



Inteligência Artificial e Investigação Criminal: Desafios Constitucionais no Uso de Reconhecimento Facial e Análise Preditiva pelos Órgãos de Segurança Pública

Artificial Intelligence and Criminal Investigation: Constitutional Challenges in the Use of Facial Recognition and Predictive Analytics by Public Security Agencies

Felipe Santiago Soares Alves

Resumo: O presente estudo analisa os desafios constitucionais e processuais decorrentes do uso da inteligência artificial (IA) em investigações criminais, com foco nas tecnologias de reconhecimento facial e análise preditiva. Partindo da crescente incorporação desses sistemas pela segurança pública, examina-se sua compatibilidade com os princípios da Constituição Federal de 1988, notadamente a privacidade, a igualdade, a presunção de inocência e o devido processo legal. A pesquisa, de abordagem qualitativa e natureza exploratória, baseia-se em revisão doutrinária e em experiências internacionais, como o AI Act da União Europeia e o modelo regulatório chinês. Constatou-se que, embora a IA possa aprimorar a eficiência investigativa, sua aplicação sem adequada regulação e transparência algorítmica implica sérios riscos de discriminação, violação de dados e produção de provas ilícitas. Conclui-se que o uso constitucionalmente válido da IA na persecução penal depende da observância de critérios como legalidade, proporcionalidade, proteção de dados e preservação da cadeia de custódia digital, de modo a equilibrar inovação tecnológica e respeito aos direitos fundamentais.

Palavras-chave: inteligência artificial; reconhecimento facial; análise preditiva; direitos fundamentais; processo penal.

Abstract: This study examines the constitutional and procedural challenges arising from the use of artificial intelligence (AI) in criminal investigations, focusing on facial recognition and predictive policing technologies. Based on the increasing adoption of such systems by law enforcement agencies, it analyzes their compatibility with the principles enshrined in the 1988 Brazilian Federal Constitution, particularly privacy, equality, the presumption of innocence, and due process of law. The research follows a qualitative and exploratory approach, supported by legal doctrine and comparative analysis of international experiences, such as the European Union's AI Act and China's regulatory model. Findings indicate that although AI may enhance investigative efficiency, its application without clear regulation and algorithmic transparency entails serious risks of discrimination, data breaches, and unlawful evidence production. It concludes that the constitutionally valid use of AI in criminal proceedings requires adherence to principles of legality, proportionality, data protection, and preservation of digital chain of custody, ensuring a balance between technological innovation and the safeguarding of fundamental rights.

Keywords: artificial intelligence; facial recognition; predictive policing; fundamental rights; criminal procedure.

INTRODUÇÃO

O avanço da inteligência artificial (IA) tem impactado de forma significativa o direito, especialmente no âmbito do processo penal, em que novas tecnologias vêm sendo incorporadas às atividades de investigação e persecução criminal. A utilização de sistemas como o reconhecimento facial e o policiamento preditivo revela-se promissora em termos de eficiência, mas ao mesmo tempo suscita preocupações quanto à preservação de direitos e garantias fundamentais, como a privacidade, a igualdade e a presunção de inocência. Nesse contexto, torna-se indispensável analisar em que medida tais inovações podem ser compatibilizadas com a ordem constitucional brasileira e com os princípios estruturantes do processo penal democrático.

A importância do presente estudo reside justamente na atualidade e na relevância prática da temática, considerando que a expansão do uso da IA em investigações policiais no Brasil ocorre em meio a uma ausência de regulamentação clara e a decisões judiciais ainda incipientes sobre a admissibilidade das provas obtidas por esses meios. O objetivo geral consiste em examinar os desafios constitucionais e processuais decorrentes do emprego da inteligência artificial em investigações criminais, enquanto os objetivos específicos se concentram em: (i) descrever as principais aplicações da IA no campo da segurança pública; (ii) identificar os direitos fundamentais potencialmente afetados; e (iii) discutir critérios de admissibilidade das provas digitais à luz da doutrina, jurisprudência e experiências internacionais.

No que se refere à metodologia, a pesquisa adota uma abordagem qualitativa, de caráter exploratório, fundamentada em revisão bibliográfica interdisciplinar, que abrange a doutrina jurídica nacional e estrangeira, documentos técnicos sobre vieses algorítmicos e relatórios de organismos internacionais. Adicionalmente, são analisadas legislações estrangeiras — como o AI Act da União Europeia — e casos práticos de utilização de inteligência artificial no Brasil, a fim de realizar um estudo crítico-comparado.

A pesquisa estrutura-se em três momentos: inicialmente, apresenta-se a conceituação da inteligência artificial e suas aplicações na segurança pública; em seguida, discute-se a tensão entre eficiência investigativa e proteção de direitos fundamentais; como terceiro ponto, analisa-se o processo penal diante do uso da IA, com ênfase na admissibilidade das provas digitais e nos parâmetros de controle necessários para garantir sua legitimidade constitucional. Adicionalmente, será exposto como anda o desenvolvimento da regulação da inteligência artificial em alguns países.

Diante desse panorama, emerge o problema central que orienta o presente estudo: em que medida o uso de sistemas de inteligência artificial — especialmente o reconhecimento facial e a análise preditiva — pelos órgãos de segurança pública é compatível com os princípios constitucionais que regem o processo penal brasileiro, notadamente a presunção de inocência, a igualdade e o direito à privacidade, diante da ausência de uma regulamentação específica sobre o tema. A questão revela-se

de alta relevância prática e teórica, uma vez que o emprego dessas tecnologias, embora prometa maior eficiência investigativa, suscita o risco de violação de direitos fundamentais e de contaminação da legitimidade probatória no processo penal. Assim, compreender os limites constitucionais e processuais dessa utilização torna-se essencial para equilibrar o avanço tecnológico com a proteção das garantias individuais que sustentam o Estado Democrático de Direito.

INTELIGÊNCIA ARTIFICIAL: NATUREZA E DEFINIÇÕES

A inteligência artificial (IA), embora já integrada ao cotidiano das pessoas, suscita amplos debates quanto à sua natureza e modo de operação, sendo praticamente inviável estabelecer um conceito único e universal que a defina de forma completa e objetiva. Apesar dessa dificuldade conceitual, é possível delineá-la de maneira satisfatória a partir de diferentes perspectivas. Nesse sentido, Oliveira (2018) a caracteriza como a aptidão de sistemas cibernéticos — compostos por computadores, programas, sensores e atuadores — para replicar habilidades cognitivas humanas, sobretudo aquelas voltadas à solução de problemas, mediante processos de aprendizagem orientados pela percepção do ambiente. Em linha semelhante, Stryker e Kavlakoglu (2024) definem a IA como uma tecnologia que possibilita a computadores e máquinas simular o aprendizado, a compreensão, a resolução de problemas, a tomada de decisões, a criatividade e a autonomia típicas dos seres humanos.

