos e sociais decorrentes de falhas nos sistemas de reconhecimento facial, que podem resultar em prisões injustas, discriminação racial e violações de garantias constitucionais. Soma-se a isso o fato de que ainda são escassos os estudos jurídicos aprofundados e a regulamentação específica acerca da utilização

dessas tecnologias em investigações criminais no Brasil, evidenciando a necessidade de maior debate acadêmico e legislativo sobre a temática.

Ademais, a presente pesquisa tem como objetivo geral analisar como o uso de provas obtidas por reconhecimento facial pelo Estado brasileiro pode violar direitos fundamentais, como a intimidade, a vida privada, os direitos da personalidade e o direito de não produzir prova contra si mesmo.

No que se refere aos objetivos específicos, pretende-se identificar a forma como o ordenamento jurídico brasileiro enfrenta o conflito entre direitos individuais e interesses coletivos na utilização de tecnologias de vigilância; avaliar se a LGPD oferece mecanismos suficientes para suprir eventuais lacunas jurídicas relacionadas ao uso do reconhecimento facial em investigações criminais no Brasil; e examinar os direitos fundamentais afetados por erros de identificação decorrentes do uso dessa tecnologia em processos criminais, verificando se essa prática é compatível com os princípios constitucionais.

Diante disso, parte-se da hipótese científica de que os erros no reconhecimento facial, decorrentes de tecnologias de vigilância em massa, podem violar direitos fundamentais do acusado. No contexto contemporâneo brasileiro, a expansão das tecnologias avançadas, especialmente da inteligência artificial e dos sistemas de reconhecimento facial, tem sido impulsionada pela promessa de maior eficiência na segurança pública e nas investigações criminais. Contudo, essa inovação levanta sérias preocupações jurídicas, pois pode comprometer garantias constitucionais asseguradas pela Constituição Federal.

Dessa forma, o estudo busca examinar como o ordenamento jurídico brasileiro trata o conflito entre interesses coletivos e direitos individuais, avaliando o papel da LGPD e suas limitações, especialmente diante da ausência de regulamentação específica para o uso do reconhecimento facial na segurança pública.

Além disso, analisa os impactos de identificações equivocadas, os riscos de vieses algorítmicos e as consequências jurídicas e sociais dessas falhas, que podem resultar em graves violações de direitos fundamentais. Assim, o presente trabalho defende a necessidade de criação de legislação específica que regule o uso dessas tecnologias, estabelecendo limites claros, mecanismos de controle e garantias de proteção aos direitos fundamentais, assegurando que o avanço tecnológico ocorra em conformidade com os princípios do Estado Democrático de

Direito.

Metodologicamente, devido à natureza do tema abordado, adota-se o método dedutivo e a abordagem qualitativa de caráter exploratório, considerando que o objeto de estudo demanda análise jurídica e social de questões complexas. Parte-se de premissas gerais estabelecidas na Constituição Federal e na LGPD para examinar situações específicas e, a partir delas, formular conclusões acerca da validade e dos limites do uso de provas obtidas por reconhecimento facial no ordenamento jurídico brasileiro.

A pesquisa possui enfoque na interpretação de textos normativos, da doutrina e de produções acadêmicas relacionadas ao tema, bem como na compreensão dos impactos da tecnologia, especialmente no que se refere aos vieses algorítmicos e à possível violação de direitos fundamentais. Para tanto, o trabalho desenvolve-se por meio de pesquisa bibliográfica e documental, com análise da legislação pertinente, obras acadêmicas e consultas a portais oficiais.

Por fim, o presente trabalho encontra-se estruturado em cinco seções, sendo uma destinada à introdução, outra às considerações finais e três voltadas ao desenvolvimento da pesquisa. Nessas seções serão abordados os seguintes temas: os meios tecnológicos de vigilância em massa e a colisão de direitos fundamentais; a LGPD e o reconhecimento facial na investigação criminal; e os erros do reconhecimento facial decorrentes do uso de tecnologias de vigilância em massa.

2 OS MEIOS TECNOLÓGICOS DE VIGILÂNCIA EM MASSAS E A COLISÃO DE DIREITOS

Nesta seção será analisada a forma como o ordenamento jurídico brasileiro trata o conflito entre direitos individuais e interesses coletivos na utilização de tecnologias de vigilância, especialmente no contexto do reconhecimento facial em investigações criminais. A incorporação dessas ferramentas tecnológicas pelo Estado brasileiro intensificou o debate jurídico acerca dos limites constitucionais da atuação estatal, impondo a necessidade de compatibilizar a segurança pública com a preservação dos direitos individuais.

A priori, faz-se necessário compreender o que se entende por meios tecnológicos de vigilância em massa. Esses mecanismos consistem no conjunto de ferramentas tecnológicas utilizadas para monitoramento, coleta, processamento e análise de dados pessoais em larga escala, geralmente empregados pelo poder

público com a finalidade de prevenção de infrações penais, segurança pública e investigação criminal. Entre os principais instrumentos atualmente utilizados destacam-se os sistemas de videomonitoramento, câmeras inteligentes integradas à inteligência artificial, reconhecimento facial biométrico, geolocalização por dispositivos móveis, monitoramento de dados, além do cruzamento automatizado de bancos de dados (Privacy International, [s.d.]).

No cenário contemporâneo, o reconhecimento facial destaca-se como uma das principais ferramentas de vigilância tecnológica utilizadas pelo poder público. De modo geral, seu funcionamento ocorre por meio da detecção da face do indivíduo em determinada imagem, seguida da padronização do rosto capturado para possibilitar comparação uniforme entre as imagens analisadas. Posteriormente, o sistema extrai características biométricas específicas, convertendo essas informações em representações matemáticas individualizadas que serão comparadas com bancos de dados previamente armazenados (Silva *et al.*, 2021).

A partir desse processamento algorítmico, o sistema emite níveis de compatibilidade capazes de identificar ou verificar a identidade da pessoa analisada. Trata-se de tecnologia baseada no tratamento automatizado de dados biométricos e associada ao uso de inteligência artificial. Embora frequentemente apresentada como instrumento de modernização da segurança pública e eficiência investigativa, sua utilização em larga escala suscita preocupações relacionadas a falhas técnicas, vieses algorítmicos, discriminação racial e riscos de identificação equivocada (Silva *et al.*, 2021).

A expansão dessas tecnologias amplia consideravelmente a capacidade estatal de vigilância contínua sobre a população, o que pode gerar impactos significativos sobre direitos fundamentais constitucionalmente protegidos. Entre os principais direitos suscetíveis à violação encontram-se a intimidade, a vida privada, a personalidade e o direito de não produzir provas contra si mesmo, consagrado pelo princípio *nemo tenetur se detegere*.

