

RECONHECIMENTO FACIAL ATRAVÉS DE INTELIGÊNCIA ARTIFICIAL: IMPLICAÇÕES NA PERSECUÇÃO PENAL



Thiago Augusto de Lima¹; Alder Thiago Bastos²

RESUMO: O presente artigo analisa as complexas implicações decorrentes da utilização de sistemas de reconhecimento facial baseados em inteligência artificial (IA) como ferramenta na persecução penal no Brasil. Diante da crescente adoção dessa tecnologia por órgãos de segurança pública, torna-se imperativo investigar sua compatibilidade com o ordenamento jurídico pátrio e os direitos fundamentais. O objetivo geral é analisar essas implicações, considerando aspectos técnicos, legais, éticos e jurisprudenciais. Especificamente, busca-se descrever o funcionamento da tecnologia, identificar o marco legal aplicável (incluindo o Art. 226 do CPP e a LGPD), examinar a jurisprudência recente dos tribunais superiores (STF e STJ) sobre reconhecimento de pessoas e provas tecnológicas, discutir os riscos inerentes (vieses algorítmicos, discriminação, erros judiciais, violação da privacidade e da presunção de inocência) e apontar desafios para sua regulamentação e uso responsável. A metodologia adotada consiste em revisão narrativa e análise documental de artigos científicos, legislação e decisões judiciais. Conclui-se que, embora a tecnologia ofereça potencial investigativo, seu uso atual na persecução penal brasileira enfrenta sérios questionamentos legais e éticos, dada a falta de regulamentação específica, os riscos de vieses discriminatórios e falhas, e a jurisprudência restritiva dos tribunais superiores quanto à validade do reconhecimento como prova isolada, demandando cautela extrema, controle rigoroso e um amplo debate sobre seus limites e necessidade.

PALAVRAS-CHAVE: Reconhecimento Facial. Inteligência Artificial. Processo Penal. Prova Penal. Direitos Fundamentais. Persecução Penal.

FACIAL RECOGNITION THROUGH ARTIFICIAL INTELLIGENCE: IMPLICATIONS FOR CRIMINAL PROSECUTION

ABSTRACT: This article analyzes the complex implications arising from the use of facial recognition systems based on artificial intelligence (AI) as a tool in criminal prosecution in

¹ Graduado em Direito pela Faculdade Bertogã. Advogado.

² Pós-doutorando em Direito pela Universidade Federal da Bahia. Pós-doutor em direitos humanos pela *Mediterranea International Centre for Human Rights Research* - Università "Mediterranea" di Reggio Calabria. Doutor em Direito Ambiental Internacional pela Universidade Católica de Santos – UNISANTOS. Tese selecionada para o programa de Bolsa CAPES (2023). Mestre em Direito pela Universidade Santa Cecília (UNISANTA) – Santos/SP (2018). Membro da *International Association of Artificial Intelligence* – I2AI. Membro da Associação Nacional das Advogadas e Advogados de Direito Digital – ANADD. Pesquisador junto ao Grupo de Pesquisa - Direito Ambiental, Estado e Sociedade da Universidade Católica de Santos (UNISANTOS). Compõe os Núcleos de Desenvolvimento Estruturantes da FABE e Faculdades Integradas Campos Salles. Advogado. ORCID: <https://orcid.org/0000-0001-6878-3986> (Orientador).

Brazil. Given the increasing adoption of this technology by public security agencies, it is imperative to investigate its compatibility with the national legal system and fundamental rights. The general objective is to analyze these implications, considering technical, legal, ethical, and jurisprudential aspects. Specifically, it seeks to describe the functioning of the technology, identify the applicable legal framework (including Article 226 of the Brazilian Code of Criminal Procedure and the LGPD), examine recent investigations by the higher courts (STF and STJ) on the recognition of persons and technological evidence, discuss the inherent risks (algorithmic biases, discrimination, judicial errors, violation of privacy and the presumption of innocence), and specific challenges for its regulation and responsible use. The methodology adopted consists of a narrative review and documentary analysis of scientific articles, legislation, and judicial decisions. It is concluded that, although the technology presents investigative potential, its current use in Brazilian criminal prosecution faces serious legal and ethical questions, given the lack of specific regulations, the risks of discriminatory evidence and errors, and the restrictive regulation of the courts regarding the validity of recognition as isolated evidence, requiring extreme caution, superior control, and a broad debate about its limits and necessity.

KEYWORDS: Facial Recognition. Artificial Intelligence. Criminal Procedure. Criminal Evidence. Fundamental Rights. Criminal Prosecution.

