OS LIMITES DO RECONHECIMENTO FACIAL POR INTELIGÊNCIA ARTIFICIAL E O DIREITO À PRIVACIDADE

Bruce Willian da Silva[1]

RESUMO
O uso de tecnologias de reconhecimento facial baseadas em inteligência artificial (IA) tem se expandido em diversos contextos, como segurança pública, controle de fronteiras e serviços privados. No entanto, essa difusão suscita intensos debates sobre seus impactos na esfera dos direitos fundamentais, em especial no direito à privacidade. O presente artigo analisa criticamente os limites do reconhecimento facial sob a perspectiva constitucional, destacando riscos de vigilância em massa, discriminação algorítmica e violação de garantias individuais. A pesquisa adota abordagem interdisciplinar, dialogando com a doutrina jurídica, documentos internacionais de direitos humanos e decisões judiciais brasileiras e estrangeiras, a fim de examinar a compatibilidade do uso dessa tecnologia com os princípios da dignidade da pessoa humana, da proporcionalidade e da proteção de dados pessoais. A ausência de regulamentação específica no Brasil potencializa riscos à privacidade e acentua desigualdades sociais, tornando imprescindível a construção de um marco regulatório que assegure transparência, controle democrático e respeito aos direitos fundamentais frente às inovações tecnológicas.

Palavras-chave: Direitos Fundamentais; Inteligência Artificial; Reconhecimento Facial; Regulação Tecnológica.

ABSTRACT
The use of facial recognition technologies based on artificial intelligence (AI) has expanded in various contexts, such as public security, border control, and private services. However, this diffusion has sparked intense debate about its impact on fundamental rights, particularly the right to privacy. This article critically analyzes the limits of facial recognition from a constitutional perspective, highlighting the risks of mass surveillance, algorithmic discrimination, and violations of individual rights. The research adopts an interdisciplinary approach, engaging with legal doctrine, international human rights documents, and Brazilian and foreign court decisions to examine the compatibility of this technology's use with the principles of human dignity, proportionality, and the protection of personal data. The lack of specific regulation in Brazil increases privacy risks and exacerbates social inequalities, making it essential to develop a regulatory framework that ensures transparency, democratic oversight, and respect for fundamental rights in the face of technological innovations.

Keywords: Fundamental Rights; Artificial Intelligence; Facial Recognition; Technological Regulation.

1. INTRODUÇÃO

Nas últimas décadas, a expansão das tecnologias de inteligência artificial (IA) tem transformado profundamente a forma como indivíduos, empresas e Estados interagem com

[1]Discente do curso de Direito, 10° semestre, da Universidade Federal do Mato Grosso do Sul, Campus do Pantanal, e-mail: bruce.willian@ufms.br

dados e informações. Dentre essas inovações, o reconhecimento facial desponta como um dos instrumentos mais controversos, seja pela sua aplicabilidade em áreas estratégicas como segurança pública, vigilância urbana e controle de fronteiras, seja pelos riscos que representa aos direitos fundamentais, especialmente ao direito à privacidade e à proteção de dados pessoais.

A crescente adoção de sistemas de reconhecimento facial no Brasil e no mundo evidencia um duplo movimento: de um lado, a promessa de maior eficiência na identificação de pessoas, na prevenção de crimes e no fornecimento de serviços; de outro, a intensificação de preocupações acerca de violações de garantias constitucionais, reforço de práticas discriminatórias e vigilância em massa. Esse cenário torna urgente a análise crítica dos limites jurídicos e éticos da utilização dessa tecnologia.

No plano normativo, observa-se que, enquanto países como a União Europeia vêm avançando em regulamentações mais restritivas, por meio de instrumentos como o AI Act, o Brasil ainda carece de um marco regulatório específico sobre reconhecimento facial. Apesar da aprovação da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), que estabelece diretrizes relevantes para o tratamento de informações pessoais, não há disciplina detalhada sobre os riscos decorrentes da aplicação dessa tecnologia em larga escala, o que gera insegurança jurídica e abre espaço para violações aos direitos fundamentais.

Diante disso, o problema de pesquisa que orienta este artigo é formulado nos seguintes termos: quais são os limites constitucionais e jurídicos do uso de tecnologias de reconhecimento facial no Brasil, especialmente à luz do direito à privacidade e da proteção de dados pessoais? O objetivo geral consiste em analisar criticamente o reconhecimento facial por inteligência artificial, considerando sua compatibilidade com os direitos fundamentais previstos na Constituição de 1988 e em tratados internacionais de direitos humanos. Especificamente, pretende-se: investigar o marco normativo nacional e internacional aplicável ao tema; avaliar os riscos sociais e jurídicos relacionados à vigilância e ao uso discriminatório dessa tecnologia; e discutir a necessidade de um marco regulatório específico que assegure transparência, controle democrático e respeito aos direitos fundamentais.

Do ponto de vista metodológico, o trabalho adota abordagem qualitativa, com base em pesquisa bibliográfica e documental, incluindo análise de doutrina, legislação, jurisprudência nacional e internacional, bem como documentos técnicos produzidos por organismos multilaterais e organizações da sociedade civil.