A questão central consiste, portanto, em compreender de que modo o ordenamento jurídico brasileiro soluciona os conflitos entre a proteção dos direitos individuais e a promoção do interesse coletivo, preservando os fundamentos do Estado Democrático de Direito. A Constituição Federal de 1988, pilar normativo do sistema jurídico brasileiro, consagra amplo rol de direitos e garantias fundamentais, especialmente no artigo 5º, destinados à proteção da dignidade da pessoa humana

(Brasil, 1988).

Recentemente, esse rol foi ampliado pela Emenda Constitucional nº 115/2022, que incluiu o inciso LXXIX ao art. 5º, elevando a proteção de dados pessoais, inclusive nos meios digitais, à categoria de direito fundamental (Brasil, 2022c). Do mesmo modo, o texto constitucional também atribui ao Estado deveres positivos de atuação, dentre os quais se destaca a segurança, prevista no art. 6º como direito social e no art. 144 como dever do Estado, direito e responsabilidade de todos (Brasil, 1988).

Segundo Saes (2011), a interpretação sistemática da Constituição Federal evidencia que não existem direitos fundamentais absolutos. Essa inexistência de absolutismo decorre da própria complexidade das relações sociais e da pluralidade de valores consagrados pela ordem constitucional. Nesse contexto, a colisão entre direitos fundamentais é compreendida como um fenômeno característico das Constituições compromissárias, a exemplo da Constituição brasileira, que reúne diversos valores, princípios e correntes ideológicas. Essas Constituições distinguem-se justamente por incorporarem normas e diretrizes de diferentes matrizes ideológicas, o que favorece a ocorrência de conflitos entre princípios constitucionais e torna necessária a utilização de mecanismos jurídicos aptos à sua harmonização e resolução.

Assim, os direitos fundamentais não possuem caráter ilimitado, pois encontram restrições nos demais direitos igualmente protegidos pela Constituição. A relatividade dos direitos decorre do princípio da convivência das liberdades públicas, segundo o qual o exercício de um direito deve compatibilizar-se com os demais bens jurídicos constitucionalmente assegurados, exigindo harmonização quando houver conflito entre eles (Moraes, 2025).

Ingo Sarlet (2014) preleciona que os direitos fundamentais não possuem caráter absoluto, sendo possíveis limitações decorrentes da colisão entre direitos fundamentais e outros bens jurídico-constitucionais. Para o autor, mesmo direitos formalmente ilimitados podem sofrer restrições quando isso se mostrar imprescindível para assegurar a proteção de outros direitos constitucionalmente tutelados. Nesse contexto, em face de situação concreta de colisão, a solução não decorre da prevalência automática de um direito sobre outro, mas de um processo de ponderação no caso concreto, orientado pela necessidade de harmonização entre os valores constitucionais em tensão.

Essa compreensão revela-se particularmente relevante na análise das tecnologias de vigilância em massa, uma vez que a segurança pública, embora constitucionalmente protegida, não pode justificar restrições arbitrárias ou desproporcionais aos direitos individuais. Da mesma forma, a proteção das liberdades individuais não pode inviabilizar por completo a atuação estatal legítima na prevenção e repressão de infrações penais. O desafio constitucional reside justamente em harmonizar esses interesses em conflito.

O Supremo Tribunal Federal (STF, Brasil, 2003), consolidou entendimento no sentido de que nenhum direito fundamental possui caráter absoluto, conforme expressamente reconhecido no HC 82.424, ao afirmar que direitos e garantias constitucionais podem sofrer limitações quando em confronto com outros valores constitucionais. Além disso, em precedente recente, a Corte reafirmou a necessidade de ponderação entre valores constitucionais, especialmente em situações que envolvem o direito à informação e o direito à intimidade, destacando que a solução deve ser construída a partir das circunstâncias do caso concreto. Leia-se:

Agravos regimentais em recurso extraordinário. Ação civil pública. Divulgação de imagens de presos provisórios. Direito à informação versus direito à intimidade. **Aparente conflito normativo entre direitos fundamentais, os quais não são absolutos.** Ponderação de valores. Solução no caso concreto dada pelas instâncias ordinárias. Exposição de imagem de preso provisório desacompanhada do respectivo nome, endereço ou profissão apenas de forma excepcional e motivada. Precedentes. Agravos regimentais não providos. 1. A Corte de Origem determinou que os agentes públicos apenas excepcionalmente e de forma motivada promovam a exposição de imagem de preso provisório, a qual, nesse caso, deve ser desacompanhada do respectivo nome, endereço ou profissão, a fim de minimizar os danos provocados pela exposição midiática da imagem. 2. Adotou-se como critério de julgamento, no acórdão recorrido, a razoabilidade, exercendo-se um juízo de ponderação entre valores de igual estatura constitucional, entre os quais sobressaem o direito à informação e o direito à intimidade. **3. Não há direitos fundamentais absolutos, cabendo ao julgador, dadas as circunstâncias do caso concreto, em juízo de ponderação, avaliar qual princípio deverá prevalecer.** 4. Agravos regimentais não providos. (Brasil, 2023).

Dessa forma, o eventual conflito entre o interesse público na promoção da segurança pública e direitos fundamentais individuais, tais como a privacidade, a intimidade, os direitos da personalidade e a garantia contra a autoincriminação, deve ser resolvido mediante a técnica da ponderação, observando-se as circunstâncias do caso concreto e os parâmetros constitucionais aplicáveis.

Nesse contexto, destaca-se a teoria dos direitos fundamentais desenvolvida por Robert Alexy (2008), segundo a qual esses direitos possuem natureza

principiológica, configurando-se como mandamentos de otimização, cuja realização deve ocorrer na maior medida possível, dentro das possibilidades fáticas e jurídicas existentes. Para o autor, conflitos entre princípios constitucionais não se resolvem por exclusão definitiva de um deles, mas mediante técnica de sopesamento.

Como leciona Alexy:

Essa relação de tensão não pode ser solucionada com base em uma precedência absoluta de um desses deveres, ou seja, nenhum desses deveres goza, "por si só, de prioridade". O conflito deve, ao contrário, ser resolvido "por meio de um sopesamento entre os interesses conflitantes". O objetivo desse sopesamento é definir qual dos interesses - que abstratamente estão no mesmo nível - tem maior peso no caso concreto. (Alexy, 2008, p.95).