Autores como Russell e Norvig (2013) classificam a inteligência artificial em duas grandes categorias: a denominada IA fraca, voltada a funções específicas, e a IA forte, que se aproximaria da capacidade cognitiva humana em sentido amplo. A primeira já é realidade consolidada, presente em mecanismos de busca, filtros de spam, reconhecimento de padrões e mesmo em sistemas de reconhecimento facial utilizados em investigações criminais. Já a segunda permanece em grande medida no campo das pesquisas teóricas, mas projeta debates éticos e jurídicos cada vez mais relevantes.

Essa ausência de consenso conceitual também se projeta no campo jurídico. O ordenamento brasileiro, por exemplo, não dispõe de uma definição normativa de inteligência artificial, limitando-se a uma mera menção a decisões automatizadas na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), sem apresentar um conceito. Em contrapartida, o AI Act da União Europeia (2024) propõe um conceito abrangente, que inclui qualquer sistema desenvolvido por técnicas automatizadas capazes de gerar resultados que influenciem ambientes físicos ou virtuais. Essa diversidade de conceituações demonstra que, para o direito, a IA não deve ser compreendida apenas sob a ótica técnica, mas também à luz de seus impactos normativos e sociais.

Em relação ao modo de funcionamento, os algoritmos que compõem os sistemas de IA operam com base em diferentes técnicas, como o machine learning, que reconhece padrões e tendências nos dados, permitindo ao sistema melhorar

suas respostas ao longo do tempo — é mais utilizado quando o objetivo é analisar grandes quantidades de dados. Uma vertente mais avançada, o deep learning, utiliza redes neurais artificiais inspiradas no cérebro humano, possibilitando à IA realizar tarefas mais complexas, como reconhecimento de voz, imagem e linguagem natural. Desse modo, a IA se desenvolve conforme interação com novos dados, o que justifica seu uso crescente em diferentes setores, como a saúde, o comércio e o direito (PUCRS, 2023).

APLICAÇÕES PRÁTICAS DO RECONHECIMENTO FACIAL E DA ANÁLISE PREDITIVA NO PROCESSO PENAL

Após a análise de sua natureza e das dificuldades conceituais que permeiam a inteligência artificial, faz-se necessário examinar como tais tecnologias se materializam na prática e impactam diretamente o campo jurídico. A despeito das divergências teóricas acerca de sua definição, o fato é que a IA já vem sendo incorporada em diversos contextos relacionados à persecução penal, tornando possível a previsão de condutas criminosas, contribuindo para a tomada de decisões judiciais e assegurando a proteção dos direitos fundamentais no âmbito do processo penal (Vieira *et al.*, 2024). Nesse sentido, entram em cena o reconhecimento facial e a análise preditiva, que ilustram os potenciais benefícios e riscos decorrentes da aplicação da inteligência artificial no processo penal.

Com a expansão do uso de câmeras de vigilância em espaços públicos e a crescente adoção de tecnologias de monitoramento por órgãos de segurança, o reconhecimento facial vem adquirindo grande relevância no debate jurídico e social. Dentre seus diversos usos, destaca-se pela crescente utilização na persecução penal e no controle estatal. Outrossim, trata-se de uma tecnologia já presente no cotidiano das pessoas em múltiplos contextos, como no desbloqueio de dispositivos móveis, na autorização de acesso a ambientes restritos, na validação de transações financeiras e até mesmo na confirmação de contratos eletrônicos (Stainr *et al.*, 2023).

Conceitualmente, o reconhecimento facial pode ser entendido como uma tecnologia de biometria que identifica indivíduos a partir das características únicas de seu rosto. O funcionamento do software baseia-se na detecção e análise de padrões faciais, os quais são comparados com imagens previamente armazenadas em bases de dados. Para tanto, os algoritmos utilizam os chamados pontos nodais — tais como a distância entre os olhos, a largura do nariz, a profundidade das órbitas e o contorno da mandíbula — a fim de criar uma espécie de “impressão digital do rosto”. Uma das vantagens dessa tecnologia é a capacidade de converter imagens bidimensionais em modelos tridimensionais, o que permite a identificação mesmo diante de variações de idade, iluminação, expressão facial ou ângulo de captura (Nama, 2021).

A utilização do reconhecimento facial tem se expandido de maneira significativa na segurança pública, em razão de sua capacidade de auxiliar na

identificação de suspeitos com elevado grau de precisão. Levantamento realizado pela revista eletrônica Consultor Jurídico aponta que já foram registradas mais de 1,7 mil prisões por meio dessa tecnologia, concentradas em sua maioria no estado da Bahia. Em outras localidades, como Rio de Janeiro e Belo Horizonte, o recurso tem sido empregado de forma recorrente em grandes eventos, especialmente durante o período carnavalesco, possibilitando a captura de indivíduos procurados por crimes diversos, incluindo homicídio, tráfico de drogas, roubo e inadimplemento de pensão alimentícia (Alcântara; Cassiano, 2024).

Com função semelhante, a predição criminal (ou policiamento preditivo) emerge como outra dimensão relevante do uso da inteligência artificial na persecução penal. Diferentemente do reconhecimento facial, que identifica indivíduos, essa modalidade foca em analisar grandes volumes de dados — relatórios policiais, registros de ocorrências e padrões de criminalidade — com o intuito de antecipar onde e quando eventos delitivos têm maior probabilidade de ocorrer. Trata-se de uma ferramenta que permite direcionar patrulhamento e recursos estatais com maior precisão operacional, mas que também impõe desafios significativos do ponto de vista ético e de direitos fundamentais (Arruda; Resende; Fernandes, 2022).

Apredição criminal pode assumir diferentes modalidades práticas, destacando-se o modelo baseado no lugar, voltado à identificação de áreas com maior probabilidade de ocorrência de delitos, e o modelo baseado na pessoa, que utiliza informações como histórico criminal, registros de prisões e de liberdade condicional para atribuir uma espécie de “pontuação de risco” a determinados indivíduos. Essas técnicas têm sido utilizadas para orientar a alocação de recursos policiais e o planejamento de operações de segurança, funcionando como instrumentos de apoio à tomada de decisão estatal (Arruda; Resende; Fernandes, 2022).

Além dos exemplos tradicionais de mapeamento de pontos de alta criminalidade, a predição criminal está sendo expandida para o ambiente digital. Um exemplo é a análise de dados em redes sociais, onde algoritmos podem processar postagens, compartilhamentos e informações de geolocalização para identificar padrões de comportamento e interações que possam indicar a iminência de crimes. Ademais, tais técnicas são capazes de construir perfis de risco individuais, de modo que o sistema pode atribuir pontuações a pessoas com base em seu histórico criminal, afiliações a grupos e até mesmo atividades em redes sociais, como o uso de linguagens ou o compartilhamento de imagens associadas a gangues (Kar, 2024).