1. Introdução

A contemporaneidade é marcada por avanços tecnológicos exponenciais, dentre os quais a Inteligência Artificial (IA) assume um protagonismo próprio e peculiar na Era Digital, permeando diversas esferas da vida pessoal e interpessoal de indivíduos alinhando a perspectiva de otimização de trabalho e agilidade em processos de criação, de identificação e de correção.

Nessa perspectiva, considerando a amplitude de atuação e alcance das discussões sobre a inteligência artificial, torna-se necessário o recorte epistemológico para dialogar, nesse trabalho acadêmico, as controversas reside nos sistemas de reconhecimento facial. Isso porque, por intermédio da IA se tornou possível identificar ou verificar a identidade de um indivíduo a partir de características únicas de seu rosto, comparando-as com vastas bases de dados previamente cadastrada e disponibilizada a fim de reconhecê-lo³.

³ É de salientar que os recursos são igualmente presentes em outros meios de identificação, como fechaduras eletrônicas, computadores, celulares, mas, por intermédio da IA o alcance torna-se mais eficaz em processamento e busca em bases de dados.

A referida ferramenta vem sendo progressivamente incorporada por governos em escala global como estratégia de política e segurança pública na busca da persecução penal. A adoção de sistemas de reconhecimento facial que utilizam a IA pelos órgãos policiais e judiciários tem revelado uma ampla instalação de câmeras de vigilância equipadas com IA em espaços públicos, eventos e sistemas de transporte, alimentando bancos de dados e realizando comparações (em tempo real ou posterior) para identificação de indivíduos com passagens criminais ou com mandados de prisão decretados para cumprimento da persecução penal.

O Brasil, seguindo essa tendência, tem incorporado referidos sistemas de reconhecimento facial, com prévia alimentação de dados. Contudo, exsurge a desconfiança na confiabilidade, precisão e neutralidade algorítmica das informações de identificação do indivíduo frente a aparente colisão entre direitos fundamentais à privacidade, à imagem e à proteção de dados (art. 5º, Incisos X e LXXIX, CF).

Diante disto, emerge o problema central que norteia este trabalho: Quais as principais implicações jurídicas, éticas e processuais do uso do reconhecimento facial por IA na persecução penal brasileira? A busca por respostas a essa indagação é crucial, pois a incorporação acrítica de novas tecnologias no âmbito penal, sem a devida análise de sua compatibilidade com os princípios constitucionais e as garantias processuais, pode resultar em graves violações de direitos e na fragilização do Estado Democrático de Direito.

Nesse sentido, o objetivo geral deste artigo é analisar as implicações do uso da tecnologia de reconhecimento facial baseada em IA como ferramenta na busca da concretização da persecução penal no Brasil, à luz do ordenamento jurídico interno. Para alcançar tal propósito, delinear-se-ão os seguintes objetivos específicos: descrever o funcionamento básico da tecnologia de reconhecimento facial por IA, identificando suas potencialidades e limitações; identificar o marco legal e processual penal aplicável ao reconhecimento de pessoas e à produção de provas tecnológicas no Brasil, com especial atenção ao artigo 226 do Código de Processo Penal (CPP) e à Lei Geral de Proteção de Dados Pessoais (LGPD); analisar a jurisprudência recente dos tribunais superiores (Supremo Tribunal Federal - STF e Superior Tribunal de Justiça - STJ) sobre o tema; discutir as principais implicações éticas e os riscos aos direitos fundamentais, como privacidade, presunção de inocência, devido processo legal e igualdade/não discriminação; e, por fim,

apontar desafios e perspectivas para a regulamentação e utilização responsável da tecnologia no contexto brasileiro.

4

A relevância desta pesquisa situa-se na existência ou não de aparato jurídico normativo válido à incorporação do reconhecimento facial via IA em câmeras de monitoramento das cidades brasileiras, em especial em qual medida que referidos aparatos tecnológicos possam atingir direitos fundamentais subscritos na Constituição Federal brasileira.

A metodologia é descrita em capítulo próprio, tendo ao final do presente trabalho criticada a utilização indiscriminada da referida tecnologia com possíveis violações de direitos fundamentais, em especial pela liberdade individual, especialmente daquelas pessoas que não são previamente cadastradas em bases de dados e erros algorítmicos que foram apontados na utilização dos dados para busca de indivíduos em persecução penal.