A técnica da ponderação concretiza-se por intermédio do princípio da proporcionalidade, estruturado em três subcritérios, a adequação, necessidade e proporcionalidade em sentido estrito. Inicialmente, deve-se verificar se a medida adotada é apta a alcançar finalidade constitucional legítima. Em seguida, exige-se demonstração de que não há meio alternativo menos gravoso ao direito restringido. Por fim, avalia-se se os benefícios proporcionados pela medida superam os prejuízos impostos aos direitos fundamentais afetados (Alexy, 2008).

Esse entendimento encontra respaldo na jurisprudência pátria, que reconhece a utilização da técnica da ponderação como instrumento adequado para a solução de conflitos entre direitos fundamentais, com base nos critérios de adequação, necessidade e proporcionalidade em sentido estrito, sempre com vistas à preservação da dignidade da pessoa humana em ambos os polos da relação jurídica, conforme se depreende do seguinte julgado:

AGRAVO DE INSTRUMENTO - EFEITO SUSPENSIVO - CONFLITO DE DIREITOS FUNDAMENTAIS CONSTITUCIONAIS - PROPORCIONALIDADE - DIGNIDADE HUMANA - PRINCÍPIOS CONSTITUCIONAIS. - **Havendo colisão de direitos fundamentais é razoável a utilização de técnicas de ponderação entre princípios com base na proporcionalidade e razoabilidade.** - À luz da adequação, necessidade e proporcionalidade em sentido estrito nos casos de conflito de direitos fundamentais, busca-se garantir a dignidade humana para ambos os lados. - Princípios constitucionais são fortes orientadores do direito objetivo. (Minas Gerais, 2022).

A discussão sobre a colisão de direitos no contexto da vigilância tecnológica transcende o âmbito nacional, inserindo-se na proteção internacional dos Direitos Humanos. A Declaração Universal dos Direitos Humanos (DUDH), adotada em 1948, estabelece em seu artigo 12 que "ninguém será sujeito a interferências arbitrárias em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem a ataques à sua honra e à sua reputação", conforme dispõe a

Organização das Nações Unidas (ONU, 1948). Esse preceito fundamental ressalta a importância da privacidade como pilar da dignidade humana, um valor que deve ser salvaguardado diante do avanço de tecnologias como o reconhecimento facial.

A dignidade da pessoa humana, princípio basilar da Constituição Federal brasileira, encontra respaldo nos documentos internacionais, exigindo que qualquer intervenção estatal que afete a esfera privada dos indivíduos seja pautada pela estrita legalidade, necessidade e proporcionalidade, evitando a violação de direitos inerentes à pessoa humana (Santos, 2025).

No âmbito do reconhecimento facial e de outras tecnologias de vigilância em massa, essa análise demanda exame rigoroso de sua efetiva eficiência, dos índices de erro, dos riscos de discriminação algorítmica, da segurança no tratamento de dados e da existência de métodos investigativos menos invasivos (Rey; Francescato, 2025). A mera invocação da segurança pública não é suficiente para legitimar, por si só, medidas potencialmente violadoras de direitos fundamentais. Caso a utilização dessas tecnologias não demonstre necessidade concreta, adequação técnica comprovada e respeito ao núcleo essencial das garantias individuais, sua compatibilidade com a Constituição Federal estará juridicamente comprometida.

Dessa forma, a utilização de meios tecnológicos de vigilância em massa pelo Estado brasileiro somente se mostra constitucionalmente legítima quando submetida a parâmetros normativos claros, controle institucional rigoroso e observância dos direitos fundamentais. A ausência de regulamentação específica, associada à expansão tecnológica, amplia o risco de abusos, vigilância desproporcional e violações incompatíveis com os princípios estruturantes do Estado Democrático de Direito. Assim, o desafio jurídico contemporâneo não consiste apenas em admitir ou rejeitar a tecnologia, mas em estabelecer limites jurídicos capazes de assegurar que sua utilização ocorra em conformidade com a dignidade da pessoa humana e as garantias constitucionais.

3 A LEI GERAL DE PROTEÇÃO DE DADOS E O RECONHECIMENTO FACIAL POR MEIOS TECNOLÓGICOS DE VIGILÂNCIA EM MASSA NA INVESTIGAÇÃO CRIMINAL

A LGPD foi instituída com a finalidade de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa

natural, estabelecendo diretrizes para o tratamento de dados pessoais no Brasil (Brasil, 2018). Nesse contexto, a crescente adoção de tecnologias de vigilância pelo Estado brasileiro, especialmente sistemas de reconhecimento facial no âmbito da segurança pública, suscita relevantes questionamentos quanto à compatibilidade dessas práticas com a proteção de direitos fundamentais.

Diante desse cenário, questiona-se se a LGPD oferece mecanismos jurídicos suficientes para suprir as lacunas normativas relacionadas ao uso do reconhecimento facial em investigações criminais (Brasil, 2018). Embora a lei represente um avanço significativo na proteção de dados pessoais, sua aplicação revela limitações importantes quando confrontada com tecnologias de monitoramento biométrico em larga escala, como aponta (Santos, 2021).

No contexto da sociedade informacional do século XXI, a noção de privacidade ultrapassa a dimensão física e passa a abranger o ambiente digital, no qual a coleta, o armazenamento e o compartilhamento de dados pessoais se tornaram práticas amplamente disseminadas. A expansão da internet e das plataformas digitais ampliou significativamente a exposição dos indivíduos, redefinindo as dinâmicas sociais e intensificando os riscos associados ao tratamento de dados. Nesse cenário, o uso de tecnologias de reconhecimento facial constitui uma manifestação concreta dessa ampliação, ao permitir a identificação automatizada de indivíduos em espaços públicos conforme sustenta Doneda (2019).

A utilização de sistemas de reconhecimento facial em espaços públicos no Brasil evidencia a expansão de práticas de vigilância em massa, especialmente em ambientes urbanos de grande circulação, como sistemas de transporte. Reportagens jornalísticas indicam que a implementação dessas tecnologias ocorreu, em determinados contextos, sem transparência adequada quanto à coleta e ao tratamento de dados biométricos dos usuários do modo como esclarece (Souza, 2018).

No Brasil, já existem casos concretos de identificação equivocada decorrente da utilização de sistemas de reconhecimento facial pelo poder público. Um exemplo relevante da discussão sobre privacidade e proteção de dados no Brasil ocorreu na Linha 4-Amarela do metrô de São Paulo, onde foram instaladas portas digitais equipadas com câmeras capazes de identificar características dos passageiros, como gênero, faixa etária e expressões faciais (Souza, 2018).