O DIREITO À PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

O direito à privacidade, por seu enquadramento como um direito da personalidade e, principalmente, como direito fundamental, revela também a necessidade de seu tratamento cuidadoso e adequado às questões da sociedade contemporânea. Em sua acepção mais ampla, a privacidade trata-se do direito

que tem o indivíduo de manter indevassados dados e informações que lhe digam respeito. Essa proteção reflete os valores constitucionais da dignidade da pessoa humana e da liberdade, pilares centrais da ordem jurídica brasileira (Hirata, 2017).

A ampliação do uso do reconhecimento facial automatizado, aliado à crescente adoção de inteligência artificial em investigações criminais, coloca em evidência o direito à privacidade e à proteção de dados pessoais, especialmente no contexto do Estado de Direito brasileiro. Na Constituição Federal, o art. 5º, X, assegura que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas”. No plano infraconstitucional, a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) estabelece que o uso de informações sensíveis — como dados biométricos — deve respeitar princípios como finalidade, necessidade, e segurança, mecanismos-chave afetados pelo advento de técnicas avançadas de análise facial e algoritmos preditivos.

Embora o uso de tecnologias de reconhecimento facial nos sistemas de vigilância do setor público brasileiro esteja em expansão, ainda não há ferramentas adequadas para uma análise objetiva dos riscos envolvidos na sua implementação. Nesse sentido, ainda que a tecnologia represente uma poderosa ferramenta de combate à criminalidade, sua adoção demanda acompanhamento por meio de uma robusta estrutura regulatória que proteja os direitos dos cidadãos, com garantias como transparência, consentimento informado e proteção de dados sensíveis. Sem um marco regulatório bem definido e a vigilância constante da sociedade civil e de instituições de direitos humanos, o uso dessa tecnologia pode descambar em violações generalizadas ao direito à privacidade e demais liberdades fundamentais (Silva *et al*, 2024).

A Lei Geral de Proteção de Dados (LGPD) disciplina de forma rigorosa o tratamento de dados pessoais no Brasil, estabelecendo distinções fundamentais entre dados pessoais comuns e dados pessoais sensíveis. Dados pessoais são aqueles que permitem a identificação direta ou indireta de uma pessoa natural — incluem nome, CPF, imagem, endereço, entre outros. No ambiente de inferência comportamental por IA, também são considerados dados pessoais os que formam perfis identificáveis de indivíduos (Brasil, 2024).

Além disso, a Autoridade Nacional de Proteção de Dados (ANPD) lançou, em junho de 2024, o segundo volume do seu “Radar Tecnológico — Biometria e Reconhecimento Facial”, no qual enfatiza os perigos dessa tecnologia quando não há diretrizes claras de governança e manejo de riscos — destacando preocupações com vazamento de dados, viés algorítmico e falta de transparência (ANPD, 2024).

No âmbito da investigação criminal, esta deve ocorrer em harmonia com os preceitos da Lei Geral de Proteção de Dados, isso significa que a coleta e o uso de informações faciais só podem ser admitidos quando indispensáveis à persecução penal, mediante base legal adequada e acompanhados de mecanismos de governança e mitigação de riscos. Assim, a compatibilização entre eficiência investigativa e salvaguarda dos direitos fundamentais não constitui apenas exigência ética, mas verdadeiro imperativo jurídico, sem o qual a adoção de tais tecnologias pode comprometer a legitimidade da atuação estatal e a confiança social no sistema de justiça criminal (ANPD, 2024).

PRESUNÇÃO DE INOCÊNCIA E DEVIDO PROCESSO LEGAL

Apresunção de inocência, também chamada de princípio da não culpabilidade, constitui um dos pilares do devido processo legal e representa a garantia de que ninguém poderá ser considerado culpado antes do trânsito em julgado de sentença penal condenatória. Esse princípio, previsto expressamente no artigo 5º, inciso LVII, da Constituição Federal, encontra respaldo tanto na tradição do constitucionalismo brasileiro quanto em tratados internacionais de direitos humanos ratificados pelo país, como a Convenção Americana sobre Direitos Humanos (art. 8.2).

Trata-se de cláusula pétrea, ou seja, insuscetível de supressão, que assegura ao indivíduo o direito de responder em liberdade até que sua culpabilidade seja definitivamente comprovada, salvo em hipóteses excepcionais previstas em lei, como nas prisões cautelares. Nesse sentido, observa-se que a presunção de inocência configura não apenas uma regra probatória, que impõe ao acusador o ônus da prova, mas também uma regra de tratamento, que impede que o acusado seja tratado como culpado antes da condenação definitiva (Andrade, [2020?]).

Quando colocamos essa matriz principiológica em diálogo com as tecnologias de investigação baseadas em inteligência artificial, surgem tensões evidentes. O reconhecimento facial, por exemplo, ao identificar automaticamente um indivíduo em espaço público e classificá-lo como suspeito, muitas vezes sem a necessária intervenção humana qualificada, pode criar um estado de culpabilidade antecipada, invertendo a lógica da presunção de inocência (ANPD, 2024). Casos de falsos positivos acontecem com certa frequência, em que pessoas inocentes chegam a ser detidas em razão de falhas no sistema. Tais erros ocorrem principalmente quando se trata de pessoas negras, o que gera uma espécie de racismo institucional, que quando não submetido a mecanismos robustos de controle, compromete diretamente essa garantia fundamental de presunção de inocência (BDF, 2024).

IGUALDADE E RISCO DE DISCRIMINAÇÃO ALGORÍTMICA

O princípio da igualdade, consagrado no artigo 5º, caput, da Constituição Federal de 1988, assegura que “todos são iguais perante a lei, sem distinção de qualquer natureza [...]”. Trata-se de cláusula fundamental que orienta a atuação do Estado e protege os indivíduos contra discriminações arbitrárias, sendo considerado um dos pilares do Estado Democrático de Direito. Tal dispositivo tem a missão de impedir que critérios seletivos e discriminatórios sejam criados pelo poder estatal, consagrando um tratamento igualitário perante a lei (Masson, 2019).

De forma mais profunda, a igualdade ainda pode ser observada sob a ótica formal e a material. A primeira refere-se ao tratamento uniforme de todos perante a lei, vedando distinções arbitrárias. Já a segunda parte da premissa de que não basta ao Estado abster-se de discriminar, sendo também seu dever adotar medidas ativas para assegurar igualdade de oportunidades. Isso se concretiza por meio da elaboração de leis e da implementação de políticas públicas voltadas à redução ou eliminação das desigualdades existentes na realidade social (Silva, 2017).

