v7.n7.2026

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

A UTILIZAÇÃO DE ALGORITMOS DE INTELIGÊNCIA ARTIFICIAL NA INVESTIGAÇÃO CRIMINAL

THE USE OF ARTIFICIAL INTELLIGENCE ALGORITHMS IN CRIMINAL INVESTIGATION

LA UTILIZACIÓN DE ALGORITMOS DE INTELIGENCIA ARTIFICIAL EN LA INVESTIGACIÓN CRIMINAL

Rayane Kellen Martins Marques[1]

e778325
https://doi.org/10.47820/recima21.v7i7.8325

PUBLICADO: 07/2026

RESUMO

O presente artigo analisa a utilização da inteligência artificial na investigação criminal, examinando seus impactos jurídicos, sociais e constitucionais no contexto contemporâneo. O avanço das tecnologias digitais, aliado ao desenvolvimento de algoritmos de aprendizado de máquina, sistemas de reconhecimento facial e análise massiva de dados, ampliou significativamente a capacidade estatal de monitoramento e produção de provas no âmbito da persecução penal. Nesse cenário, a pesquisa busca compreender de que forma essas tecnologias vêm sendo incorporadas aos mecanismos investigativos e quais desafios surgem em relação à proteção dos direitos e garantias fundamentais previstos na Constituição Federal de 1988. Para tanto, adotou-se o método dedutivo, mediante pesquisa qualitativa de natureza bibliográfica e documental, com análise da legislação pertinente, da doutrina especializada e de produções científicas relacionadas à inteligência artificial, ao processo penal e à proteção de dados pessoais. O estudo aborda os principais conceitos e a evolução histórica da inteligência artificial, bem como suas aplicações na atividade investigativa estatal. Além disso, examina os limites jurídicos da obtenção e utilização de provas digitais à luz da Lei Geral de Proteção de Dados e do Marco Civil da Internet. Também são analisados os riscos decorrentes da utilização indiscriminada dessas tecnologias, tais como a violação da privacidade, a vigilância em massa, os vieses algorítmicos e a reprodução de discriminações estruturais. Conclui-se que a inteligência artificial possui potencial para aumentar a eficiência investigativa e contribuir para a segurança pública, mas sua utilização exige transparência, supervisão humana e mecanismos efetivos de controle, a fim de assegurar a proteção dos direitos fundamentais no Estado Democrático de Direito.

PALAVRAS-CHAVE: Inteligência Artificial. Investigação Criminal. Reconhecimento Facial. Direitos Fundamentais. Algoritmos. Proteção de Dados.

ABSTRACT

This article analyzes the use of artificial intelligence in criminal investigations, examining its legal, social, and constitutional impacts in the contemporary context. The advancement of digital technologies, combined with the development of machine learning algorithms, facial recognition systems, and large-scale data analysis, has significantly expanded the State's capacity to monitor activities and produce evidence within criminal prosecution. In this scenario, the research seeks to understand how these technologies have been incorporated into investigative mechanisms and what challenges arise regarding the protection of fundamental rights guaranteed by the Brazilian Federal Constitution of 1988.

[1] Graduanda em Direito pelo Centro Universitário de Goiatuba – UNICERRADO.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

To this end, a deductive method was adopted through qualitative bibliographic and documentary research, including the analysis of legislation, specialized doctrine, and scientific studies related to artificial intelligence, criminal procedure, and personal data protection. The study addresses the main concepts and historical evolution of artificial intelligence, as well as its applications in criminal investigations. Furthermore, it examines the legal limits of obtaining and using digital evidence under the General Data Protection Law and the Brazilian Civil Rights Framework for the Internet. The research also discusses risks arising from the indiscriminate use of such technologies, including privacy violations, mass surveillance, algorithmic bias, and the reproduction of structural discrimination. It concludes that artificial intelligence can enhance investigative efficiency and contribute to public security; however, its use requires transparency, human oversight, and effective control mechanisms to ensure the protection of fundamental rights within a Democratic State governed by the rule of law.