2. Metodologia

A presente pesquisa caracteriza-se como um estudo de natureza qualitativa, desenvolvido por meio de revisão narrativa que foca a base teórica, através de revisões bibliográfica e análise do arcabouço documental jurídico e jurisprudencial em prol das discussões que dialoguem com o objetivo central sobre a análise de implicações no uso da tecnologia de reconhecimento facial baseada em IA como mecanismo de persecução penal no Brasil, à luz do ordenamento jurídico interno e direitos fundamentais consagrados.

A revisão bibliográfica compreendeu a busca e seleção de artigos científicos publicados em periódicos nacionais e internacionais indexados, livros, capítulos de livros, teses e dissertações que versam sobre os temas centrais da pesquisa: inteligência artificial, reconhecimento facial, processo penal, prova penal, direitos fundamentais, vieses algorítmicos e ética na tecnologia. Foram priorizadas publicações recentes e de autores com reconhecida expertise nas áreas do Direito, Ciência da Computação e Ciências Sociais, buscando uma abordagem interdisciplinar.

A análise documental envolveu o exame da legislação brasileira pertinente, com destaque para a Constituição Federal de 1988, o Código de Processo Penal (especialmente o Art. 226), a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e outras normas

relacionadas à prova digital e aos direitos fundamentais. Adicionalmente, procedeu-se à análise de decisões judiciais relevantes, emanadas principalmente do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ), que tratam do reconhecimento de pessoas e da validade de provas tecnológicas no processo penal. Foram consultadas as bases de dados de jurisprudência dos respectivos tribunais e notícias sobre julgamentos recentes.

O método de abordagem utilizado foi o hipotético-dedutivo, partindo-se da problemática das implicações do reconhecimento facial na persecução penal e buscando, através da análise das fontes selecionadas, verificar as hipóteses levantadas quanto aos riscos legais, éticos e processuais. A análise do material coletado foi realizada de forma crítica e interpretativa, buscando identificar os principais argumentos, pontos de convergência e divergência na doutrina e na jurisprudência, bem como as lacunas e desafios existentes no tratamento do tema pelo ordenamento jurídico brasileiro.

A redação do artigo buscou seguir as normas da Associação Brasileira de Normas Técnicas (ABNT), especialmente as NBR 6022 (Artigo em publicação periódica científica impressa – Apresentação), NBR 14724 (Trabalhos acadêmicos – Apresentação), NBR 10520 (Citações em documentos – Apresentação) e NBR 6023 (Informação e documentação – Referências – Elaboração), conforme detalhado no levantamento inicial de requisitos.

3. Inteligência Artificial e Tecnologia de Reconhecimento Facial

A IA pode ser compreendida, de forma ampla, como um campo da ciência da computação dedicado à criação de sistemas capazes de realizar tarefas que normalmente exigiriam inteligência humana, como aprendizado, raciocínio, percepção, resolução de problemas e tomada de decisão. Longe de ser uma entidade monolítica, a IA abrange diversas abordagens e subcampos, incluindo o aprendizado de máquina (*machine learning*), onde os algoritmos aprendem padrões a partir de grandes volumes de dados, e o aprendizado profundo (*deep learning*), um subconjunto do *machine learning* que utiliza redes neurais artificiais com múltiplas camadas para analisar dados complexos, como imagens (Ferreira, Avanci; 2022).

Nesse contexto, tal como aconteceu no avanço da tecnologia *internet*, a inteligência artificial sofreu suas diversas fases, descrevendo Lee quatro importantes fases, sendo elas: a) a

interligação as tecnologias de *internet* e de IA, b) as IA's voltadas ao mercado de trabalho, c) a interação da IA com imagens e som e a última por sistemas autônomos (Bastos, 2023, Lee, 2018).

6

A análise do presente trabalho é focada no que denominou o autor supramencionado como sendo "*Perception AI*", já que permite a utilização de seus aspectos físicos para corroborar com a análise algorítmica e atingir o resultado previamente programado pela referida IA (Lee, 2018, p. 117).

A *deep learning* compreendendo referida interação, permite simular um cérebro humano, com interligações neurais, adotando mecanismo de aprendizagem, de memorização e de implementação de ações, fazendo ou auxiliando trabalhos que, antes, eram identificados apenas pela atuação humana (Rosana et al, 2024). Em sua essência, um sistema de reconhecimento facial opera em etapas: primeiramente, detecta a presença de um rosto em uma imagem ou vídeo; em seguida, extrai características faciais únicas (pontos nodais, distâncias entre olhos, nariz, boca, formato do maxilar), convertendo-as em uma representação matemática (uma "assinatura facial" ou *template* biométrico); por fim, compara essa assinatura com um banco de dados de faces conhecidas (modo de identificação 1:N) ou com a assinatura de um rosto específico (modo de verificação 1:1). O sucesso dessas etapas depende crucialmente da qualidade dos algoritmos, da vastidão e representatividade dos dados utilizados no treinamento e da qualidade das imagens capturadas.