Com base no princípio da igualdade, ao se analisar a inserção de sistemas de inteligência artificial na persecução penal, torna-se evidente a necessidade de uma avaliação criteriosa acerca da forma como essas ferramentas serão utilizadas. Por se tratar de uma criação humana, a inteligência artificial inevitavelmente reflete características transmitidas por seus programadores. Isso implica reconhecer que, ainda que concebidos sob parâmetros objetivos e lógicos, tais sistemas permanecem suscetíveis à reprodução de estigmas e vieses presentes na sociedade (Mendes; Mattiuzzo, 2019).

A inteligência artificial estrutura-se a partir de regras e procedimentos destinados à execução de tarefas específicas, geralmente voltadas à identificação de padrões e à geração de insights a partir de dados, bem como à previsão de resultados com base em determinadas variáveis de entrada. Nessa lógica, quanto maior o volume de informações disponíveis, melhor tende a ser o desempenho do sistema desenvolvido. Contudo, os bancos de dados utilizados no treinamento dos algoritmos — conhecidos como big data — representam a origem de inúmeros problemas relacionados à discriminação algorítmica, seja pela quantidade imensa de informações que reúnem, bem como pela ausência de filtros adequados (Mendes; Mattiuzzo, 2019).

A chamada discriminação algorítmica decorre justamente do fato de que sistemas de inteligência artificial não são neutros, mas refletem os padrões e vieses presentes nos dados com os quais são treinados. Embora computadores não tenham opinião própria, os filtros e critérios utilizados para identificar, moderar e reproduzir conteúdo carregam inevitavelmente a marca de seus criadores humanos. Assim, preconceitos como racismo, machismo ou homofobia podem ser incorporados e amplificados pelos algoritmos (Caon, 2021).

Um exemplo emblemático foi o chatbot Tay, lançado pela Microsoft em 2016, que, ao aprender com interações de usuários por meio de machine learning, rapidamente passou a adotar discursos discriminatórios, reproduzindo e disseminando estereótipos presentes na sociedade. O episódio demonstra como a ausência de salvaguardas adequadas permite que a tecnologia se torne um espelho das opressões sociais, reforçando desigualdades em vez de superá-las (Caon, 2021).

Em relação aos dispositivos de reconhecimento facial, que em tese deveriam ser uma forma objetiva e imparcial de identificar indivíduos, comumente apresentam um péssimo desempenho para identificar pessoas negras, sobretudo mulheres. Essa dificuldade de identificar corretamente pessoas negras recebe o nome de viés racial e, no âmbito dos sistemas de reconhecimento facial, pode acarretar sérias consequências, como prisões equivocadas de pessoas negras e o consequente sentimento de que mais uma vez o Estado falhou ao garantir proteção e respeito à população negra (Santos *et al.*, 2023).

Um caso de bastante repercussão envolvendo reconhecimento facial ocorreu com Robert Williams, homem negro estadunidense, acusado de roubar uma loja de luxo. Ele foi abordado e algemado na porta de sua casa, em frente as suas duas filhas e esposa. A prisão ocorreu com o auxílio de um sistema de reconhecimento facial

que, ao comparar a foto da carteira de motorista de Robert com o vídeo do assalto, filmado pelas câmeras de segurança, soltou o alerta para a prisão. Posteriormente foi constatado que Williams era inocente (Santos *et al.*, 2023).

A situação narrada demonstra uma forte necessidade de acompanhar astuciosamente a integração da inteligência artificial no processo de investigação criminal. Pontua André Estefam (2023) que o Direito Penal só deve agir quando houver uma “grave lesão ou perigo a um bem jurídico fundamental para a paz e o convívio em sociedade”, isso se deve ao fato de que a persecução penal é a forma mais invasiva que o Estado dispõe para apuração de ilícitos. Assim, ao implementar sistemas inteligentes, os órgãos de segurança pública não devem observar apenas a promessa de eficiência e capacidade operacional, mas, principalmente, a capacidade de entender as inerentes falhas que acompanham tais dispositivos e tomar todas as cautelas necessárias para que não aconteça com outras pessoas o ocorrido com Robert Williams.

A ADMISSIBILIDADE DAS PROVAS DIGITAIS E O RISCO DAS PROVAS ILÍCITAS

O Código de Processo Penal admite a introdução de diferentes meios de prova, como o exame de corpo de delito, a oitiva de testemunhas e o reconhecimento de pessoas e coisas. Entretanto, ainda que não haja referência expressa às chamadas provas atípicas — categoria em que se inserem as provas digitais —, o Superior Tribunal de Justiça já firmou entendimento de que o sistema probatório previsto no CPP não é taxativo. Assim, admite-se a produção de provas não disciplinadas em lei, desde que observadas determinadas restrições, conforme decidido no HC n. 740.431/DF, de relatoria do Ministro Rogerio Schietti Cruz, Sexta Turma, julgado em 13/9/2022 (DJe de 19/9/2022).

Sabendo que as provas digitais são meios aceitos no processo penal, cumpre destacar o que elas são, conforme bem conceituado por Thamay e Tamer (2020, *apud* Silva, 2022):

(...) o instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento de sua demonstração. A prova digital é o meio de demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato (e) de seu conteúdo.

Pelo conceito apresentado, observa-se que as provas digitais possuem características que as distinguem das provas tradicionais, também chamadas de analógicas. Entre essas particularidades, destacam-se a imaterialidade, por não possuírem suporte físico; a volatilidade, em razão da facilidade com que podem sofrer alterações em sua composição; e o desprendimento do corpo físico, já que podem ser transferidas entre dispositivos ou reproduzidas em múltiplas cópias, sem perda do conteúdo original (Saad *et al.*, 2024).

O artigo 5º, inciso LVI, da Constituição Federal estabelece que “são inadmissíveis, no processo, as provas obtidas por meios ilícitos”, consagrando um dos mais importantes limites à atividade probatória do Estado. Esse dispositivo expressa o compromisso do ordenamento jurídico com a proteção dos direitos fundamentais, assegurando que a busca pela verdade real não se sobreponha à legalidade e à dignidade da pessoa humana. No contexto contemporâneo, em que a produção de provas passa a envolver instrumentos tecnológicos complexos e fontes digitais, a observância desse preceito constitucional assume relevância ainda maior. A licitude do meio de obtenção e a integridade do procedimento de coleta e armazenamento tornam-se elementos indispensáveis para que a prova digital seja admitida no processo penal, sob pena de comprometimento da legitimidade da persecução estatal.