KEYWORDS: *Artificial Intelligence. Criminal Investigation. Facial Recognition. Fundamental Rights. Algorithms. Data Protection.*

RESUMEN

Este artículo analiza la utilización de la inteligencia artificial en la investigación criminal, examinando sus impactos jurídicos, sociales y constitucionales en el contexto contemporáneo. El avance de las tecnologías digitales, junto con el desarrollo de algoritmos de aprendizaje automático, sistemas de reconocimiento facial y análisis masivo de datos, ha ampliado significativamente la capacidad estatal de monitoreo y producción de pruebas en el ámbito de la persecución penal. En este escenario, la investigación busca comprender cómo estas tecnologías han sido incorporadas a los mecanismos investigativos y cuáles son los desafíos relacionados con la protección de los derechos y garantías fundamentales previstos en la Constitución Federal de 1988. Para ello, se adoptó el método deductivo mediante una investigación cualitativa de carácter bibliográfico y documental, con análisis de la legislación pertinente, doctrina especializada y estudios científicos relacionados con la inteligencia artificial, el proceso penal y la protección de datos personales. El estudio aborda los principales conceptos y la evolución histórica de la inteligencia artificial, así como sus aplicaciones en la actividad investigativa estatal. Además, examina los límites jurídicos de la obtención y utilización de pruebas digitales a la luz de la Ley General de Protección de Datos y del Marco Civil de Internet. También se analizan los riesgos derivados del uso indiscriminado de estas tecnologías, tales como la vulneración de la privacidad, la vigilancia masiva, los sesgos algorítmicos y la reproducción de discriminaciones estructurales. Se concluye que la inteligencia artificial posee potencial para aumentar la eficiencia investigativa y contribuir a la seguridad pública; sin embargo, su utilización exige transparencia, supervisión humana y mecanismos efectivos de control para garantizar la protección de los derechos fundamentales en un Estado Democrático de Derecho.

PALABRAS CLAVE: *Inteligencia Artificial. Investigación Criminal. Reconocimiento Facial. Derechos Fundamentales. Algoritmos. Protección de Datos.*

INTRODUÇÃO

A evolução tecnológica observada nas últimas décadas provocou profundas transformações nas estruturas sociais, econômicas e jurídicas contemporâneas. Entre as

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

inovações que mais impactaram a sociedade destaca-se a inteligência artificial (IA), compreendida como um conjunto de tecnologias capazes de processar grandes volumes de dados, identificar padrões e executar tarefas que tradicionalmente demandavam intervenção humana. Inicialmente restrita ao campo acadêmico e científico, a IA passou a integrar diversos setores estratégicos, como saúde, educação, economia, administração pública e segurança pública.

No contexto da persecução penal, a utilização da inteligência artificial tornou-se cada vez mais frequente em razão da crescente digitalização das relações sociais e do surgimento de novas modalidades criminosas associadas ao ambiente virtual. Ferramentas como reconhecimento facial, análise preditiva, geolocalização e cruzamento automatizado de dados ampliaram significativamente a capacidade investigativa do Estado, permitindo maior eficiência na coleta, organização e análise de informações relevantes para a apuração de infrações penais.

As bases teóricas da inteligência artificial remontam aos estudos de Alan Turing (1950), que propôs a possibilidade de máquinas reproduzirem comportamentos associados à inteligência humana mediante adequada programação computacional. Desde então, os avanços tecnológicos possibilitaram o desenvolvimento de sistemas cada vez mais sofisticados, capazes de desempenhar funções complexas em diferentes áreas da atividade humana. No âmbito da investigação criminal, tais ferramentas passaram a desempenhar papel relevante na identificação de suspeitos, no monitoramento de ambientes e na análise de grandes bases de dados.

Contudo, a incorporação dessas tecnologias à atividade investigativa suscita importantes questionamentos jurídicos e constitucionais. Embora a inteligência artificial possa contribuir para o aprimoramento da segurança pública e da eficiência investigativa, seu emprego envolve riscos relacionados à privacidade, à proteção de dados pessoais, à transparência algorítmica, à presunção de inocência, ao contraditório, à ampla defesa e à dignidade da pessoa humana. Além disso, estudos apontam que sistemas automatizados podem reproduzir vieses presentes nas bases de dados utilizadas para seu treinamento, potencializando discriminações e desigualdades já existentes no sistema de justiça criminal.