Nesse exato ponto que reside a preocupação, pois as aplicações dessa tecnologia na segurança pública têm se vislumbrado em diversas fases da persecução penal, desde a própria interação na investigação, como, com ênfase nesse estudo, a ideia de reconhecimento em modernos sistemas de vigilância urbana utilizam câmeras com IA para monitorar espaços públicos, mas não só, também com a função de identificar indivíduos em lista de procurados ou suspeitos em tempo real.

É justamente nesse ponto que se reside a preocupação, pois, como anota Garcia:

É justamente para este ponto que queremos chamar a atenção. A inteligência da máquina depende da qualidade dos dados e dos exemplos a que ela é submetida, e vai reproduzir o conhecimento que está impregnado nesses dados. Não é o suficiente se garantir que os dados estejam corretos. Esta seria a premissa básica, mas não é suficiente. Se a máquina receber dados e informações carregados de vieses e preconceitos de raça, de gênero, de escolha sexual, de forma física ou de qualquer

outro traço, ela irá não só aprender com eles como perpetuá-los, durante o seu processo de aprendizado, quando exposta a novos dados. Nos exemplos a seguir, procuraremos apontar algum dos riscos de se aplicar indiscriminadamente a Inteligência Artificial sem discutir os dilemas éticos entremeados na enorme massa de dados que circulam pelos sistemas inteligentes do mundo todo (Garcia, 2020, p.15).

7

Nesse contexto, Santos afirmar que a aprendizagem das máquinas implica na “capacidade de a partir da própria experiência, gerando soluções e decisões originais” e a problemática reside, segundo a autora no exato momento em que “considerando os algoritmos capazes de aprender, uma vez que eles são deixados soltos em um manancial de dados, eles podem trazer inferências muitas vezes não esperadas pelo programador” (Santos, 2025, p. 6).

Evidentemente que tal situação pode conflitar com direitos fundamentais ou outros que, mesmo não fundamentais, são igualmente protegidos por lei. Isso porque, na seara criminal, o processamento desses dados, criando-se percepções algorítmicas em prol da identificação de autores de delitos ou localização de testemunhas previamente cadastradas em bancos de dados podem gerar erros já que, conforme anotam os estudos consultados, vez que a *deep learning* permite a criação de novos dados a partir da consulta daqueles existentes, na ideia de aprendizagem da máquina dentro da programação previamente estabelecida.

Portanto, se a confiabilidade não é absoluta, permitindo-se margem de erros, a precisão pode variar significativamente a depender das variáveis previamente programadas na IA, além de fatores condizentes com posicionamento de câmeras, resoluções e ângulos de imagens, oclusões parciais do rosto (máscara, óculos etc.) e as próprias características humanas que variam com o passar do tempo e intervenções cirúrgicas que possam ocorrer (plásticas), o que traduz na perda da confiabilidade e precisão do resultado anotado pela IA.

Além disso, também é identificado por esta revisão narrativa que própria definição de “precisão” é complexa, envolvendo métricas como taxa de falsos positivos (identificar incorretamente uma pessoa) e taxa de falsos negativos (não conseguir identificar uma pessoa presente no banco de dados), o que gera conflito de confiabilidade na aplicação da IA.

Desse modo, estudos têm demonstrado consistentemente que muitos algoritmos de reconhecimento facial apresentam taxas de erro significativamente maiores para determinados grupos, como pessoas negras, mulheres e indivíduos mais jovens, um fenômeno conhecido como viés algorítmico, causando discriminações que podem levar a identificações equivocadas

e sua grave consequência a direito penal material e processual (Costa, Kremer, 2022; Silva, Silva, 2019; Machado, Barros, 2023; Koch; Lopes, 2023).

Extraí-se nesse ponto que as perspectivas de persecução penal com base na inteligência artificial se mostram conflitante através das próprias inexistências de confiabilidade e precisão, através dos dados que podem ser criados a partir da interpretação trazida pelo algoritmo que resultará em imprecisão de dados formados a partir da IA.

4. O Direito Penal Interno

O direito penal interno é formado pela ideia piramidal que anota a existência de uma observância das normas constitucionais e infraconstitucionais, com as devidas garantias a direitos fundamentais consagrados, em grande parte, entre os artigos 5º e 7º da Constituição Federal de 1988, permitindo uma hierarquização de normas jurídicas para aplicação, em especial no direito penal, da restrição de liberdade (Kelsen, 1998; 2006).