Nessa perspectiva, quando os órgãos de segurança pública realizam procedimentos de reconhecimento facial ou de análise preditiva, é indispensável a adoção de medidas que assegurem a integridade e a legitimidade dos dados utilizados, de modo a evitar que os resultados da operação sejam contaminados por informações obtidas de forma abusiva ou sem a devida verificação. A prova digital, por sua natureza técnica e dinâmica, demanda um tratamento processual diferenciado, no qual a cadeia de custódia deve ser rigorosamente observada e adaptada às suas especificidades, garantindo a autenticidade e a confiabilidade dos elementos probatórios produzidos (Saad *et al.*, 2024).

Enquanto a prova documental tradicional, em papel, apresenta elevada confiabilidade em razão da estabilidade do suporte em que a informação é registrada — como ressaltam Marinoni e Arenhart (*apud* Silva, 2020) —, a prova digital caracteriza-se pela volatilidade e pela facilidade de alteração de seu conteúdo. O documento físico, uma vez assinado, goza de presunção de autenticidade, cabendo ao impugnante o ônus de provar eventual falsidade (arts. 410, II; 412 e 429, I, do CPC). Já os documentos produzidos em meio eletrônico, por estarem armazenados em ambientes sujeitos a regravações constantes e grande fluxo de dados, carecem dessa estabilidade, podendo ser modificados com relativa facilidade. Assim, a confiabilidade da prova digital depende de mecanismos técnicos capazes de assegurar que a informação apresentada corresponda, de fato, à original.

Para que as provas digitais possuam a mesma credibilidade das provas em suporte físico, é indispensável que atendam a requisitos específicos de validade, capazes de garantir a sua segurança jurídica. Esses requisitos são: autenticidade, integridade e preservação da cadeia de custódia. A autenticidade refere-se à identificação clara da origem do documento digital e de sua autoria; a integridade, à manutenção inalterada do conteúdo armazenado, de modo que não haja dúvidas quanto à fidedignidade das informações; e a cadeia de custódia, à documentação de todas as etapas pelas quais a prova digital passa, desde sua coleta até sua apresentação em juízo. A ausência de qualquer desses elementos compromete a confiabilidade do material e pode torná-lo inapto à produção de efeitos no processo judicial (Silva, 2020).

ATEORIA DOS FRUTOS DA ÁRVORE ENVENENADA APLICADA À IA

A chamada teoria dos frutos da árvore envenenada (*fruits of the poisonous tree*) teve origem na jurisprudência da Suprema Corte dos Estados Unidos, a partir do caso *Silverthorne Lumber Co. v. United States* (1920), sendo posteriormente consolidada em *Mapp v. Ohio* (1961). De acordo com essa doutrina, toda prova obtida por meio ilícito — a “árvore envenenada” — contamina as provas dela derivadas — os “frutos” —, tornando-as igualmente inadmissíveis no processo. O objetivo é impedir que o Estado se beneficie de violações de direitos fundamentais para sustentar uma acusação, reafirmando o princípio da legalidade e a supremacia do devido processo legal.

No ordenamento jurídico brasileiro, tal orientação encontra amparo no art. 5º, inciso LVI, da Constituição Federal, que estabelece a inadmissibilidade das provas ilícitas, e foi incorporada expressamente ao art. 157, §§1º e 2º, do Código de Processo Penal, que também veda a utilização de provas derivadas das ilícitas, salvo quando demonstrada a independência entre elas ou a descoberta inevitável.

A doutrina nacional reconhece que a teoria exerce papel essencial na preservação da legitimidade da persecução penal e na limitação da atuação estatal. Para Aury Lopes Jr. (2022), “devem ser desentranhados o ato originariamente viciado e todos os que dele derivem ou decorram, pois igualmente ilícita é a prova que deles se obteve.”. De forma semelhante, Renato Brasileiro de Lima (2020) observa que a teoria dos frutos da árvore envenenada traduz a ideia de que não é possível extrair validade de um ato processual cuja origem é viciada. Assim, o princípio da licitude probatória não se restringe à forma de obtenção da prova, mas alcança também toda a cadeia de informações e evidências que dela decorrem, funcionando como um filtro ético e jurídico indispensável à preservação da justiça e da confiabilidade das decisões judiciais.

A aplicação da teoria dos frutos da árvore envenenada assume especial relevância no contexto das investigações criminais que utilizam sistemas de inteligência artificial, como o reconhecimento facial e a análise preditiva. Tais tecnologias dependem do tratamento de grandes volumes de dados pessoais, os quais, se forem obtidos ou processados sem a devida observância das garantias legais previstas na Lei Geral de Proteção de Dados Pessoais, comprometeriam toda a persecução penal.

Assim, se as bases de dados empregadas na programação ou no funcionamento de sistemas algorítmicos forem constituídas a partir de informações coletadas de maneira ilícita — sem consentimento, transparência ou finalidade legítima —, todo o produto gerado pela inteligência artificial estará igualmente maculado. Nesse cenário, Vaz (2023) considera que houve uma quebra da cadeia de custódia, o que leva à inutilização da prova, razão pela qual é vedada a sua valoração, devendo haver o seu desentranhamento do processo.

Diante do exposto, surgem diversos pontos que merecem atenção. A princípio, tem-se a cadeia de custódia prevista no Código de Processo Penal, que embora tenha trazido grandes mudanças positivas, não é capaz de regular as provas digitais com o rigor e técnica que elas exigem. Apesar da omissão legislativa, é possível utilizar a norma ABNT ISO/IEC 27037:2013, que traz diretrizes para identificação, coleta, aquisição e preservação de provas digitais.

A referida norma ISO elenca diversas características que devem estar presentes nas provas digitais para que estas tenham validade, a dizer: a) relevância; b) confiabilidade; c) suficiência; d) justificabilidade; e) auditabilidade; f) repetibilidade; e g) reprodutibilidade (Vaz, 2023). Dessa forma, é possível enxergar o quão complexa é a utilização desses meios de prova no processo penal. A análise preditiva e, principalmente, o reconhecimento facial — pela quantidade massiva de dados que utiliza —, encontram enormes desafios ao se depararem com os requisitos da norma ABNT ISO/IEC 27037:2013.

Outrossim, o avanço do mundo digital exige uma releitura da teoria dos frutos da árvore envenenada, especialmente quando aplicada aos sistemas de inteligência artificial. No contexto algorítmico, em que se operam grandes volumes de dados, frequentemente não é possível identificar de maneira transparente quais parâmetros ou critérios conduziram o sistema às suas conclusões — fenômeno conhecido como *black box* ou caixa preta (Kosinski, [2024?]). Essa opacidade dificulta a verificação da licitude das informações utilizadas e, por consequência, compromete a avaliação sobre a validade tanto da “árvore” — a fonte originária resultante da interpretação algorítmica — quanto de seus “frutos” — os desdobramentos derivados dessa fonte. Em outras palavras, a ausência de transparência algorítmica pode inviabilizar a identificação da eventual contaminação ilícita da prova digital, dificultando a aplicação do mandamento constitucional previsto no artigo 5º, inciso LVI.