Essas informações eram utilizadas para direcionamento publicitário e análise

de comportamento dos usuários. O caso gerou grande repercussão por envolver a coleta de dados sem que os passageiros tivessem conhecimento claro sobre o monitoramento realizado, levantando debates sobre os limites do uso da tecnologia em espaços públicos e a necessidade de garantir o direito à privacidade e à proteção de dados pessoais como evidência (Souza, 2018).

Em continuidade a essa problemática, em Aracaju/SE, Gildeane Taislaine Santos foi confundida duas vezes com uma foragida durante o Pré-Caju de 2023 em razão de falha no sistema utilizado pela segurança pública. Após ser submetida a abordagem policial humilhante e exposição pública indevida, a Justiça sergipana reconheceu a responsabilidade do Estado e do Município de Aracaju, condenando-os ao pagamento de indenização por danos morais no valor total de R\$120 mil consoante demonstra Santiago (2023).

Na mesma linha de ocorrências, outro episódio envolveu João Antônio Trindade, abordado indevidamente durante a final do Campeonato Sergipano em razão de falha semelhante, episódio que levou o governo de Sergipe a suspender temporariamente o uso da tecnologia. Especialistas ouvidos pela matéria afirmam que esses sistemas apresentam vieses raciais significativos, atingindo desproporcionalmente pessoas negras e grupos vulnerabilizados na forma descrita por Durães (2024).

Os casos evidenciam que falhas algorítmicas podem atingir diretamente direitos fundamentais, como a dignidade da pessoa humana, a liberdade, a privacidade, a intimidade, o direito de não produzir prova contra si mesmo e a presunção de inocência. Além disso, destaca-se a ausência de regulamentação específica e a falta de transparência estatal quanto aos índices de erro e aos critérios utilizados pelos algoritmos empregados na segurança pública brasileira, o que agrava a insegurança jurídica e amplia o risco de violações a direitos fundamentais. Ademais, observa-se a atuação conjunta do poder público e de empresas privadas na operacionalização desses sistemas, o que amplia as preocupações relativas à governança e à destinação dos dados coletados.

Essas práticas evidenciam questionamentos quanto à sua legalidade e legitimidade, sobretudo diante da ausência de informações claras aos titulares dos dados e da indefinição de bases legais específicas que fundamentam o tratamento dessas informações. De acordo com estudos do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio, 2021), o reconhecimento facial, por se basear em dados

biométricos classificados como sensíveis, potencializa riscos de violação a direitos fundamentais, incluindo a privacidade, a liberdade de expressão, a liberdade de reunião e o princípio da não discriminação. Ademais, esses sistemas podem reproduzir vieses algorítmicos, contribuindo para práticas discriminatórias.

Do ponto de vista técnico, o reconhecimento facial opera por meio da coleta e do processamento de dados biométricos, consistindo na extração de características específicas da face humana, como distâncias entre pontos faciais e padrões estruturais, convertidas em representações matemáticas capazes de identificar indivíduos. Na forma preconizada por Santos (2021), após a fase de treinamento com bancos de dados previamente estruturados, os algoritmos tornam-se aptos a realizar a identificação automatizada a partir de imagens ou vídeos. Nos termos do art. 5º, II, da LGPD, os dados são classificados como dados pessoais sensíveis, exigindo, portanto, um nível mais elevado de proteção jurídica (Brasil, 2018).

Sob a perspectiva constitucional, a proteção à privacidade encontra fundamento no art. 5º, X, da Constituição da República Federativa do Brasil de 1988, que assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (Brasil, 1988). Nesse sentido, a utilização indiscriminada de sistemas de vigilância biométrica em espaços públicos, sem critérios claros de necessidade, adequação e proporcionalidade, pode configurar violação a esses direitos, especialmente na ausência de mecanismos efetivos de controle. A proteção da privacidade também é reconhecida no âmbito internacional, notadamente na DUHD, cujo artigo 12 veda interferências arbitrárias na vida privada (ONU, 1948). Como observa Doneda (2019), a evolução desse direito na sociedade da informação reforça a necessidade de instrumentos jurídicos capazes de assegurar aos indivíduos o controle sobre seus dados pessoais.

Não obstante os avanços promovidos pela LGPD no ordenamento jurídico brasileiro, sua eficácia revela-se significativamente limitada no âmbito da segurança pública e da investigação criminal. Isso porque, conforme dispõe o art. 4º, III, a referida norma exclui expressamente essas atividades de sua incidência, remetendo sua regulamentação a legislação específica ainda inexistente (Brasil, 2018). Essa exclusão normativa fragiliza a proteção de dados pessoais sensíveis, como os biométricos, e cria um cenário de incerteza jurídica que favorece a adoção de tecnologias invasivas, como o reconhecimento facial, sem parâmetros claros de legalidade, necessidade e proporcionalidade.

Logo, a ausência de um marco regulatório específico compromete a efetividade dos direitos fundamentais à privacidade e à autodeterminação informativa, ao mesmo tempo em que amplia o risco de práticas estatais potencialmente arbitrárias no âmbito da vigilância em massa. A utilização de tecnologias de reconhecimento facial deve estar condicionada à existência de previsão legal específica e à elaboração de relatórios de impacto à proteção de dados pessoais, instrumentos essenciais para a identificação e mitigação de riscos. Outrossim, a adoção dessas tecnologias exige a implementação de mecanismos efetivos de transparência, auditoria e controle institucional, sob pena de violação aos princípios do Estado Democrático de Direito sob o prisma sustentado por (Santos, 2021).

4 O ERRO DO RECONHECIMENTO FACIAL POR MEIOS TECNOLÓGICOS DE VIGILÂNCIA EM MASSA

A presente seção tem por objetivo examinar os direitos fundamentais afetados por erros de identificação em processos criminais decorrentes do uso de tecnologias de reconhecimento facial em sistemas de vigilância em massa, verificando se essa prática é compatível com os princípios constitucionais que regem o processo penal brasileiro.

A introdução do reconhecimento facial no sistema de justiça é frequentemente justificada como um passo necessário para a modernização da segurança pública, com a promessa de agilizar a identificação de suspeitos e inibir a criminalidade. No entanto, essa narrativa tecnológica precisa ser confrontada com os princípios que sustentam o Estado Democrático de Direito. A Constituição de 1988, ao estabelecer limites à atuação estatal, protege a liberdade e a dignidade da pessoa humana de forma que a eficiência administrativa não possa sobrepor-se aos direitos fundamentais (Brasil, 1988).