Deste modo, analisar a utilização do reconhecimento facial por IA na persecução penal brasileira perpassa, inevitavelmente, pelo exame do arcabouço legal e processual existente, que, embora não trate especificamente dessa tecnologia, fornece parâmetros essenciais para sua avaliação. Destacam-se, nesse contexto, as regras sobre o reconhecimento de pessoas no Código de Processo Penal (CPP) e a legislação mais recente sobre proteção de dados.

O principal dispositivo processual, amparado pelo Código Penal brasileiro, é artigo 226 do CPP ao estabelecer um procedimento formalístico detalhado que deve ser observado quando houver necessidade de se proceder ao reconhecimento de pessoa, assegurando que a pessoa a ser reconhecida seja descrita previamente pela vítima ou testemunha, bem como seja colocada, sempre que possível, ao lado de outras que com ela tiverem semelhança; e que a vítima ou testemunha seja convidada a apontá-la, como mecanismo de precisão da identificação do infrator penal.

Após o reconhecimento supramencionado, o parágrafo único ainda prevê a lavratura de auto pormenorizado, subscrito pela autoridade, pela pessoa chamada para proceder ao reconhecimento e por duas testemunhas presenciais. Embora a jurisprudência por muito tempo

tenha relativizado a obrigatoriedade dessas formalidades, considerando-as meras recomendações, há uma mudança paradigmática de interpretações dadas pelo Supremo Tribunal Federal e pelo Superior Tribunal de Justiça.

Isso porque, a jurisprudência do STJ já aponta para a impossibilidade de utilizar o reconhecimento (mesmo o tradicional) como prova única para condenação. Esse entendimento pode ser estendido e igualmente aplicado no que tange ao reconhecimento facial por IA, especialmente quando não se tem precisão sobre os dados coletados e possíveis erros que possam levar, sobremaneira à discriminação (Costa, Kremer, 2022).

Se de um lado a IA permite a perspectiva de resultados sólidos e agilidades, ela não pode se divorciar das garantias constitucionais e preceitos fundamentais, em especial quando há uma imprecisão de reconhecimentos faciais por intermédio da IA ou a sua confiabilidade não resulta em mecanismos precisos de tratamento de dados a exemplo do que descreve o tratamento de dados encabeçado pela Lei Geral de Proteção de Dados – LGPD (Sousa, 2021).

Muito embora não haja uma vedação legal da utilização de provas por intermédio do princípio da liberdade dos meios de prova (Art. 155 do CPP), deve ser respeitadas as garantias constitucionais e legais, como o devido processo legal, o contraditório e a ampla defesa. A validade de uma prova digital, incluindo aquela gerada por sistemas de IA, depende da demonstração de sua autenticidade, integridade e cadeia de custódia, conforme preveem os artigos 158-A e seguintes do CPP (introduzidos pela Lei nº 13.964/2019 - Pacote Anticrime). No caso do reconhecimento facial, isso implicaria a necessidade de demonstrar a confiabilidade do algoritmo, a qualidade do banco de dados utilizado, a metodologia de comparação e a ausência de manipulações, o que nem sempre é factível dada a opacidade de muitos sistemas comerciais.

Referido arcabouço legislativo infraconstitucional ainda deve ser convalidado às próprias garantias de direito fundamentais subscritas no Arquetipo Constitucional de 1988, evidenciando-se, no momento, que a Lei Geral de Proteção de Dados não traz qualquer questão sobre o tratamento de dados ou armazenamento para fins de persecução penal, devendo tais perspectivas algorítmicas observar, ao menos, os preceitos estabelecidos para o tratamento de dados e sua utilização.

Agrava-se a situação quando os dados estabelecidos podem ser gerados através de algoritmos criados através da *deep learning*, trazendo constrangimentos e ações policiais indesejadas, tornando o mecanismo impróprio para tomada de decisões automatizadas que afetem direitos fundamentais sem supervisão humana qualificada⁴.

Deste modo, se identifica que a tecnologia opera de forma distinta do reconhecimento humano tradicional previsto no CPP, baseando-se em comparações algorítmicas de características faciais inseridas previamente em bancos de dados, podendo, nesse contexto, revelar erros essenciais e levantar dúvidas cruciais sobre a validade probatória do reconhecimento facial, seja para a investigação criminal, seja para a identificação de suspeitos, não sendo amplamente acobertado pelo disposto no art. 226 do CPP (CENCI, 2023) e essa ausência de previsão legal específica para essa nova modalidade de reconhecimento gera um vácuo normativo procedimental que pode contribuir para a insegurança jurídica no contexto acusatório ou de identificação precisa do indivíduo.