Em síntese, a teoria dos frutos da árvore envenenada traduz o princípio de que a busca da verdade no processo penal não pode ser realizada a qualquer preço, exigindo o respeito irrestrito aos direitos e garantias fundamentais da pessoa humana. Segundo Brasileiro (2020), a vedação ao uso de provas ilícitas (CF, art. 5º, LVI) funciona como um crucial mecanismo de controle da regularidade da persecução penal, atuando de forma a inibir a adoção de práticas probatórias ilegais por parte do Estado-acusador e cumprindo uma eminente função pedagógica. Seria contraditório e comprometeria a legitimidade de todo o sistema punitivo que o próprio Estado se valesse de métodos violadores de direitos para sustentar uma acusação. Destarte, o mandamento constitucional desautoriza qualquer elemento probatório cuja obtenção decorra da transgressão a cláusulas de ordem constitucional ou legal, repelindo a máxima do *male captum, bene retentum* (mal colhida, mas bem conservada). A teoria impede, em sua essência, que se extraia validade de um ato processual cuja origem é viciada, alcançando toda a cadeia de informações que dela derivem, garantindo um processo justo.

NECESSIDADE DE TRANSPARÊNCIA ALGORÍTMICA FRENTE AO PANORAMA MUNDIAL DE REGULAMENTAÇÃO DA IA

O avanço exponencial de sistemas de Inteligência Artificial (IA) nas investigações criminais, especialmente por meio de tecnologias como o reconhecimento facial e a análise preditiva, impôs um novo e inadiável requisito para a legitimidade processual: a transparência algorítmica. Em uma era digital onde os algoritmos estão profundamente inseridos em decisões que afetam direitos fundamentais, definindo desde resultados de buscas até sentenças judiciais, a urgência em compreender como esses sistemas operam se tornou o novo alicerce da confiança digital. Conforme aponta o debate contemporâneo sobre o tema, a transparência não é apenas uma exigência técnica, mas sim um imperativo ético e jurídico para que os processos de decisão automatizados sejam considerados compreensíveis, auditáveis e, sobretudo, explicáveis. Sem essa clareza sobre os dados utilizados, os critérios definidores e os riscos associados, a “caixa-preta” algorítmica compromete a capacidade de questionamento e contestação, essencial para a defesa em um processo penal (Santos, 2025).

A necessidade de transparência e regulamentação decorre justamente da natureza não neutra e potencialmente enviesada dos algoritmos. Desenvolvidos por humanos e treinados com bases de dados que podem refletir e reforçar vieses sociais e estruturais, esses sistemas carregam riscos inerentes de discriminação, erro e aprofundamento de desigualdades. Quando aplicados ao contexto da investigação criminal, onde o direito à liberdade e o devido processo legal estão em jogo, a opacidade algorítmica pode obscurecer a origem de uma prova digital, impedindo a verificação de sua licitude. Assim, a regulação se torna vital para estabelecer o que de fato significa ser transparente neste contexto: não a revelação irrestrita de um código-fonte, mas a garantia de que os critérios de tomada de decisão e os impactos de risco do sistema sejam plenamente explicados e documentados, permitindo que o acusado e a autoridade judicial possam questionar, corrigir e entender o resultado da aplicação da IA, promovendo, por fim, uma Inteligência Artificial (IA) mais compreensível e responsável (Santos, 2025).

Ao se observar o cenário global, nota-se um movimento crescente em direção à regulamentação da inteligência artificial, impulsionado pela necessidade de conciliar inovação tecnológica com a proteção de direitos fundamentais. Essas iniciativas variam conforme as tradições jurídicas, os marcos normativos internos, o grau de maturidade institucional e o estágio de desenvolvimento tecnológico de cada país. À medida que a legislação evolui, espera-se que os sistemas inteligentes sejam concebidos de forma mais transparente, ética e responsável, o que poderá gerar impactos positivos diretos na precisão dos softwares de reconhecimento facial e na confiabilidade dos modelos de análise preditiva, tornando-os mais alinhados à realidade e aos princípios constitucionais que regem a persecução penal (Soares, 2025).

A União Europeia instituiu o AI Act (Regulation (EU) 2024/1689) como o primeiro marco jurídico abrangente para inteligência artificial no mundo, com o

objetivo de garantir que sistemas de IA sejam confiáveis, seguros e compatíveis com os direitos fundamentais. O regulamento adota uma abordagem baseada em níveis de risco (*risk-based approach*), classificando os sistemas de IA conforme seu potencial de causar danos. Sistemas que envolvem a coleta aleatória de dados para identificação biométrica em tempo real em espaços públicos, ou avaliação de risco criminal individual, por exemplo, são considerados de risco inaceitável (*unacceptable risk*) e estão proibidos, salvo exceções muito bem justificadas. Isso por si só já demonstra um grande avanço, visto que impede uma varredura descontrolada de dados disponíveis na internet (European Commission, 2025).

No oriente, a China adotou um modelo regulatório multicamadas, fortemente centrado na supervisão estatal, que combina medidas setoriais, normas técnicas e exigências administrativas para fornecedores de IA. Nesse arranjo, a Administração do Ciberespaço da China (CAC) e o Ministério da Indústria e Tecnologia da Informação (MIIT) desempenham papel central — impondo, entre outras obrigações, o registro de algoritmos, avaliações de segurança para serviços com potencial de mobilização social e requisitos técnicos para dados e modelos de IA. O país tem ainda editado normas específicas, como medidas provisórias sobre IA generativa e regras de rotulagem de conteúdo gerado por IA, além de aprimorar requisitos de segurança para conjuntos de treinamento (p. ex., verificação de amostras de dados) — tudo dentro de uma lógica que prioriza a estabilidade social e a segurança nacional (Soares, 2025).

No âmbito das investigações criminais, esse quadro regulatório apresenta dupla implicação: por um lado, as obrigações de registro, avaliação de segurança e requisitos sobre qualidade de dados podem oferecer ferramentas formais para controles técnicos sobre sistemas de reconhecimento facial e mecanismos preditivos; por outro, a ênfase estatal na supervisão e no controle de conteúdo cria um ambiente em que o uso destes sistemas pela polícia e por órgãos de segurança pode ser amplamente integrado às políticas públicas, com risco de expansão da vigilância em massa. Ademais, existem preocupações sobre uso público excessivo e possíveis impactos sobre direitos (incluindo o risco de reforço de discriminações), bem como para o efeito extraterritorial das normas chinesas à medida que tecnologias e produtos regulados na China se difundem internacionalmente. Assim, por mais que a regulação da IA na China represente avanços, é necessário ter em mente que isso poderá aumentar ainda mais o controle estatal (Soares, 2025).