A expansão dessa tecnologia no país se dá em um cenário de vacuidade normativa. Ao contrário de países como o Reino Unido, que possuem diretrizes mais consolidadas, o Brasil opera sem uma regulamentação específica e sistematizada para o uso do reconhecimento facial na persecução penal. A incorporação das ferramentas ocorre de maneira dispersa, marcada por baixa transparência e controle institucional insuficiente (Amaral et al., 2025).

O reconhecimento facial, quando empregado em sistemas de vigilância em

massa, opera de forma contínua e indiscriminada sobre toda a população que circula nesses espaços, independentemente de qualquer suspeita individualizada. Para Grother et al., (2019), do ponto de vista técnico, o sistema funciona em três etapas: captura da imagem facial do indivíduo, extração de padrões matemáticos a partir de pontos de referência do rosto e comparação automatizada com bancos de dados preexistentes.

Por depender de dados biométricos sensíveis e de difícil alteração, conforme classifica a LGPD, o erro nesses sistemas não pode ser tratado como fenômeno meramente excepcional, sobretudo quando a tecnologia é utilizada em larga escala sobre populações inteiras. Quanto maior o volume de pessoas monitoradas, maior o número absoluto de identificações equivocadas, ainda que a taxa de erro percentual pareça baixa (Brasil, 2018).

Sua utilização inadequada pode levar a violações dos direitos à privacidade, à proteção de dados, à liberdade de locomoção e à igualdade. No atual estágio de desenvolvimento da tecnologia, ITS Rio (2021) aponta que o seu potencial danoso é ainda maior para grupos vulneráveis, como negros, mulheres e demais minorias, principalmente quando se observa a questão por meio de lentes de interseccionalidade.

A suposta objetividade da inteligência artificial, contudo, não isenta os sistemas de condicionamentos humanos. Os algoritmos reproduzem padrões definidos por programadores e alimentados por bases de dados selecionadas, o que desmonta a ideia de neutralidade tecnológica. O código, portanto, reflete escolhas humanas que podem carregar vieses implícitos, conforme argumentam Cani e Alcantara Nunes (2022). Nesse sentido, estudos demonstram que sistemas de reconhecimento facial apresentam taxas de erro significativamente superior na identificação de pessoas negras e mulheres (ITS Rio, 2021).

No Brasil, onde a população negra é majoritária e historicamente hipervulnerável à violência do sistema de justiça criminal, esse viés algorítmico não é um detalhe técnico. Esse cenário pode violar o direito de não ser confundido, especialmente quando falhas tecnológicas resultam em prisões indevidas e na submissão de inocentes ao aparato punitivo do Estado, conforme destaca Neto (2025). Casos documentados no Brasil e no exterior demonstram que pessoas inocentes foram presas com base em falsos positivos de sistemas de reconhecimento facial, evidenciando que o erro do algoritmo tem rosto, cor e

endereço (Cani; Alcantara Nunes, 2022).

O erro de identificação produzido por esses sistemas desencadeia consequências severas no plano processual. Um falso positivo pode resultar em investigação criminal, condução coercitiva, prisão em flagrante ou decretação de prisão preventiva. A confiança cega na tecnologia compromete a segurança jurídica, pois decisões restritivas de direitos fundamentais passam a basear-se em probabilidades estatísticas geradas por um algoritmo, e não em prova robusta produzida sob o crivo do contraditório. Machado e Barros (2024) alertam que a aparente objetividade atribuída aos sistemas de inteligência artificial pode levar à aceitação acrítica de seus resultados, ampliando o risco de violações a direitos fundamentais quando tais ferramentas são utilizadas como fundamento para intervenções estatais na esfera penal.

A fragilidade estrutural da prova produzida por reconhecimento facial já é tema consolidado na jurisprudência brasileira. O Superior Tribunal de Justiça (Brasil, 2024), ao julgar o Tema 1.258 dos recursos repetitivos, reforçou a obrigatoriedade do cumprimento do art. 226 do Código de Processo Penal, destacando que a inobservância do procedimento previsto nesse dispositivo pode comprometer a validade da prova de reconhecimento. O tribunal também firmou o entendimento de que o reconhecimento deve ser corroborado por outros elementos probatórios, afastando a condenação fundada exclusivamente nesse meio de prova, conforme se verifica da seguinte ementa:

(...) II. QUESTÃO EM DISCUSSÃO 2. Há duas questões em discussão: (i) definir se a nulidade do reconhecimento pessoal, realizada sem as formalidades do art. 226 do CPP, afeta os demais reconhecimentos e provas no processo; (ii) estabelecer se, diante da nulidade do reconhecimento pessoal, subsistem outras provas suficientes para manter a condenação. III. RAZÕES DE DECIDIR 3. O reconhecimento pessoal do réu, realizado em desconformidade com o art. 226 do CPP, é nulo e não convalida reconhecimentos posteriores, ainda que realizados em Juízo. (...) 5. A nulidade do reconhecimento inicial contamina os subsequentes, conforme entendimento consolidado por esta Corte, especialmente quando não há outras provas independentes que confirmem a autoria delitiva. 6. A condenação, baseada em reconhecimento pessoal irregular e sem provas independentes que demonstrem a autoria, deve ser afastada, em observância ao princípio da presunção de inocência. (...). Recurso desprovido. (Brasil, 2024).

Esse entendimento é tanto mais relevante quando se trata do reconhecimento produzido por vigilância em massa: o resultado do algoritmo, gerado de forma automática, sem a presença do acusado, sem contraditório e sem qualquer supervisão judicial no momento da identificação, não pode ser tratado como prova

suficiente de autoria delitiva.

O STF também reconheceu a relevância constitucional do tema ao afetar, sob o rito da repercussão geral, a discussão acerca da validade probatória do reconhecimento pessoal realizado em desconformidade com o art. 226 do Código de Processo Penal (Brasil, 2025). O Tema 1.380 da Repercussão Geral coloca em debate a compatibilidade dessa prática com as garantias do devido processo legal, da ampla defesa e da vedação às provas ilícitas, nos seguintes termos:

(...) II. Questão em discussão 2. A questão em discussão consiste em saber se o reconhecimento de pessoa investigada ou processada pela prática de ilícito criminal sem a observância do procedimento do art. 226 do Código de Processo Penal viola as garantias constitucionais do devido processo legal, da ampla defesa e da vedação às provas ilícitas (CF/1988, art. 5º, LIV, LV e LVI). III. Razões de decidir 3. A Resolução CNJ nº 484/2022, que estabelece diretrizes para a realização do reconhecimento de pessoas em procedimentos e processos criminais, registrou que “o reconhecimento de pessoas equivocado é uma das principais causas de erro judiciário”. Ressaltou, ainda, que pesquisa realizada pela Defensoria Pública do Estado do Estado do Rio de Janeiro anotou que “em 83% dos casos de reconhecimento equivocado as pessoas apontadas eram negras, o que reforça as marcas da seletividade e do racismo estrutural do sistema de justiça criminal”. (...) (Brasil, 2025).