Diante das incertezas legais e éticas, a utilização responsável da tecnologia de reconhecimento facial por IA na persecução penal brasileira enfrenta desafios significativos, mas também abre perspectivas para a construção de salvaguardas e boas práticas. A simples proibição total da tecnologia pode não ser a solução mais adequada, dada a sua potencial utilidade em contextos específicos e controlados, mas sua implementação acrítica e desregulada pode causar inseguranças jurídicas e discriminações incorretas (Costa, Kremer, 2022).

O principal desafio reside na ausência de uma regulamentação específica e abrangente, posto que a legislação vigente não tem marco normativo claro para o uso de reconhecimento facial pelo Estado para fins penais. A implementação da IA de forma indiscriminada e sem prévia definição legal, especialmente a garantir os preceitos fundamentais de direito, impõe insegurança jurídica quanto aos desfechos do reconhecimento da IA por intermédio de *deep learning* e criação de um perfil discriminatório que pode reverberar em identificações incoerentes ou pré-direcionada a classes sociais menos favorecidas.

⁴ A própria operabilidade da IA pelos operadores do direito deve passar pela capacitação dos agentes envolvidos, com a garantia dos dados processados e identificação crítica sobre o resultado gerado por IA permitindo-se, com isso, a aplicação do princípio consagrado de ampla defesa e contraditório.

5. Conclusão

A crescente integração da inteligência artificial, e especificamente da tecnologia de reconhecimento facial, no aparato de segurança pública e na persecução penal brasileira representa um fenômeno complexo, repleto de promessas de eficiência, mas também carregado de riscos significativos e profundas implicações jurídicas, éticas e sociais. Este artigo analisou essas implicações, partindo da descrição da tecnologia e do marco legal aplicável, passando pela análise da jurisprudência recente e culminando na discussão dos riscos aos direitos fundamentais e dos desafios para uma utilização responsável.

Ao longo do desenvolvimento, constatou-se que, embora o reconhecimento facial por IA ofereça ferramentas potencialmente úteis para a investigação criminal, sua implementação no contexto brasileiro ocorre em um cenário de vácuo normativo específico e de crescentes questionamentos por parte dos tribunais superiores quanto à validade do reconhecimento de pessoas como prova penal. A análise do funcionamento da tecnologia revelou suas limitações intrínsecas, como a possibilidade de erros e, mais gravemente, a presença de vieses algorítmicos que podem perpetuar e amplificar discriminações, afetando desproporcionalmente grupos já marginalizados. A falta de transparência e auditabilidade de muitos sistemas agrava a dificuldade de aferir sua real confiabilidade.

O marco legal brasileiro, centrado no artigo 226 do CPP para o reconhecimento de pessoas e ainda carente de legislação específica sobre o tratamento de dados para fins penais (conforme exigido pela LGPD), mostra-se inadequado para lidar com as especificidades do reconhecimento facial automatizado. A recente e consolidada jurisprudência do STJ, ao exigir o cumprimento rigoroso das formalidades do Art. 226 como condição de validade do reconhecimento e ao relegar o reconhecimento fotográfico (e, por extensão lógica, o tecnológico) a um papel meramente inicial e confirmatório, impõe barreiras legais robustas à sua utilização como prova autônoma e decisiva para a condenação.

As implicações éticas e os riscos aos direitos fundamentais são igualmente alarmantes. A potencial violação da privacidade pela coleta massiva de dados biométricos, a ameaça à presunção de inocência por identificações falhas, o impacto discriminatório dos vieses algorítmicos e a dificuldade de exercer o contraditório e a ampla defesa diante de sistemas

opacos configuram um quadro preocupante. A vigilância biométrica generalizada pode, ainda, comprometer liberdades civis essenciais e alterar a própria natureza da relação entre Estado e cidadão.

Respondendo ao problema de pesquisa e aos objetivos propostos, conclui-se que as implicações do uso do reconhecimento facial por IA na persecução penal brasileira são majoritariamente negativas no cenário atual, dada a ausência de regulamentação adequada, os riscos técnicos e éticos comprovados, e a incompatibilidade com as garantias processuais e a jurisprudência garantista dos tribunais superiores. Sua utilização demanda extrema cautela, devendo ser restrita a hipóteses muito específicas, com controle rigoroso, transparência e sempre como um meio subsidiário, jamais como prova única ou principal.