Portanto, este estudo se justifica não apenas pela atualidade e relevância social do tema, mas também pela necessidade de fomentar um debate jurídico crítico sobre os limites do

reconhecimento facial no contexto brasileiro, em diálogo com experiências estrangeiras e com os princípios constitucionais que orientam a proteção da dignidade da pessoa humana.

2. RECONHECIMENTO FACIAL E SEUS DESAFIOS TECNOLÓGICOS E SOCIAIS

O reconhecimento facial é uma tecnologia de identificação biométrica que utiliza algoritmos de inteligência artificial para mapear características únicas do rosto humano e compará-las a bancos de dados previamente existentes (Cavalcanti, 2021). Trata-se de uma subárea da visão computacional, que combina técnicas de aprendizado de máquina (*machine learning*) e redes neurais profundas (*deep learning*), possibilitando a extração de padrões em imagens e vídeos em tempo real (Cavalcanti, 2021).

Segundo o relatório da National Institute of Standards and Technology (NIST, 2019), os sistemas de reconhecimento facial apresentam altos índices de acurácia em ambientes controlados, mas sua eficiência cai significativamente em contextos de iluminação irregular, movimentação intensa ou baixa qualidade das câmeras. Ademais, pesquisas recentes demonstram que os algoritmos apresentam vieses raciais e de gênero, resultando em maior margem de erro na identificação de mulheres, pessoas negras e populações não brancas (Buolamwini; Gebru, 2018).

No Brasil, a adoção dessa tecnologia tem ocorrido de forma acelerada, principalmente por órgãos de segurança pública e empresas privadas de transporte, comércio e serviços financeiros, ainda que sem regulação específica que discipline seu alcance, limites e responsabilidades (Cavalcanti, 2021).

2.1 ÁREAS DE APLICAÇÃO - SEGURANÇA PÚBLICA, SETOR PRIVADO E FRONTEIRAS

O principal campo de uso do reconhecimento facial no Brasil tem sido a segurança pública. Experiências em estados como Rio de Janeiro, Bahia e São Paulo incluem a instalação de câmeras inteligentes em espaços públicos, como metrôs, estádios e festas populares. Em 2019, por exemplo, a Secretaria de Segurança Pública da Bahia anunciou a prisão de mais de 100 pessoas em eventos carnavalescos com base em sistemas de reconhecimento facial (G1 Bahia, 2019).

No setor privado, grandes redes varejistas e instituições bancárias passaram a adotar a biometria facial tanto para fins de autenticação de usuários quanto para estratégias de marketing personalizadas. Contudo, essa utilização suscita críticas por ocorrer muitas vezes

sem consentimento informado, ferindo princípios da Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

Já em fronteiras, aeroportos e rodoviárias, a tecnologia é empregada no controle migratório, em consonância com práticas globais, como ocorre nos Estados Unidos e na União Europeia. Todavia, diferentemente do que se observa no *General Data Protection Regulation* (GDPR) europeu, no Brasil ainda não há regras claras que estabeleçam salvaguardas à privacidade do passageiro (Cavalcanti, 2021).

Apesar de sua promessa de eficiência, o reconhecimento facial é alvo de críticas pela possibilidade de instaurar um regime de vigilância permanente, que reduz drasticamente a esfera de anonimato no espaço público. Para Shoshana Zuboff (2019) a sociedade contemporânea vive sob a lógica do "capitalismo de vigilância", no qual dados biométricos se tornam recurso estratégico para governos e corporações.

Erros de identificação, amplamente documentados, representam outro problema central (Zuboff, 2019). O estudo da NIST (2019) mostrou que a probabilidade de falso positivo em pessoas negras e asiáticas é até 100 vezes maior que em pessoas brancas. Casos de prisões indevidas em cidades norte-americanas, como Detroit e Nova Jérsei, demonstram que tais falhas podem gerar graves violações de direitos, especialmente quando associadas a políticas criminais seletivas.

No contexto brasileiro, marcado por desigualdades raciais e sociais estruturais, esses riscos assumem contornos ainda mais preocupantes, pois tendem a reforçar o viés seletivo já existente no sistema penal. A intersecção entre gênero, raça e classe social aponta para maior vulnerabilidade de mulheres negras e jovens periféricos diante da expansão dessa tecnologia.

2.2 PANORAMA DE USO NO BRASIL E NO CENÁRIO INTERNACIONAL

De acordo com levantamento do InternetLab (2021), pelo menos 20 unidades da federação já testaram ou implantaram sistemas de reconhecimento facial em algum nível, especialmente para fins de segurança pública (InternetLab, 2021). Contudo, tais projetos são marcados pela ausência de transparência: não há informações claras sobre contratos, bases de dados utilizadas e mecanismos de auditoria algorítmica.

No plano internacional, observa-se diversidade regulatória. Enquanto países como a China utilizam massivamente a tecnologia para fins de vigilância estatal, a União Europeia propõe, por meio do AI Act, a categorização do reconhecimento facial em tempo real como tecnologia de "alto risco", exigindo autorização prévia e salvaguardas rigorosas. Em contraste, cidades como São Francisco e Boston, nos Estados Unidos, já proibiram o uso governamental

dessa ferramenta, justamente pela preocupação com abusos e falhas técnicas (InternetLab, 2021).