De acordo com a Constituição Federal (Brasil, 1988), a presunção de inocência, prevista no art. 5º, inciso LVII, garante que ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória. Quando a identificação produzida por um sistema de vigilância em massa é tratada como indício suficiente de autoria, opera-se uma inversão indireta do ônus da prova: na prática, exige-se que o acusado demonstre a falha do sistema, e não que o Estado prove a autoria delitiva.

Leite e Bahia (2023) destacam que esse deslocamento é especialmente problemático porque coloca o réu em posição de inferioridade epistêmica, com sua narrativa sistematicamente desvalorizada em razão de estereótipos sociais, raciais e processuais que comprometem a distribuição equitativa de credibilidade no processo penal.

O devido processo legal, o contraditório e a ampla defesa também podem ser prejudicados pela opacidade dos algoritmos. Muitos sistemas apresentam funcionamento pouco transparente, dificultando o acesso da defesa às informações técnicas necessárias para questionar a confiabilidade da ferramenta utilizada. Sem clareza quanto aos critérios de funcionamento, às taxas de erro e aos métodos de treinamento empregados, o contraditório fica limitado a uma impugnação formal incapaz de desconstruir a aparente objetividade da prova tecnológica.

O processo penal, que deveria constituir um espaço de debate dialético entre acusação e defesa, sob a supervisão de um juiz imparcial, corre o risco de transformar-se em mera ratificação de decisões tecnológicas previamente adotadas, sem qualquer participação ou possibilidade de intervenção do acusado (Amaral et al., 2025).

Embora a LGPD represente um avanço na tutela de dados pessoais, ela não disciplina especificamente o uso do reconhecimento facial na persecução penal. A ausência de regras específicas para coleta, armazenamento, auditoria e descarte de dados biométricos captados em sistemas de vigilância em massa cria um vácuo jurídico passível de exploração abusiva. Há, portanto, uma expansão desordenada de mecanismos de vigilância no âmbito da justiça criminal, sem parâmetros normativos claros e sem fiscalização independente adequada (Amaral et al., 2025).

A inovação tecnológica avança em ritmo superior à consolidação das garantias jurídicas, e a ausência de regulação específica para esse uso representa um risco concreto ao Estado de Direito. Diante desse panorama, impõe-se a necessidade de critérios rigorosos para o uso processual do reconhecimento facial: controle judicial prévio para autorizar a coleta e o uso das imagens; auditorias técnicas independentes sobre os sistemas utilizados; transparência obrigatória sobre taxas de erro e vieses dos algoritmos; e exigência irrestrita de corroboração probatória, de modo que o resultado do reconhecimento facial nunca possa ser a única prova de autoria delitiva.

A tecnologia pode auxiliar a investigação criminal, mas não pode substituir o exame crítico humano nem dispensar o debate contraditório. O reconhecimento facial no sistema de justiça brasileiro não representa apenas um avanço técnico, mas um desafio constitucional complexo. A eficiência estatal não pode se sobrepor à dignidade da pessoa humana, à presunção de inocência e ao devido processo legal. Sem salvaguardas adequadas, o risco transcende o erro individual e aponta para a erosão progressiva das bases democráticas do processo penal.

5 CONSIDERAÇÕES FINAIS

A implementação de sistemas de vigilância em massa, especialmente o reconhecimento facial, intensifica a discussão sobre a colisão entre direitos fundamentais e interesses coletivos na segurança pública. Embora a segurança seja dever estatal constitucional, sua efetivação não pode ocorrer com restrições

desproporcionais a direitos como intimidade, vida privada, personalidade e o direito de não produzir prova contra si mesmo. Assim, tais tecnologias devem respeitar os princípios da proporcionalidade, adequação e necessidade, em conformidade com a Constituição Federal e a dignidade da pessoa humana.

A LGPD (Brasil, 2018) representa avanço na proteção de dados, mas o uso do reconhecimento facial pelo Estado revela limitações relevantes, especialmente na segurança pública e investigação criminal. Os dados biométricos são sensíveis e exigem proteção reforçada; contudo, o art. 4º, III, exclui essas atividades da LGPD, gerando lacuna normativa e permitindo o uso sem critérios claros de controle, transparência e necessidade. Nesse contexto, a ausência de regulamentação específica compromete a proteção de dados e amplia riscos de violações à privacidade, discriminação algorítmica e vigilância em massa, tornando essencial a criação de mecanismos legais de controle e fiscalização.

A utilização do reconhecimento facial na persecução penal traz implicações constitucionais relevantes, atingindo de forma desproporcional grupos vulnerabilizados. O sistema opera de forma contínua e sem suspeita individualizada, e os erros algorítmicos são estruturais, afetando principalmente pessoas negras e mulheres. Nesse sentido, o STJ afasta condenações baseadas apenas em reconhecimento não corroborado, enquanto o STF discute sua compatibilidade com o devido processo legal (Brasil, 2024; Brasil, 2025).

Além disso, a presunção de inocência é enfraquecida quando o acusado precisa provar falhas do sistema, o que é dificultado pela opacidade algorítmica. Por isso, o uso do reconhecimento facial deve depender de autorização judicial, auditorias independentes, divulgação de taxas de erro e vedação de sua utilização como prova exclusiva.

Embora a tecnologia possa auxiliar investigações, não substitui a análise judicial nem o contraditório. Assim, é indispensável legislação específica construída com debate público, como o Projeto de Lei nº 3.069/2022 (Brasil, 2022b), de autoria do ex-deputado federal Subtenente Gonzaga, que busca regulamentar o uso da tecnologia (Brasil, 2022a). O projeto representa avanço ao prever diretrizes para coleta, tratamento e descarte de dados, mas não é suficiente por si só, sendo necessários mecanismos rigorosos de transparência, controle e responsabilização estatal.

Diante dos fatos, confirma-se a hipótese de que o uso do reconhecimento

facial sem regulamentação adequada representa risco aos direitos fundamentais. A ausência de normas claras favorece práticas abusivas incompatíveis com dignidade, privacidade e garantias processuais.

O estudo contribui para o debate sobre reconhecimento facial na segurança pública e seus impactos nos direitos fundamentais, destacando a necessidade de regulamentação. Como limitação, aponta-se a ausência de pesquisa empírica. Logo, sugere-se que estudos futuros analisem experiências e mecanismos de auditoria algorítmica e responsabilização estatal, visando maior equilíbrio entre inovação tecnológica, segurança pública e proteção de direitos fundamentais.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. 5. ed. alemã. São Paulo: Malheiros Editores, 2008.