Outro desafio relevante refere-se à denominada opacidade algorítmica, caracterizada pela dificuldade de compreensão dos critérios utilizados pelos sistemas de inteligência artificial na formulação de seus resultados. A ausência de transparência pode comprometer o controle jurisdicional e dificultar a fiscalização dos elementos probatórios produzidos por meio dessas tecnologias, afetando diretamente garantias processuais fundamentais.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

No Brasil, embora a transformação digital das instituições públicas tenha impulsionado a adoção de ferramentas tecnológicas por órgãos de segurança pública, Ministério Público e Poder Judiciário, ainda não existe regulamentação específica e suficientemente detalhada sobre a utilização da inteligência artificial na investigação criminal. Apesar da relevância da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e da Lei nº 12.965/2014 (Marco Civil da Internet), permanecem desafios normativos relacionados à obtenção, ao tratamento e à utilização de dados em atividades investigativas automatizadas.

Diante desse cenário, o problema de pesquisa consiste em verificar de que maneira a utilização da inteligência artificial na investigação criminal pode ser compatibilizada com os direitos e garantias fundamentais previstos na Constituição Federal de 1988. A hipótese adotada sustenta que, embora a inteligência artificial represente importante instrumento de aprimoramento das investigações criminais, sua utilização sem mecanismos adequados de transparência, supervisão humana e controle jurisdicional pode resultar em violações constitucionais relacionadas à privacidade, à presunção de inocência, ao contraditório e à dignidade da pessoa humana.

O objetivo geral deste estudo consiste em analisar os impactos jurídicos decorrentes da utilização de algoritmos de inteligência artificial na investigação criminal brasileira, verificando sua compatibilidade com os direitos fundamentais assegurados pelo ordenamento constitucional. Como objetivos específicos, busca-se compreender o funcionamento das tecnologias de inteligência artificial aplicadas à persecução penal, identificar os principais riscos decorrentes de sua utilização, examinar os limites constitucionais da atividade investigativa tecnológica, analisar a legislação aplicável ao tema e discutir mecanismos regulatórios voltados à proteção das garantias fundamentais.

Para a realização da pesquisa, adotou-se o método dedutivo, mediante abordagem qualitativa, utilizando-se pesquisa bibliográfica, legislativa e documental. O estudo fundamenta-se na análise da doutrina especializada, da legislação nacional, da jurisprudência e de produções científicas relacionadas à inteligência artificial, à investigação criminal, ao processo penal e à proteção de dados pessoais.

A relevância da pesquisa justifica-se pela crescente expansão da inteligência artificial nas atividades estatais e pela necessidade de construção de parâmetros jurídicos que permitam conciliar inovação tecnológica, eficiência investigativa e proteção dos direitos fundamentais, garantindo que a utilização dessas ferramentas ocorra em conformidade com os princípios do Estado Democrático de Direito.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

A INVESTIGAÇÃO CRIMINAL NO BRASIL

A investigação criminal consiste na atividade estatal destinada à apuração da materialidade das infrações penais e à identificação de seus possíveis autores, desempenhando papel fundamental na formação da *opinio delicti* e no desenvolvimento da persecução penal. Segundo Lopes Jr. (2024), a investigação preliminar tem por finalidade reunir elementos informativos capazes de subsidiar a atuação do Ministério Público e do Poder Judiciário, sem que isso implique antecipação de juízo condenatório. No ordenamento jurídico brasileiro, essa atividade encontra fundamento na Constituição Federal de 1988 e no Código de Processo Penal, sendo exercida predominantemente pelas polícias judiciárias por meio do inquérito policial.

O inquérito policial constitui o principal instrumento investigativo utilizado no sistema jurídico brasileiro. Trata-se de procedimento administrativo destinado à coleta de elementos informativos acerca da existência da infração penal e de sua autoria. Embora possua natureza inquisitiva e não esteja submetido ao contraditório pleno, a atividade investigativa deve observar os direitos e garantias fundamentais assegurados pela Constituição Federal, especialmente quando as medidas adotadas possam afetar a esfera jurídica do investigado.

A investigação criminal contemporânea passou por profundas transformações em decorrência da expansão das tecnologias digitais e da consolidação da denominada sociedade da informação. Conforme observa Castells (2018), a crescente circulação de dados em ambientes digitais alterou significativamente os processos de produção, armazenamento e compartilhamento de informações, ampliando as possibilidades de obtenção de elementos probatórios pelas instituições estatais. Nesse contexto, redes sociais, dispositivos móveis, bancos de dados digitais e sistemas automatizados passaram a desempenhar papel cada vez mais relevante na atividade investigativa.