Esse cenário demonstra que o Brasil se encontra em encruzilhada regulatória: pode optar por replicar experiências de controle democrático e proteção de dados ou, ao contrário, aprofundar práticas de vigilância sem amparo legal adequado, ampliando riscos às liberdades civis e ao direito à privacidade (InternetLab, 2021).

3. FUNDAMENTOS CONSTITUCIONAIS E DIREITOS FUNDAMENTAIS NO USO DO RECONHECIMENTO FACIAL

A Constituição Federal de 1988 consagrou a dignidade da pessoa humana como um dos pilares da República (art. 1º, III). Essa cláusula fundamental funciona como núcleo axiológico do sistema jurídico e orienta a interpretação dos direitos fundamentais.

Segundo Ingo Wolfgang Sarlet (2001), a dignidade humana é tanto princípio quanto valor jurídico, implicando um limite material ao exercício do poder estatal e das práticas privadas. Nesse sentido, tecnologias que afetam a esfera mais íntima da vida, como o reconhecimento facial, que captura e processa dados biométricos, devem ser avaliadas sob o prisma da compatibilidade com a dignidade, evitando situações de redução da pessoa a objeto de vigilância ou de tratamento discriminatório.

No mesmo sentido, Luís Roberto Barroso (2019) sustenta que a dignidade funciona como parâmetro de ponderação entre inovação tecnológica e preservação dos direitos individuais, exigindo que qualquer uso invasivo de dados pessoais seja justificado por finalidade legítima, proporcional e necessário em um Estado Democrático de Direito.

3.1 O DIREITO À PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

O direito à privacidade, previsto no art. 5º, X, da Constituição Federal, assegura a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas. Essa proteção, em tempos de sociedade digital, deve ser interpretada de modo a abarcar também o direito à autodeterminação informativa, isto é, o poder de o indivíduo controlar o uso de seus dados pessoais (Doneda, 2006).

Com a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), o Brasil passou a reconhecer expressamente a proteção de dados como dimensão autônoma da privacidade. O Supremo Tribunal Federal reforçou esse entendimento no julgamento da ADI 6.387 (Rel. Min. Rosa Weber, 2020), reconhecendo a proteção de dados pessoais como direito

fundamental autônomo, mesmo antes da Emenda Constitucional nº 115/2022, que positivou o tema no art. 5º, LXXIX.

No caso do reconhecimento facial, a coleta e o tratamento de dados biométricos configuram dados pessoais sensíveis (art. 5º, II, LGPD), exigindo hipóteses estritas de tratamento, como consentimento expresso ou fundamento legal específico. A ausência de transparência sobre bases de dados, critérios algorítmicos e mecanismos de fiscalização contraria diretamente os princípios da finalidade, necessidade e proporcionalidade previstos na LGPD (LGPD (Lei nº 13.709/2018)).

O uso crescente de tecnologias de reconhecimento facial levanta preocupações significativas sobre a proteção da privacidade, especialmente no contexto de dados biométricos sensíveis. Como lembra Doneda (2006, p. 25), "a privacidade deve ser entendida como um direito fundamental de primeira grandeza, ligado à própria noção de dignidade da pessoa humana, funcionando como limite à ingerência do Estado e de particulares na vida das pessoas". Essa compreensão reforça que o tratamento de dados biométricos exige cuidado especial, alinhado aos princípios da finalidade, necessidade e proporcionalidade previstos na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

A LGPD, ao classificar dados biométricos como sensíveis, impõe hipóteses estritas para seu tratamento. Segundo Mendes, Doneda e Sarlet (2020, p. 97), "os dados biométricos estão entre os mais sensíveis, pois permitem a identificação unívoca do indivíduo, e, por isso, exigem regime mais rigoroso de proteção, sob pena de se comprometer o núcleo essencial do direito à privacidade." A ausência de transparência sobre bases de dados, critérios algorítmicos e mecanismos de fiscalização, portanto, viola diretamente esses preceitos legais.

No plano conceitual mais amplo, a vigilância digital também representa um desafio ao controle individual sobre informações pessoais. Zuboff (2019, p. 45) observa que "na era do capitalismo de vigilância, a extração e o processamento de dados pessoais deixam de ser meros instrumentos e passam a constituir a principal fonte de poder e dominação sobre indivíduos e sociedades". Stefano Rodotà (2008, p. 41) reforça essa perspectiva ao afirmar que "o direito à proteção de dados pessoais representa uma nova forma de tutela da liberdade, pois o controle sobre a circulação das informações é condição indispensável para a preservação da identidade pessoal".

Finalmente, do ponto de vista constitucional, Luís Roberto Barroso (2021, p. 363) destaca que "o direito à privacidade é parte do patrimônio jurídico da cidadania, integrando o rol dos direitos fundamentais e funcionando como um freio ao exercício abusivo do poder público e privado." Esse fundamento evidencia que qualquer implementação de sistemas de reconhecimento facial deve ser precedida de regulamentação clara, garantindo que a

tecnologia não se transforme em instrumento de vigilância desproporcional ou violação de direitos.