AMARAL, Augusto Jobim do; TRAVASSOS, Gabriel Saad; ANDREATA, Samuel Medeiros. Reconhecimento facial e inteligência artificial: limites regulatórios entre Brasil e Reino Unido. **Revista Jurídica Gralha Azul**, [S. l.], v. 1, n. 28, 2025. Disponível em: <https://revista.tjpr.jus.br/gralhaazul/article/view/194>. Acesso em: 14 abr. 2026.

BRASIL. Câmara dos Deputados. **Parecer ou documento legislativo relacionado ao PL 3.069/2022**. Brasília, DF: Câmara dos Deputados, 2022a. Disponível em: [Câmara dos Deputados. Parecer ou documento legislativo relacionado ao PL 3.069/2022](#). Acesso em: 26 maio 2026.

BRASIL. Câmara dos Deputados. **Projeto de Lei n.º 3.069/2022**. Dispõe sobre a tramitação da proposição. Brasília, DF: Câmara dos Deputados, 2022b. Disponível em: [Câmara dos Deputados – Ficha de tramitação do PL 3069/2022](#). Acesso em: 26 maio 2026.

BRASIL. Constituição (1988). **Emenda Constitucional n. 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022c. Disponível em: [Planalto – Emenda Constitucional nº 115/2022](#). Acesso em: 3 maio 2026.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: [Constituição da República Federativa do Brasil de 1988](#). Acesso em: 14 abr. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: [Planalto](#). Acesso em: 14 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Habeas Corpus n. 819.550/SP**. Relatora: Ministra Daniela Teixeira. Quinta Turma, julgado em 05 nov. 2024. *Diário da Justiça Eletrônico*, Brasília, DF, 06 nov. 2024. Disponível em: [Agravo Regimental no Habeas Corpus n. 819.550/SP](#). Acesso em: 30 maio 2026.

BRASIL. Supremo Tribunal Federal. **Habeas Corpus n. 82.424/RS**. Relator originário: Min. Moreira Alves. Redator para o acórdão: Min. Maurício Corrêa. Tribunal Pleno. Julgado em 17 set. 2003. *Diário da Justiça*, Brasília, DF, 19 mar. 2004. Disponível em: [Habeas Corpus n. 82.424/RS](#). Acesso em: 3 maio 2026.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário com Agravo n. 1.467.470/RG**. Tema 1.380 da Repercussão Geral. Julgado em 28 fev. 2025. Disponível em: [STF - RE com Agravo n. 1.467.470/RG](#). Acesso em: 30 maio 2026.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário n. 1.292.275 AgR/RJ**. Relator: Ministro Dias Toffoli. Primeira Turma. Julgado em 3 maio 2023. *Diário da Justiça Eletrônico*, Brasília, DF, publicação em 22 maio 2023. Disponível em: [STF – RE 1292275 AgR/RJ](#). Acesso em: 30 maio 2026.

CANI, Luiz Eduardo; NUNES, João Alcantara. Erros judiciais em tempos de digital surveillance: os algoritmos de reconhecimento facial em questão. **Revista Brasileira de Direito Processual Penal**, [S. l.], v. 8, n. 2, 2022. DOI: 10.22197/rbdpp.v8i2.720. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/720>. Acesso em: 11 jun. 2026.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2019.

DURÃES, Uesley. Reconhecimento facial: erros expõem falta de transparência e viés racista. **UOL Notícias**, São Paulo, 28 abr. 2024. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/04/28/reconhecimento-facial-erros-falta-de-transparencia.htm>. Acesso em: 29 maio 2026.

GROTHER, Patrick J.; NGAN, Mei; HANAOKA, Kayee K. **Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects**. NIST Interagency/Internal Report (NISTIR) 8280. Gaithersburg, MD: National Institute of Standards and Technology, 2019. Disponível em: <https://doi.org/10.6028/NIST.IR.8280>. Acesso em: maio 2026.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO DE JANEIRO (ITS RIO). **7 recomendações para a regulação do reconhecimento facial**. Rio de Janeiro, 2021. Disponível em: <https://itsrio.org/pt/artigos/7-recomendacoes-para-a-regulacao-do-reconhecimento-facial/>. Acesso em: 05 maio 2026.

LEITE, Sara Ribas Ortigosa Leite; BAHIA, Claudio José Amaral. O erro judiciário e a injustiça epistêmica no reconhecimento de pessoas. **Revista Brasileira de Direito Processual Penal**, [S. l.], v. 9, n. 2, 2023. DOI: 10.22197/rbdpp.v9i2.815. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/815>. Acesso em: 11 jun. 2026.

MACHADO, Gabriela Mendes; BARROS, Vinícius Diniz Monteiro de. RECONHECIMENTO FACIAL POR INTELIGÊNCIA ARTIFICIAL E PRINCÍPIO DA INOCÊNCIA: investigações em torno dos processos penais brasileiro e comparado. **Revista EJEJ**, Belo Horizonte, Brasil, v. 1, n. 1, 2024. DOI: 10.70982/rejef.v1i4.47. Disponível em: <http://revistaejef.tjmg.jus.br/index.php/revista-ejef/article/view/47>. Acesso em: 11 jun. 2026.

MORAES, Alexandre de. **Direito Constitucional**. 41. ed. Rio de Janeiro: Atlas, 2025. E-book. pág.40. ISBN 9786559777143. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559777143/>. Acesso em: 3 maio. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos**. Brasília, DF: UNICEF Brasil, 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 29 maio 2026.

PRIVACY INTERNATIONAL. **Mass surveillance**. Londres: Privacy International, [s.d.]. Disponível em: [Privacy International](https://www.privacyinternational.org/). Acesso em: 29 maio 2026.

REY, Bruna; FRANCESCATO, Caroline. O uso do reconhecimento facial na segurança pública: proteção ou ameaça aos direitos fundamentais da população? **IBEROJUR**, 2025. Disponível em: <https://repositorioiberojur.com/index.php/catalog/catalog/download/43/806/884?inline=1>. Acesso em: 30 maio 2026.

SAES, Wandimara Pereira dos Santos. Colisão de direitos fundamentais: princípio da dignidade humana como critério material de ponderação. **Revista de Direito Constitucional e Internacional**, São Paulo, v. 76, p. 115-138, jul./set. 2011. Disponível em: https://www.cjf.jus.br/caju/colisao.direitos.fundamentais_1.pdf. Acesso em: 3 maio 2026.