Este estudo, contudo, possui limitações, como a rápida evolução tecnológica e jurisprudencial, que podem tornar algumas análises datadas em curto espaço de tempo. Sugere-se, para trabalhos futuros, o aprofundamento em estudos de caso específicos de implementação da tecnologia no Brasil, a análise comparada com regulamentações internacionais mais avançadas e a investigação de alternativas tecnológicas ou procedimentais menos invasivas. É fundamental que o debate sobre o reconhecimento facial na persecução penal continue, de forma aberta, crítica e multidisciplinar, buscando caminhos que conciliem os legítimos anseios por segurança com a intransigente defesa dos direitos e garantias fundamentais no Estado Democrático de Direito.

Referências

BASTOS, Alder Thiago. **O Reconhecimento da Dimensão Autônoma do Meio Ambiente Digital em um Contexto Global**. New York: Lawinter Editions, 2023.

BRASIL. Associação Brasileira de Normas Técnicas (ABNT). **NBR 6022: Informação e documentação – Artigo em publicação periódica científica impressa – Apresentação**. Rio de Janeiro, 2018. Disponível em: https://www.cetam.am.gov.br/wp-content/uploads/2022/02/01_ABNT_NBR_6022-2018_Artigo-em-publicacao-periodica-tecnica-eou-cientifica-1.pdf. Acesso em: 25 maio 2025.

_____. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2025]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 maio 2025.

_____. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Brasília, DF: Presidência da República, [2025]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 25 maio 2025.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2025]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 maio 2025.

_____. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, [2025]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 25 maio 2025.

_____. Superior Tribunal de Justiça (STJ). **Habeas Corpus nº 598.886/SC**. Relator: Ministro Rogerio Schietti Cruz. Sexta Turma. Julgado em 27 out. 2020. DJe 18 nov. 2020. Disponível em: <https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/27102020%20HC598886-SC.pdf>. Acesso em: 25 maio 2025.

_____. Superior Tribunal de Justiça (STJ). **Habeas Corpus nº 652.284/SC**. Relator: Ministro Reynaldo Soares da Fonseca. Quinta Turma. Julgado em 23 fev. 2021. DJe 01 mar. 2021. Disponível em: <https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=125129142&tipo=5&nreg=202100769343&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20210503&formato=PDF&salvar=false>. Acesso em: 25 maio 2025.

_____. Superior Tribunal de Justiça (STJ). Pesquisa no STJ mostra ainda resistências à jurisprudência sobre reconhecimento de pessoas. **Notícias STJ**, 17 maio 2024. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/17052024-Pesquisa-no-STJ-mostra-ainda-resistencias-a-jurisprudencia-sobre-reconhecimento-de-pessoas.aspx>. Acesso em: 25 maio 2025.

_____. Superior Tribunal de Justiça (STJ). Reconhecimento de pessoas: um campo fértil para o erro judicial. **Notícias STJ**, 06 fev. 2022. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/06022022-Reconhecimento-de-pessoas-um-campo-fertil-para-o-erro-judicial.aspx>. Acesso em: 25 maio 2025.

_____. Supremo Tribunal Federal (STF). **Agravo em Recurso Extraordinário nº 1.437.641/SP** (Tema 1.297). Relator: Ministro Gilmar Mendes. Repercussão Geral reconhecida em 17 mar. 2025. Disponível em: <https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=68>

[52548&numeroProcesso=1479602&classeProcesso=RE&numeroTema=1297](#). Acesso em: 25 maio 2025.

14

_____. Supremo Tribunal Federal (STF). STF vai decidir sobre validade de reconhecimento pessoal em processo penal. **Notícias STF**, 17 mar. 2025. Disponível em: <https://noticias.stf.jus.br/postsnoticias/stf-vai-decidir-sobre-validade-de-reconhecimento-pessoal-em-processo-penal/>. Acesso em: 25 maio 2025.

CENCI, Gabrielle. Reconhecimento facial pela IA e sua (in)compatibilidade com o CPP brasileiro. **Consultor Jurídico (ConJur)**, 20 jun. 2023. Disponível em: <https://www.conjur.com.br/2023-jun-20/gabrielle-cenci-reconhecimento-facial-ia-cpp-brasileiro/>. Acesso em: 25 maio 2025.

CONJUR. STF e STJ divergem em reconhecimento e geram insegurança jurídica. **Consultor Jurídico (ConJur)**, 31 jul. 2023. Disponível em: <https://www.conjur.com.br/2023-jul-31/stf-stj-divergem-reconhecimento-geram-inseguranca-juridica/>. Acesso em: 25 maio 2025.