3.2 PROPORCIONALIDADE E LIMITES AO PODER DE VIGILÂNCIA ESTATAL NO ÂMBITO INTERNACIONAL

A proporcionalidade, derivada do devido processo constitucional, é critério central para avaliar a legitimidade de restrições a direitos fundamentais. Segundo Robert Alexy (2008), esse princípio envolve três subprincípios: adequação, necessidade e proporcionalidade em sentido estrito.

Aplicando ao reconhecimento facial:

- Adequação: a tecnologia deve ser apta a atingir um fim legítimo (ex.: segurança pública).
- Necessidade: deve-se verificar se não há medidas menos invasivas igualmente eficazes.
- Proporcionalidade em sentido estrito: é preciso ponderar se os benefícios obtidos superam as restrições impostas à privacidade e liberdade dos cidadãos.

No Brasil, experiências de uso indiscriminado em locais de grande circulação pública não passam pelo crivo da proporcionalidade, já que não distinguem entre suspeitos e cidadãos comuns, configurando verdadeira vigilância em massa (Doneda, 2006).

O Supremo Tribunal Federal, em julgados como a ADPF 347 (2015), já reconheceu a gravidade estrutural de violações a direitos fundamentais quando há falhas sistêmicas na proteção da dignidade humana.

O princípio da proporcionalidade e a proteção de direitos fundamentais, reafirmados pelo Supremo Tribunal Federal na ADPF 347, oferecem referência relevante para o debate sobre o uso do reconhecimento facial em espaços públicos. Na ADPF 347, o STF reconheceu que a superlotação e condições degradantes do sistema prisional configuravam violação a preceitos fundamentais, determinando a adoção de medidas que priorizassem alternativas proporcionais à prisão preventiva e garantissem responsabilidade estatal e fiscalização judicial (BRASIL, STF, ADPF 347, 2015).

Embora a decisão trate do sistema prisional, o princípio da proporcionalidade é aplicável ao uso de tecnologias de vigilância. Sistemas de reconhecimento facial implementados de forma indiscriminada em locais de grande circulação, sem distinção entre suspeitos e cidadãos comuns, reproduzem, em certa medida, a lógica de controle massivo condenada pelo STF, colocando em risco direitos como privacidade, liberdade e dignidade

humana. Como destaca Doneda (2006, p. 25) que “a privacidade deve ser entendida como um direito fundamental de primeira grandeza, ligado à própria noção de dignidade da pessoa humana, funcionando como limite à ingerência do Estado e de particulares na vida das pessoas”.

Portanto, a experiência da ADPF 347 reforça a necessidade de que o uso do reconhecimento facial seja pautado por critérios claros, mecanismos de fiscalização, transparência e respeito à proporcionalidade, evitando a transformação da tecnologia em instrumento de vigilância em massa que comprometa o núcleo essencial dos direitos fundamentais. Embora não tenha ainda julgado casos específicos sobre reconhecimento facial, a jurisprudência do STF indica que tecnologias invasivas devem ser submetidas a controle rigoroso de constitucionalidade.

A análise não pode prescindir do marco internacional dos direitos humanos. O Pacto Internacional sobre Direitos Civis e Políticos (art. 17) e a Convenção Americana sobre Direitos Humanos – Pacto de San José da Costa Rica (art. 11) asseguram a proteção à vida privada contra ingerências arbitrárias do Estado.

Além disso, as Diretrizes da ONU sobre Privacidade na Era Digital (2013) enfatizam que práticas de vigilância em massa violam direitos humanos quando não baseadas em lei clara, finalidade legítima e controle democrático (ONU, 2013).

No âmbito europeu, o Regulamento Geral de Proteção de Dados (GDPR) classifica dados biométricos como sensíveis e impõe salvaguardas adicionais, servindo como parâmetro comparativo para o Brasil (Official Journal of the European Union, L 119, p. 1–88, 2016). O GDPR classifica dados biométricos como dados pessoais sensíveis, determinando que (EUROPEAN UNION, 2016, Art. 9) “o tratamento de dados pessoais que revelem origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, bem como dados genéticos e biométricos destinados a identificar uma pessoa de forma única está sujeito a salvaguardas adicionais”.

O AI Act, em tramitação, propõe ainda restrições severas ao uso de reconhecimento facial em tempo real, admitindo sua utilização apenas em situações excepcionais, como prevenção de ameaças terroristas (EUROPEAN COMMISSION, 2021). O AI Act classifica o uso de reconhecimento facial em tempo real como tecnologia de “alto risco” e estabelece que sua aplicação é permitida apenas em situações excepcionais, incluindo “a prevenção de ameaças terroristas ou crimes graves que coloquem em risco a vida ou a segurança das pessoas” (EUROPEAN COMMISSION, 2021, Art. 5, §1).

A análise demonstra que o reconhecimento facial não é incompatível, em tese, com o ordenamento jurídico brasileiro. Contudo, sua utilização encontra barreiras constitucionais intransponíveis quando realizada de forma indiscriminada, sem transparência e sem controle social.