No Brasil, o debate sobre a regulamentação da inteligência artificial ainda se encontra em estágio inicial, com alguns projetos em tramitação no Congresso. O Projeto de Lei n.º 2.338/2023, que propõe o Marco Legal da Inteligência Artificial, busca estabelecer princípios, direitos e deveres para o desenvolvimento e a aplicação da IA, inspirando-se parcialmente no modelo europeu de regulação por níveis de risco. Entre seus fundamentos, destacam-se a centralidade da pessoa humana, a transparência, a não discriminação algorítmica e a responsabilização dos agentes envolvidos na criação e uso de sistemas inteligentes. A expectativa é que o projeto seja sancionado e se torne lei em breve.

Contudo, como observa Soares (2025), o texto ainda carece de especificidade quanto ao uso policial e às implicações penais desses sistemas, deixando lacunas importantes na delimitação da coleta e tratamento de dados biométricos e preditivos. Essa ausência de normas claras aumenta o risco de violações a direitos fundamentais, especialmente no uso de tecnologias como o reconhecimento facial e a análise preditiva em investigações criminais, que demandam parâmetros de licitude, auditabilidade e supervisão humana para se compatibilizarem com os princípios constitucionais da legalidade, privacidade e presunção de inocência.

CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste estudo permitiu constatar que o uso de sistemas de inteligência artificial nas investigações criminais — especialmente as tecnologias de reconhecimento facial e análise preditiva — apresenta um duplo caráter: de um lado, o potencial de aprimorar a eficiência das atividades de persecução penal; de outro, a possibilidade concreta de violar direitos e garantias fundamentais assegurados pela Constituição Federal de 1988. A ausência de um marco normativo específico e de mecanismos adequados de governança de dados tem contribuído para o uso desordenado dessas ferramentas, expondo cidadãos a riscos de discriminação, vigilância excessiva e produção de provas ilícitas.

Em síntese crítica, verificou-se que o reconhecimento facial, embora seja um importante instrumento de identificação e captura de suspeitos, tem gerado casos de falsos positivos e reproduzido vieses raciais e sociais presentes nas bases de dados, o que afronta os princípios da igualdade e da presunção de inocência. Do mesmo modo, os sistemas de análise preditiva — ao prever comportamentos com base em padrões estatísticos — desafiam o devido processo legal e o direito à privacidade, pois tratam dados sensíveis de maneira opaca, sem a devida transparência algorítmica. O exame jurídico-dogmático evidenciou que o ordenamento brasileiro contém alguns instrumentos aptos a limitar abusos, como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), o art. 5º, LVI, da Constituição e o art. 157 do Código de Processo Penal. Contudo, tais normas ainda não são suficientes para regular toda a gama de cenários em que a IA está presente.

Respondendo ao problema de pesquisa, conclui-se que o uso de sistemas de inteligência artificial pelos órgãos de segurança pública só será compatível com o processo penal constitucional se observar rigorosamente os princípios da legalidade, da proporcionalidade, da transparência e da proteção de dados pessoais. Em outras palavras, a eficiência tecnológica não pode se sobrepor à dignidade humana, devendo ser implementada dentro de um modelo de responsabilidade algorítmica e de controle jurisdicional efetivo. Caso contrário, a utilização indiscriminada desses sistemas tende a corroer a legitimidade da persecução penal e a confiança social nas instituições públicas.

Diante disso, propõe-se que a utilização constitucionalmente válida da inteligência artificial em investigações criminais esteja condicionada à observância

de critérios técnicos e jurídicos bem definidos. Em primeiro lugar, é necessário que haja base legal específica para o tratamento de dados pessoais sensíveis e mecanismos de auditoria independente que assegurem a rastreabilidade das decisões automatizadas. Em segundo lugar, impõe-se a publicidade dos parâmetros algorítmicos essenciais, garantindo a possibilidade de contestação e revisão judicial. Ademais, deve-se adotar a preservação integral da cadeia de custódia digital, nos termos da norma ABNT ISO/IEC 27037:2013, para garantir autenticidade e integridade probatória. Por fim, urge a criação de uma regulação setorial para o uso da IA em segurança pública, à semelhança do AI Act europeu, que estabeleça níveis de risco, imponha limites claros à vigilância biométrica e institua salvaguardas efetivas contra a discriminação algorítmica.

Assim, o desafio contemporâneo consiste em construir um modelo de governança da inteligência artificial que harmonize o avanço tecnológico com os direitos fundamentais, reafirmando que a persecução penal, em um Estado Democrático de Direito, deve ser conduzida dentro dos marcos da Constituição e da ética pública. A tecnologia pode — e deve — servir à justiça, mas nunca às custas da liberdade e da igualdade que sustentam a própria legitimidade do sistema penal brasileiro.

REFERÊNCIAS

ANDRADE, Milena Almeida de. **Aspectos Gerais do Princípio da Presunção de Inocência**. Etic 2000, p. 1-16, [2020?].

ARRUDA, Ana Julia Pozzi; RESENDE, Ana Paula Bougleux Andrade; FERNANDES, Fernando Andrade. **Sistemas de policiamento preditivo e afetação de direitos humanos à luz da criminologia crítica**. Direito Público, [S. l.], v. 18, n. 100, 2022. DOI: 10.11117/rdp.v18i100.5978. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5978> Acesso em: 11 out. 2025.

BDF. **Abordagens por reconhecimento facial têm 10% de falsos positivos, diz PM na Alerj**. BdF, Rio de Janeiro, 2024. Disponível em: <https://www.brasildefato.com.br/2024/09/04/abordagens-por-reconhecimento-facial-tem-10-de-falsos-positivos-diz-pm-na-alerj/> . Acesso em: 17 set. 0). Rio de Janeiro: Forense, 2019.

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: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 ago. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. **Agência Nacional de Proteção de Dados**. Gov.br, 2024. Disponível em: <https://www.gov.br/anpd/pt-br/aceso-a-informacao/perguntas-frequentes/perguntas-frequentes?>. Acesso em: 17 set. 2025.

CAON, Felipe. **A discriminação algorítmica é a mais nova forma de opressão.** Conjur, 2021 Disponível em: <https://www.conjur.com.br/2021-nov-11/caon-discriminacao-algoritmica-forma-opressao/>. Acesso em: 27 de set. 2025.

CASSIANO, Letícia; ALCÂNTARA, Maria Clara. **Carnaval: capitais utilizam reconhecimento facial para procurar foragidos nas festas.** CNN Brasil, São Paulo, 2024. Disponível em: <https://www.cnnbrasil.com.br/nacional/carnaval-capitais-utilizam-reconhecimento-facial-para-procurar-foragidos-nas-festas/>. Acesso em: 05 set. 2025.