A atuação investigativa do Estado, contudo, encontra limites nos direitos e garantias fundamentais previstos na Constituição Federal de 1988. Nesse sentido, Ferrajoli (2002) sustenta que o exercício do poder punitivo somente se legitima quando submetido a mecanismos jurídicos de controle capazes de assegurar a proteção das liberdades individuais. Assim, princípios como a legalidade, o devido processo legal, a proporcionalidade, a presunção de inocência e a proteção da privacidade constituem parâmetros indispensáveis para a validade das medidas investigativas adotadas no âmbito da persecução penal.

A proteção da privacidade e do sigilo das comunicações assume especial relevância diante do avanço das tecnologias de monitoramento e vigilância. A utilização de medidas investigativas invasivas, como interceptações telefônicas, acesso a dados telemáticos e

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

monitoramento digital, exige estrita observância dos requisitos legais e constitucionais, a fim de evitar restrições indevidas aos direitos fundamentais. Dessa forma, a investigação criminal deve buscar o equilíbrio entre a eficiência da atividade investigativa e a preservação das garantias individuais inerentes ao Estado Democrático de Direito.

A crescente digitalização das relações sociais ampliou significativamente a relevância das provas digitais na investigação criminal contemporânea. Conforme destaca Peck (2022), a expansão das tecnologias da informação modificou profundamente os mecanismos de produção, obtenção e preservação da prova, exigindo constante adaptação das instituições jurídicas às novas realidades tecnológicas. Nesse cenário, mensagens eletrônicas, registros de acesso, dados de geolocalização e arquivos digitais passaram a constituir importantes fontes probatórias para a persecução penal.

A utilização de provas digitais demanda cuidados específicos relacionados à preservação de sua autenticidade, integridade e confiabilidade. Nesse contexto, a cadeia de custódia assume papel fundamental na garantia da validade dos elementos probatórios obtidos em meio eletrônico, assegurando a rastreabilidade da prova desde sua coleta até sua apresentação em juízo e contribuindo para a preservação de sua credibilidade perante o sistema de justiça criminal.

Além disso, instrumentos normativos como a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) contribuíram para a consolidação de parâmetros jurídicos voltados à proteção dos direitos fundamentais no ambiente digital. Segundo Doneda (2021), o desenvolvimento de mecanismos de proteção de dados pessoais representa importante instrumento de fortalecimento das garantias individuais diante da crescente utilização de informações digitais por agentes públicos e privados. Dessa forma, a investigação criminal contemporânea deve ser conduzida em conformidade com os limites constitucionais e legais estabelecidos para a proteção da privacidade, da liberdade e da autodeterminação informativa dos cidadãos.

APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL NA INVESTIGAÇÃO CRIMINAL

Entre as principais aplicações da inteligência artificial na investigação criminal destaca-se o reconhecimento facial, tecnologia baseada na utilização de algoritmos capazes de identificar indivíduos por meio de características biométricas. O desenvolvimento desses sistemas possibilitou sua implementação em aeroportos, vias públicas, eventos de grande porte e centros

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

urbanos, ampliando significativamente a capacidade de monitoramento das instituições responsáveis pela segurança pública.

Segundo Hildebrandt (2020), a utilização de sistemas automatizados de identificação constitui uma das manifestações mais relevantes da transformação digital impulsionada pela inteligência artificial, permitindo o processamento de grandes volumes de dados em curto espaço de tempo. Entretanto, a autora adverte que tais mecanismos podem produzir impactos significativos sobre direitos fundamentais, especialmente quando empregados sem critérios adequados de transparência, supervisão e controle institucional.

A expansão das tecnologias de reconhecimento facial intensificou os debates acerca da proteção da privacidade, da igualdade e da não discriminação. Estudos desenvolvidos por instituições acadêmicas internacionais demonstraram que determinados sistemas apresentam índices de erro mais elevados quando aplicados a grupos específicos da população, especialmente mulheres e pessoas negras, evidenciando a existência de vieses algorítmicos capazes de comprometer a confiabilidade dos resultados produzidos e potencializar desigualdades já existentes.

Outra importante aplicação da inteligência artificial no âmbito da segurança pública consiste nos sistemas de policiamento preditivo. Essas ferramentas utilizam algoritmos capazes de analisar grandes volumes de dados históricos, estatísticos e geográficos com a finalidade de identificar padrões relacionados à ocorrência de delitos e orientar estratégias preventivas de atuação policial.