A dignidade da pessoa humana, a privacidade, a autodeterminação informativa e a proporcionalidade são parâmetros normativos que impõem limites claros ao Estado e ao setor privado. O desafio está em equilibrar os ganhos de eficiência prometidos pela tecnologia com a preservação de um espaço público democrático, onde a vigilância não se torne regra, mas exceção legitimada por finalidades constitucionais específicas.

4. JURISPRUDÊNCIA E EXPERIÊNCIAS COMPARADAS NO USO DO RECONHECIMENTO FACIAL

Embora o Supremo Tribunal Federal (STF) ainda não tenha julgado diretamente casos de reconhecimento facial, algumas decisões apontam diretrizes relevantes, como a ADI 6.387 (STF, Rel. Min. Rosa Weber, 2020), que suspendeu medida provisória que autorizava o compartilhamento massivo de dados pessoais entre órgãos da administração pública, ressaltando que a proteção de dados pessoais é direito fundamental autônomo e que práticas de coleta e tratamento sem limites configuram risco à privacidade.

Na ADI 6.638 (STF, Rel. Min. Gilmar Mendes, 2021), se reafirmou que dados biométricos são sensíveis e só podem ser tratados em hipóteses estritas previstas em lei. Enquanto isso, no STJ – REsp 1.334.097/SP (2013), consolidou-se a noção de que a privacidade é direito da personalidade, protegendo dados pessoais em situações de uso abusivo.

Na esfera infraconstitucional, algumas ações civis públicas questionam projetos de reconhecimento facial em estados como Bahia, Rio de Janeiro e São Paulo, com fundamento na LGPD e na violação da privacidade de transeuntes não investigados. Ainda não há decisão paradigmática, mas o Ministério Público e a Defensoria Pública vêm argumentando que a prática caracteriza vigilância em massa, vedada constitucionalmente.

4.1 EXPERIÊNCIA DOS ESTADOS UNIDOS - EFICIÊNCIA X DISCRIMINAÇÃO ALGORÍTMICA

Nos EUA, o uso do reconhecimento facial para segurança pública e controle migratório se expandiu rapidamente, mas enfrentou forte reação judicial e legislativa (TECH POLICY

PRESS., 2024). Em Carpenter v. United States (2018), a Suprema Corte norte-americana reconheceu que a coleta massiva de dados de geolocalização sem ordem judicial viola a Quarta Emenda (proteção contra buscas e apreensões arbitrárias) (CARPENTER v. UNITED STATES, 585 U.S., 2018).

Na decisão Carpenter v. United States (2018), a Suprema Corte dos EUA reconheceu que "a coleta de registros de localização de celulares de um indivíduo, abrangendo longos períodos de tempo e sem ordem judicial, constitui violação da Quarta Emenda da Constituição dos Estados Unidos, que protege contra buscas e apreensões arbitrárias" (CARPENTER v. UNITED STATES, 2018, p. 1). Embora não trate diretamente de reconhecimento facial, o precedente abriu caminho para contestar vigilâncias tecnológicas invasivas.

Diversos municípios, como São Francisco (2019) e Boston (2020), aprovaram leis proibindo o uso de reconhecimento facial por autoridades públicas, alegando risco de discriminação racial e falhas técnicas (San Francisco, 2019). Estudos do MIT Media Lab (2018) revelaram taxas de erro significativamente maiores na identificação de mulheres negras, evidenciando o viés algorítmico. Essa constatação fortaleceu o debate sobre racismo estrutural refletido em sistemas de IA (BUOLAMWINI, Joy. 2018).

4.2 UNIÃO EUROPEIA - PROTEÇÃO DE DADOS COMO PILAR REGULATÓRIO

A União Europeia adota uma postura mais protetiva. O GDPR (2016/2018) considera dados biométricos como sensíveis, exigindo salvaguardas especiais para seu tratamento (UNIÃO EUROPEIA. Regulamento (UE) 2016/679, 2016). O AI Act (aprovado em 2024) classifica o reconhecimento facial em tempo real como prática de alto risco, admitindo sua utilização apenas em hipóteses excepcionais, como busca por vítimas de sequestro, prevenção de atentados terroristas ou crimes gravíssimos, sempre sob autorização judicial.

O Tribunal Europeu de Direitos Humanos (Caso S. e Marper vs. Reino Unido, 2008) já havia decidido que a coleta indiscriminada de dados biométricos viola o direito à vida privada (art. 8º da Convenção Europeia de Direitos Humanos).

Esse cenário europeu reforça que a proporcionalidade é critério essencial e que a vigilância indiscriminada é incompatível com sociedades democráticas.

4.3 CHINA - VIGILÂNCIA EM MASSA E AUSÊNCIA DE FREIOS CONSTITUCIONAIS

Em contraste, a China implementa o uso do reconhecimento facial em larga escala, integrando-o a sistemas de monitoramento como o “Social Credit System” (WIRED, 2021). Câmeras inteligentes registram comportamentos cotidianos, vinculando-os a recompensas ou punições sociais (HUMAN RIGHTS WATCH, 2021).