SANTIAGO, Abinoan. Me urinei de medo ao ser levada no camburão da PM por erro de IA. **UOL Tilt**, Florianópolis, 15 nov. 2023. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2023/11/15/erro-camera-reconhecimento-facial.htm>. Acesso em: 29 maio 2026.

SANTOS, Jéssica Guedes. Reconhecimento facial: entre a criminologia, a mídia e a LGPD penal. **Internet & Sociedade**, São Paulo, v. 2, n. 1, p. 214–232, jun. 2021.

SANTOS, Jevan Batista. Dignidade da pessoa humana. **Revista FT**, v. 29, ed. 146, maio 2025. Disponível em: <https://revistaft.com.br/dignidade-da-pessoa-humana/>. Acesso em: 30 maio 2026.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 3. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2014.

SILVA, Lorena Abbas da; FRANQUEIRA, Bruna Diniz; HARTMANN, Ivar A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança

pública e regulação na América Latina. **Revista Digital de Direito Administrativo**, Ribeirão Preto, v. 8, n. 1, p. 171-204, 2021. Disponível em: <https://revistas.usp.br/rdda/es/article/view/173903/168395>. Acesso em: 6 maio 2026.

SOUZA, Carlos Affonso. A privacidade saiu dos trilhos no metrô de São Paulo. **UOL**, São Paulo, 18 abr. 2018. Disponível em: <https://tecfront.blogosfera.uol.com.br/2018/04/18/a-privacidade-saiu-dos-trilhos-no-metro-de-sao-paulo/>. Acesso em: 05 maio 2026.

TRIBUNAL DE JUSTIÇA DO ESTADO DE MINAS GERAIS (TJMG). **Jurisprudência – conflito entre direitos fundamentais constitucionais, proporcionalidade, dignidade da pessoa humana e princípios constitucionais**. Belo Horizonte: TJMG. Disponível em: [TJMG - Jurisprudência – conflito entre direitos fundamentais constitucionais, proporcionalidade, dignidade da pessoa humana e princípios constitucionais](#). Acesso em: 3 maio 2026

NETO, Manoel Zeferino de Magalhães. O reconhecimento facial e o direito de não ser confundido prisões indevidas e a responsabilização do agente público. **Periódicos Brasil. Pesquisa Científica**, Macapá, Brasil, v. 4, n. 2, p. 674–696, 2025. DOI: 10.36557/pbpc.v4i2.435. Disponível em: <https://periodicosbrasil.emnuvens.com.br/revista/article/view/435>. Acesso em: 11 jun. 2026.

3 CONSIDERAÇÕES FINAIS

A implementação de sistemas de vigilância em massa, especialmente o reconhecimento facial, intensifica a discussão sobre a colisão entre direitos fundamentais e interesses coletivos na segurança pública. Embora a segurança seja dever estatal constitucional, sua efetivação não pode ocorrer com restrições desproporcionais a direitos como intimidade, vida privada, personalidade e o direito de não produzir prova contra si mesmo. Assim, tais tecnologias devem respeitar os princípios da proporcionalidade, adequação e necessidade, em conformidade com a Constituição Federal e a dignidade da pessoa humana.

A LGPD (Brasil, 2018) representa avanço na proteção de dados, mas o uso do reconhecimento facial pelo Estado revela limitações relevantes, especialmente na segurança pública e investigação criminal. Os dados biométricos são sensíveis e exigem proteção reforçada; contudo, o art. 4º, III, exclui essas atividades da LGPD, gerando lacuna normativa e permitindo o uso sem critérios claros de controle, transparência e necessidade. Nesse contexto, a ausência de regulamentação específica compromete a proteção de dados e amplia riscos de violações à privacidade, discriminação algorítmica e vigilância em massa, tornando essencial a criação de mecanismos legais de controle e fiscalização.

A utilização do reconhecimento facial na persecução penal traz implicações constitucionais relevantes, atingindo de forma desproporcional grupos vulnerabilizados. O sistema opera de forma contínua e sem suspeita individualizada, e os erros algorítmicos são estruturais, afetando principalmente pessoas negras e mulheres. Nesse sentido, o STJ afasta condenações baseadas apenas em reconhecimento não corroborado, enquanto o STF discute sua compatibilidade com o devido processo legal (Brasil, 2024; Brasil, 2025).

Além disso, a presunção de inocência é enfraquecida quando o acusado precisa provar falhas do sistema, o que é dificultado pela opacidade algorítmica. Por isso, o uso do reconhecimento facial deve depender de autorização judicial, auditorias independentes, divulgação de taxas de erro e vedação de sua utilização como prova exclusiva.

Embora a tecnologia possa auxiliar investigações, não substitui a análise judicial nem o contraditório. Assim, é indispensável legislação específica construída com debate público, como o Projeto de Lei nº 3.069/2022 (Brasil, 2022b), de autoria do ex-deputado federal Subtenente Gonzaga, que busca regulamentar o uso da

tecnologia (Brasil, 2022a). O projeto representa avanço ao prever diretrizes para coleta, tratamento e descarte de dados, mas não é suficiente por si só, sendo necessários mecanismos rigorosos de transparência, controle e responsabilização estatal.

Diante dos fatos, confirma-se a hipótese de que o uso do reconhecimento facial sem regulamentação adequada representa risco aos direitos fundamentais. A ausência de normas claras favorece práticas abusivas incompatíveis com dignidade, privacidade e garantias processuais.

O estudo contribui para o debate sobre reconhecimento facial na segurança pública e seus impactos nos direitos fundamentais, destacando a necessidade de regulamentação. Como limitação, aponta-se a ausência de pesquisa empírica. Logo, sugere-se que estudos futuros analisem experiências e mecanismos de auditoria algorítmica e responsabilização estatal, visando maior equilíbrio entre inovação tecnológica, segurança pública e proteção de direitos fundamentais.

REFERÊNCIAS

BRASIL. Câmara dos Deputados. **Parecer ou documento legislativo relacionado ao PL 3.069/2022**. Brasília, DF: Câmara dos Deputados, 2022a. Disponível em: [Câmara dos Deputados – Documento legislativo codteor 2234118](#). Acesso em: 26 maio 2026.

BRASIL. Câmara dos Deputados. **Projeto de Lei n.º 3.069/2022**. Texto integral do projeto de lei. Brasília, DF: Câmara dos Deputados, 2022b. Disponível em: [Câmara dos Deputados – Integra do PL 3069/2022](#). Acesso em: 26 maio 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: [Planalto](#). Acesso em: 14 abr. 2026.