CEBRIAN, Fabiana S. P. Faraco *et al.* **Biometria e reconhecimento facial.** Radar Tecnológico, Brasília-DF, v. 2, p. 1-51, 2024.

COMMISSION, Europe. AI Act. **European Commission, [2024?]**. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>. Acesso em: 09 set. 2025.

FURTADO, Natalia; BARRETO, Anna Luiza. **Dez milhões de pessoas curtiram o carnaval no Rio [...].** CBN. Rio de Janeiro, 2025. Disponível em: <https://cbn.globo.com/rio-de-janeiro/noticia/2025/03/10/dez-milhoes-de-pessoas-curtiram-o-carnaval-no-rio-50-foram-presas-com-ajuda-do-sistema-de-reconhecimento-facial-diz-porta-voz-da-pm.ghhtml>. Acesso em: 05 set. 2025.

HIRATA, Alessandro. Direito à privacidade. Ed. 1. **Enciclopédia Jurídica da PUCSP, 2017.** Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade>. Acesso em: 06 set. 2025.

JR., Aury Lopes. **Direito Processual Penal.** São Paulo: SaraivaJur, 2022.

KAR, Spandan. **Predictive Policing Examples and Case Studies.** IGNEsa, 2024. Disponível em: <https://ignesa.com/insights/predictive-policing-examples/> . Acesso em: 05 set. 2025.

KOSINSKI, Matthew. **What is black box artificial intelligence (AI)?**. IBM, [2024?]. Disponível em: <https://www.ibm.com/think/topics/black-box-ai> . Acesso em: 07 dez. 2025.

LIMA, Renato Brasileiro de. **Manual de processo penal: volume único.** 8ª ed. Salvador: Editora JusPodivm, 2020.

MASSON, Cleber. **Direito Penal: parte geral (arts. 1o a 12).** 13ª ed. São Paulo, SP: Editora Método, 2019.

MENDES, Laura Schertel; MATTIUZZO, Marcela. **Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias.** Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. Direito Público, Porto Alegre, v. 16, p. 39-64, 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019> .Acesso em: 20 set. 2025.

NAMA, Redação. **Reconhecimento facial: conheça o lado A e B da tecnologia.** Nama. 2021. Disponível em: <https://simple.nama.ai/post/entenda-como-funciona-o-reconhecimento-facial>. Acesso em: 05 set. 2025.

OLIVEIRA, Ruy Flávio de. **Inteligência Artificial.** Londrina: Editora e Distribuidora Educacional S.A., 2018.

ONLINE, PUCRS. **Inteligência Artificial: o que é e como funciona.** PUCRS Online. 2023. Disponível em: <https://online.pucrs.br/blog/inteligencia-artificial>. Acesso em: 20 ago. 2025.

PUHL, Eduardo; CASTRO, Matheus Felipe de. **Reconhecimento facial como meio de prova no processo penal.** In: STAINR, Nara Suzana; CARMO, Valter Moura do; PONTE, Antonio Carlos da (org.). *Direito Penal, Processo Penal e Criminologia IV.* Florianópolis: CONPEDI, 2023. p. 1–26. Disponível em: <https://www.conpedi.org.br/>. Acesso em: 11 out. 2025.

RUSSELL, Stuart J.; NORVIG, Peter. **Inteligência Artificial.** Rio de Janeiro: Elsevier Editora Ltda., 2013.

SAAD, Marta *et al.* A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. **Rev. Bras. de Direito Processual Penal, Porto Alegre**, v. 10, n. 3, p. 1-34, 2024.

SANTOS *et al.* Reconhecimento facial: Tecnologia, racismo e construção de mundos possíveis. **Revista Psicologia e Sociedade, Rio de Janeiro**, v. 35, 2023. Disponível em: <https://www.scielo.br/j/psoc/a/wJFV8yjBB7cYnm3q6SXDjF/?lang=pt> Acesso em: 27/09/2025.

SANTOS, Tibério. **Transparência Algorítmica: O novo requisito da confiança digital.** EUNERD, 2025. Disponível em: https://encontreunmerd.com.br/blog/transparencia-algoritmica-o-novo-requisito-da-confianca-digital?srsId=AfmBOorQ2FCB1lv911Z2UgY6tlw6gC-NfLLk3n25_swINuewIkP97v. Acesso em: 09 set. 2025.

SILVA, Carolina Dias Martins da Rosa e. **Igualdade formal x igualdade material: a busca pela efetivação da isonomia.** *Conteúdo Jurídico*, p. 1-5, 2025.

SILVA, Claudécir Freitas da; *et al.* O Uso do Reconhecimento Facial na Segurança Pública: Divergência entre o Combate à Criminalidade e o Direito à Privacidade. **RevistaFT**, v. 28, 2024. DOI: 10.5281/zenodo.12682278. Disponível em: <https://revistaft.com.br/o-uso-do-reconhecimento-facial-na-seguranca-publica-divergencia-entre-o-combate-a-criminalidade-e-o-direito-a-privacidade/>. Acesso em: 06 set. 2025.

SILVA, José Antônio Ribeiro de Oliveira. A prova digital: Um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova. **Rev. TST, São Paulo**, vol. 88, n.2, abr/jun, 2022.

SOARES, Vítor Fonseca. **Panorama Mundial da Legislação de Inteligência Artificial. 2025.** Disponível em: <https://www2.camara.leg.br/a-camara/estruturaadm/secretarias/secretaria-da-inovacao-legislativa/publicacoes/panorama-mundial-da-legislacao-de-inteligencia-artificial/view>. Acesso em: 09 set. 2025.

STRYKER, Cole; KAVLAKOGLU, Eda. **O que é inteligência artificial?**. IBM. [2025?]. Disponível em: <https://www.ibm.com/br-pt/think/topics/artificial-intelligence>. Acesso em: 20 ago. 2025.

TAJRA, Alex. **Veja como cada estado brasileiro utiliza o reconhecimento facial para fins policiais.** Conjur, 17 mai. 2024. Disponível em: <https://www.conjur.com.br/2024-mai-17/veja-como-cada-estado-usa-o-reconhecimento-facial-para-fins-policiais/>. Acesso em: 05 set. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). **Jornal Oficial da União Europeia, L 2024/1689**, 12 jul. 2024. Disponível em: <http://data.europa.eu/eli/reg/2024/1689/oj>. Acesso em: 27 set. 2025.

VAZ, Millena Ferreira. A Preservação da Cadeia de Custódia como Pressuposto de Admissibilidade da Prova Digital. **Revista da ESMESC**, v. 30, n. 36, p.323-350, 2023.