COSTA, Rafael Ferreira de Albuquerque. Reconhecimento facial: solução ou potencialização de antigas mazelas?. **Boletim IBCCRIM**, São Paulo, v. 30, n. 361, p. 16–17, 2024. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1549. Acesso em: 22 abr. 2026.

COSTA, Ramon Silva; KREMER, Bianca. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 16, n. 1, 2022. DOI: 10.30899/dfj.v16i1.1316. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1316>. Acesso em: 22 abr. 2026.

FERREIRA, Gabrielle de O. AVANCI, Thiago Felipe. S. 10. Considerações sobre Direitos Fundamentais, Inteligência Artificial e Responsabilidade Civil. IN: Relatório sobre Inteligência Artificial e o Projeto de Lei 21/20, que visa Instituir o Marco Legal da Inteligência Artificial no Brasil. Centro de Estudos Sociedade e Tecnologia. **Global AI Ethics Institute. International Group of Artificial Intelligence. ETHICAI**. Mai/2022. DOI: 10.13140/RG.2.2.29960.14087. P. 61-72. Disponível em: https://ethikai.org/wp-content/uploads/2024/02/DOC-01-COMPLETO1BRAZIL_AI_BILL_REPORT.pdf. Acesso em: 14 abr. 2024.

GARCIA, Ana Cristina Bicharra. Ética e inteligência artificial. **Computação Brasil**, n. 43, p. 14-22, 2020. Disponível em: <https://sol.sbc.org.br/journals/index.php/comp-br/article/view/1791>. Acesso em: 14 abr. 2026.

KELSEN, Hans. **Teoria geral do direito e do estado** (Título original: *General theory of law and state*). Tradução Luís Carlos Borges. 3ª ed. - São Paulo: Martins Fontes, 1998.

_____. **Teoria pura do direito**. Tradução João Baptista Machado. - 7 ed. - São Paulo: Martins Fontes, 2006.

KOCH, Willian; LOPES, Rafael Vieira de Mello. Do reconhecimento facial a partir da inteligência artificial: a possibilidade de sua utilização como prova no processo penal brasileiro. **Revista de Direito Luso-Brasileira (RJLB)**, Lisboa, ano 9, n. 6, p. 1621-1648, 2023. Disponível em: https://www.cidp.pt/revistas/rjlb/2023/6/2023_06_1621_1648.pdf, Acesso em: 25 maio 2025.

LEE, Kai-Fu. **AI Super powers: China, Silicon Valley, and the new world order**. Nova York: Houghton Mifflin Harcourt, 2018.

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 EJEF**, Belo Horizonte, v. 3, n. 1, p. 105-124, 2023. Disponível em: <https://revistaejef.tjmg.jus.br/index.php/revista-ejef/article/view/47>. Acesso em: 24 set. 2025.

SANTOS, Keyla Cristina Farias dos. INTELIGÊNCIA ARTIFICIAL: AVANÇOS E RETROCESSOS DAS NOVAS TECNOLOGIAS NO ÂMBITO INTERNACIONAL PARA O EFETIVO ACESSO À JUSTIÇA NA ATUALIDADE. **Revista Brasileira de Desenvolvimento e Inovação**, [S. l.], v. 2, n. 3, 2025. Disponível em: <https://rbdin.com.br/index.php/revista/article/view/48>. Acesso em: 22 abr. 2026.

SANTOS, Rosana Silva dos; OLIVEIRA, Rosana Gislene Batista de; SANTOS, Marcelo Fonseca; BASTOS, Alder Thiago. LEGALTECH E A SUA UTILIZAÇÃO PELA INTELIGÊNCIA ARTIFICIAL. **Revista Brasileira de Desenvolvimento e Inovação**, [S. l.], v. 1, n. 1, 2024. Disponível em: <https://rbdin.com.br/index.php/revista/article/view/12>. Acesso em: 22 abr. 2026.

SILVA, Rosane Leal da; SILVA, Fernanda dos Santos Rodrigues da. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. In: **Congresso Internacional de Direito e Contemporaneidade, Santa Maria, RS, Brasil**. 2019. Disponível em: <https://www.ufsm.br/app/uploads/sites/563/2019/09/5.23.pdf>. Acesso em: 25 maio 2025.

SOUSA, Mariana Almirão de; DANTAS, T. K. S.; CLOZEL, Livia; LACERDA, Maria Eugênia. **Desafios da implementação de um programa de conformidade à LGPD no comércio**. In: Eduardo Tomasevicius Filho. (Org.). **A lei geral de proteção de dados brasileira: análise setorial**. 1ed. São Paulo: Almedina, 2021, v. 1, p. 171-202.