Embora eficiente em termos de segurança e controle estatal, essa prática é criticada por organismos internacionais por violar a privacidade, restringir liberdades e institucionalizar a vigilância em massa (WIKIPEDIA, 2021).

A ausência de um sistema robusto de direitos fundamentais permite que a tecnologia seja utilizada como instrumento de controle político, em nítido contraste com democracias constitucionais como Brasil e União Europeia.

Logo, cita-se:

> - Brasil: carece de precedentes diretos no STF, mas jurisprudência e LGPD apontam limites constitucionais claros.
> - EUA: crescente rejeição social e municipal ao reconhecimento facial devido a vieses raciais e riscos à liberdade.
> - EU: marco regulatório avançado (GDPR e AI Act) estabelece freios rígidos, restringindo a prática a situações excepcionais.
> - China: paradigma de vigilância em massa, em desacordo com princípios democráticos de privacidade.

Essa análise comparada revela que o Brasil se encontra em encruzilhada: pode seguir o caminho europeu de regulação protetiva, garantindo direitos fundamentais, ou correr o risco de reproduzir modelos autoritários de vigilância sem freios.

5. O RECONHECIMENTO FACIAL E SUAS FORMAS DE OCORRÊNCIA NO DIREITO PROCESSUAL PENAL

O reconhecimento facial tem se tornado uma ferramenta cada vez mais utilizada no contexto do Direito Processual Penal, seja para identificação de suspeitos, controle de acesso a locais ou suporte na instrução de provas. No entanto, seu emprego envolve desafios jurídicos significativos, pois confronta os princípios da ampla defesa, do devido processo legal e da inviolabilidade da intimidade previstos na Constituição Federal de 1988 (CF, art. 5º, LIV e X).

Segundo Danilo Doneda (2006), tecnologias de vigilância como o reconhecimento facial exigem limites normativos claros, dado que a coleta de dados biométricos representa uma das formas mais intrusivas de tratamento de informações pessoais.

Luís Roberto Barroso (2019) complementa que, em um Estado Democrático de Direito, qualquer instrumento investigativo deve respeitar a proporcionalidade e a dignidade da pessoa humana, evitando a redução de indivíduos a meros objetos de controle tecnológico.

6.1 FORMAS DE OCORRÊNCIA DO RECONHECIMENTO FACIAL NO BRASIL

O reconhecimento facial pode ocorrer de diferentes maneiras no processo penal, cada uma com peculiaridades jurídicas:

- Reconhecimento em tempo real (live recognition). Consiste na identificação imediata de pessoas em locais públicos ou privados por meio de câmeras conectadas a bancos de dados. É utilizado principalmente em ambientes urbanos e eventos de grande concentração. Vantagens: permite rápida identificação de suspeitos e prevenção de delitos (Cavalcanti, 2021). Riscos: há alto potencial de falsos positivos e violação de direitos de terceiros, configurando vigilância em massa. Laura Schertel Mendes (2020) alerta que o uso indiscriminado em espaços públicos compromete a liberdade de circulação e gera um ambiente de suspeição generalizada.
- Reconhecimento facial a partir de registros fotográficos ou videográficos. Nesta modalidade, a identificação é feita posteriormente aos fatos, com base em imagens de câmeras de segurança, mídias sociais ou vídeos amadores. Pode ser utilizada para: Identificar suspeitos em investigações criminais; Cruzar imagens com bases de dados oficiais; Contribuir para a instrução processual como prova documental (Vieira, 2018). Embora menos invasiva que o *live recognition*, ainda exige atenção quanto à autenticidade, integridade e guarda das imagens, sob pena de nulidade da prova (STJ, HC 598.051/SP, 2021).
- Reconhecimento facial em flagrante e prisões: Em situações de flagrante delito, o reconhecimento facial pode apoiar a polícia na identificação rápida de suspeitos, confirmando presença em determinada cena. Contudo, sua utilização deve observar: Controle judicial prévio, sempre que houver possibilidade de impactar direitos de terceiros; contraditório e ampla defesa, garantindo que o investigado possa contestar a prova tecnológica; Respeito aos princípios constitucionais, evitando provas ilícitas (CF, art. 5º, LIV e LV).

Logo, o reconhecimento facial no processo penal pode ocorrer de diferentes maneiras, cada uma com implicações jurídicas específicas. A identificação em tempo real (*live recognition*) permite monitoramento imediato de indivíduos em espaços públicos ou privados, sendo útil para prevenção de delitos, mas apresenta alto risco de falsos positivos e vigilância em massa. Como alerta Laura Schertel Mendes (2020), o uso indiscriminado em locais

públicos compromete a liberdade de circulação e cria um ambiente de suspeição generalizada, vulnerando direitos fundamentais previstos no art. 5º, CF.

Já o reconhecimento a partir de registros fotográficos ou videográficos, utilizado posteriormente aos fatos para cruzamento com bases de dados oficiais, apresenta menor invasividade, mas ainda requer atenção quanto à autenticidade, integridade e guarda das imagens, sob pena de nulidade da prova, conforme estabelecido pelo STJ no HC 598.051/SP (2021).

Por fim, o uso em situações de flagrante delito pode apoiar a identificação rápida de suspeitos, mas exige observância do controle judicial prévio, do contraditório e da ampla defesa, garantindo que o reconhecimento facial funcione apenas como instrumento auxiliar à investigação, sem substituir a análise humana, em conformidade com os princípios constitucionais dos arts. 5º, LIV e LV, CF.

Em todas as modalidades, a tecnologia deve ser implementada de forma proporcional, transparente e auditável, respeitando tanto a eficiência investigativa quanto a proteção dos direitos fundamentais, reforçando que o reconhecimento facial não deve se transformar em instrumento de vigilância em massa.

6.2 RECONHECIMENTO FACIAL COMO MEIO DE PROVA - RISCOS E LIMITAÇÕES NO PROCESSO PENAL

A admissibilidade do reconhecimento facial como prova processual depende de critérios legais e constitucionais, como:

1. Legalidade: a coleta de dados deve obedecer à LGPD e a outras normas que regulamentem o uso de dados sensíveis (Doneda, 2006).

2. Proporcionalidade: a medida deve ser adequada, necessária e razoável, considerando o impacto sobre direitos fundamentais (Alexy, 2008).

3. Autenticidade e integridade: as imagens devem ser preservadas de forma que sua cadeia de custódia seja segura.

4. Controle judicial: a autorização prévia de magistrado é recomendável, especialmente em casos de coleta de dados de terceiros não investigados (STF, ADI 6.387/DF; ADI 6.638/DF).

Luis Roberto Barroso (2019), reforça que a prova obtida sem observância desses requisitos pode ser considerada ilegal, contaminando a validade processual e ferindo garantias constitucionais.

Erro e viés algorítmico: algoritmos apresentam maior índice de erro em mulheres e pessoas negras, refletindo padrões de desigualdade social (Buolamwini; Gebru, 2018; Nist, 2019).

Vigilância em massa: uso indiscriminado em espaços públicos ameaça liberdade de circulação e privacidade (Schertel Mendes, 2020).

Ausência de regulamentação específica: permite que órgãos investigativos adotem tecnologias de forma arbitrária, sem fiscalização eficiente (Vieira, 2018).

CONSIDERAÇÕES FINAIS

O reconhecimento facial, enquanto expressão do avanço tecnológico no campo da segurança pública e da vigilância social, traz consigo um paradoxo fundamental, ao mesmo tempo em que promete eficiência na prevenção e repressão criminal, coloca em xeque direitos e garantias constitucionais estruturantes da democracia brasileira.

O problema de pesquisa que orientou este estudo, quais são os limites constitucionais e jurídicos do uso de tecnologias de reconhecimento facial no Brasil, especialmente à luz do direito à privacidade e da proteção de dados pessoais, demonstrou que a atual ausência de um marco normativo específico gera riscos concretos de violação de direitos fundamentais, sobretudo diante da seletividade penal e da possibilidade de reforço de padrões de discriminação estrutural.

A análise dos dados e das experiências internacionais revelou que nenhum país democrático avançado adota o uso indiscriminado do reconhecimento facial. Pelo contrário, o AI Act da União Europeia, as restrições em diversas cidades norte-americanas e as recomendações do Conselho da Europa apontam para a necessidade de controles rígidos, auditorias algorítmicas, transparência e limites estritos de proporcionalidade.

No plano nacional, a jurisprudência do STF e do STJ já consolidou parâmetros de proteção que não podem ser ignorados, a privacidade como direito fundamental autônomo, a proteção de dados pessoais como corolário da dignidade humana e a exigência de autorização judicial para práticas de vigilância que afetem liberdades individuais. Esses precedentes, ainda que não tratem diretamente do reconhecimento facial, oferecem balizas constitucionais inequívocas para sua regulamentação.

À luz das teorias apresentadas, conclui-se que a utilização do reconhecimento facial no Brasil só pode ser admitida de forma excepcional, proporcional e controlada, jamais como instrumento de vigilância em massa.

Em conclusão, o desafio central que se coloca ao legislador, ao Judiciário e à sociedade brasileira é compatibilizar inovação tecnológica e proteção de direitos fundamentais. O reconhecimento facial só será legítimo se respeitar os limites constitucionais e jurídicos da privacidade, da proteção de dados pessoais e da igualdade, sob pena de converter-se em ferramenta de autoritarismo e exclusão social.

REFERÊNCIAS

BARROSO, Luís Roberto. **A dignidade da pessoa humana e os direitos fundamentais na era digital**. São Paulo: Saraiva, 2019.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Diário Oficial da União, Brasília, 5 out. 1988.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, Brasília, 15 ago. 2018.

BRASIL. Superior Tribunal de Justiça – STJ. **Habeas Corpus nº 598.051/SP**. Rel. Min. Ribeiro Dantas. Julgamento em 2021. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/HCs/HC-598051.aspx. Acesso em: 30 ago. 2025.

BUOLAMWINI, Joy; GEBRU, Timnit. **Gender Shades**: Intersectional Accuracy Disparities in Commercial Gender Classification. In: Proceedings of Machine Learning Research, v. 81, p. 1–15, 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 30 ago. 2025.

CAVALCANTI, Leonardo Nunes. **Reconhecimento facial: limites e possibilidades no uso da inteligência artificial em segurança pública**. São Paulo: Tirant Lo Blanch, 2021.

CITY AND COUNTY OF SAN FRANCISCO. **Acquisition of Surveillance Technology Ordinance**. San Francisco, 2019. Disponível em: https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies. Acesso em: 30 ago. 2025.

CONSELHO DA EUROPA. **Guidelines on Artificial Intelligence and Human Rights**. Strasbourg, 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Forense, 2006.

EUROPEAN COMMISSION. **Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence** (Artificial Intelligence Act). COM/2021/206 final, 2021.

EUROPEAN COURT OF HUMAN RIGHTS. S. & Marper v. **United Kingdom**, App. No. 30562/04 and 30566/04, 2008.

EUROPEAN UNION. **General Data Protection Regulation – GDPR**, Regulation (EU) 2016/679, 2016.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)**. Official Journal of the European Union, L 119, p. 1–88, 2016.

EUROPEAN UNION. **AI Act, Proposal for a Regulation on Artificial Intelligence**, 2024.

G1 BAHIA. **Mais de 130 pessoas foram presas após reconhecimento facial no Carnaval de Salvador**. G1, Salvador, 7 mar. 2019. Disponível em: https://g1.globo.com/ba/bahia/noticia/2019/03/07/mais-de-130-pessoas-foram-presas-apos-reconhecimento-facial-no-carnaval-de-salvador.ghtml. Acesso em: 30 ago. 2025.

HUMAN RIGHTS WATCH. **China**: Events of 2021 – Surveillance, Social Control, and Privacy Concerns. New York, 2021. Disponível em: https://www.hrw.org/world-report/2022/country-chapters/china-and-tibet. Acesso em: 30 ago. 2025.

INTERNETLAB – Centro de Pesquisa em Direito e Tecnologia. **Panorama do Reconhecimento Facial no Brasil**. São Paulo: InternetLab, 2021.

MALAGUTI BATISTA, Vera. **Direitos fundamentais e controle do poder estatal**. São Paulo: Editora Revista dos Tribunais, 2011.

MENDES, Laura Schertel. **Privacidade e proteção de dados no espaço público**: desafios do reconhecimento facial. Rio de Janeiro: FGV, 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. **Face Recognition Vendor Test (FRVT)** Part 3: Demographic Effects. Gaithersburg, 2019. Disponível em: https://www.nist.gov/programs-projects/face-recognition. Acesso em: 24 ago. 2025.

SARLET, Ingo Wolfgang. A efetividade dos direitos fundamentais. Porto Alegre: Livraria do Advogado, 2001.

SECURITY INDUSTRY. **Nation's Strongest Regulations for Law Enforcement Use of Facial Recognition Technology Go into Effect**: Key Provisions of Maryland's New Law. [S.l.], 07 out. 2024. Disponível em: https://www.securityindustry.org/2024/10/07/nations-strongest-regulations-for-law-enforcement-use-of-facial-recognition-technology-go-into-effect-key-provisions-of-marylands-new-law/. Acesso em: 30 ago. 2025.

SUPREMO TRIBUNAL FEDERAL. **ADI 6.387/DF**. Rel. Min. Rosa Weber. Julgamento em 2020.

SUPREMO TRIBUNAL FEDERAL. **ADI 6.638/DF**. Rel. Min. Gilmar Mendes. Julgamento em 2021.

UNITED NATIONS. **Office of the High Commissioner for Human Rights**. Guidelines on Privacy in the Digital Age, 2013.

UNITED STATES COMMISSION ON CIVIL RIGHTS – USCCR. Report: **Civil Rights Implications of Federal Use of Facial Recognition Technology.** Washington, 2024.

Disponível em: https://www.usccr.gov/news/2024/us-commission-civil-rights-releases-report-civil-rights-implications-federal-use-facial. Acesso em: 30 ago. 2025.

UNITED STATES SUPREME COURT. **Carpenter v. United States,** 585 U.S. ___, 2018. Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf. Acesso em: 30 ago. 2025.

VIEIRA, João. **Provas digitais e reconhecimento facial no processo penal**. Curitiba: Juruá, 2018.

VIEIRA, Oscar Vilhena. **Direito Constitucional e novas tecnologias**: desafios contemporâneos. São Paulo: Atlas, 2018.

WASHINGTON POST. **Police Artificial Intelligence and Facial Recognition**: Investigations and Errors. Washington, 2025. Disponível em: https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/. Acesso em: 30 ago. 2025.

WBUR. **Boston City Council Bans Facial Recognition Technology**. Boston, 23 jun. 2020. Disponível em: https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban. Acesso em: 30 ago. 2025.

WIRED. **China's Social Credit System Explained:** How the Country Is Monitoring Its Citizens. [S.l.], 2021. Disponível em: https://www.wired.com/story/china-social-credit-system-explained/. Acesso em: 30 ago. 2025.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, 2019.