Conforme destacam Hildebrandt (2020) e Lyon (2007), embora tais mecanismos possam contribuir para o aumento da eficiência operacional das instituições de segurança pública, sua utilização também pode reforçar padrões históricos de seletividade e discriminação presentes nas estruturas de controle social. Isso ocorre porque os algoritmos são treinados a partir de bases de dados produzidas por práticas institucionais pretéritas, podendo reproduzir distorções e desigualdades já existentes no sistema de justiça criminal.

O avanço da inteligência artificial na investigação criminal encontra-se diretamente relacionado ao fenômeno do *big data*, caracterizado pela produção, armazenamento e processamento de grandes volumes de informações em ambientes digitais. Segundo Mayer-Schönberger e Cukier (2013), a análise massiva de dados permite identificar padrões, tendências e correlações dificilmente perceptíveis por métodos tradicionais de processamento da informação.

Nesse contexto, órgãos de segurança pública passaram a utilizar sistemas de mineração de dados capazes de processar informações provenientes de comunicações eletrônicas,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

registros financeiros, dados de geolocalização, redes sociais e outras plataformas digitais. Essas ferramentas auxiliam na identificação de vínculos entre indivíduos, movimentações suspeitas, fluxos financeiros e padrões de comportamento associados à atuação de organizações criminosas, contribuindo para o aprimoramento da atividade investigativa.

Apesar das vantagens operacionais proporcionadas por tais tecnologias, sua utilização também suscita importantes preocupações jurídicas relacionadas à privacidade, à proteção de dados pessoais e aos limites do monitoramento estatal. A integração de extensos bancos de dados amplia os riscos de coleta excessiva, tratamento inadequado e utilização indevida de informações pessoais, tornando indispensável a implementação de mecanismos efetivos de fiscalização, controle e responsabilização.

Outro desafio relevante refere-se à denominada opacidade algorítmica. Em muitos casos, os sistemas de inteligência artificial operam por meio de estruturas altamente complexas, dificultando a compreensão dos critérios utilizados para a formulação de determinadas conclusões ou recomendações. Segundo Miller (2017), a explicabilidade constitui requisito indispensável para assegurar legitimidade, transparência e confiabilidade aos sistemas inteligentes, especialmente quando empregados em atividades estatais capazes de produzir impactos diretos sobre direitos fundamentais.

No âmbito da investigação criminal, a ausência de transparência algorítmica pode comprometer o exercício do contraditório, da ampla defesa e do controle jurisdicional dos elementos informativos produzidos por sistemas automatizados. Isso porque a impossibilidade de compreender os critérios utilizados pelo algoritmo dificulta a verificação da legalidade, da precisão e da confiabilidade dos resultados obtidos durante a persecução penal.

Dessa forma, embora a inteligência artificial represente importante instrumento de modernização da investigação criminal, sua utilização deve observar os limites estabelecidos pelo ordenamento jurídico brasileiro. A adoção dessas tecnologias deve ocorrer em conformidade com os princípios constitucionais, assegurando a proteção da privacidade, o respeito ao devido processo legal, a transparência dos sistemas automatizados e a preservação das garantias fundamentais previstas na Constituição Federal de 1988.

RISCOS, LIMITES E DIREITOS FUNDAMENTAIS

O crescimento da inteligência artificial aplicada à investigação criminal promoveu profundas transformações nas atividades de segurança pública e persecução penal. A utilização de sistemas automatizados para coleta, processamento e análise de dados ampliou

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

significativamente a capacidade estatal de monitoramento, identificação de padrões e obtenção de informações relevantes para a apuração de infrações penais. Todavia, paralelamente aos avanços tecnológicos, surgiram importantes preocupações relacionadas à proteção dos direitos fundamentais e aos limites constitucionais da atuação estatal.

Segundo Doneda (2021), a proteção de dados pessoais constitui uma dimensão contemporânea do direito fundamental à privacidade, representando instrumento essencial para a proteção da liberdade individual, da autodeterminação informativa e da dignidade da pessoa humana diante do crescente tratamento automatizado de informações. Nesse contexto, a utilização indiscriminada de dados pessoais por órgãos públicos pode comprometer a autonomia dos indivíduos e ampliar riscos de violações aos direitos fundamentais assegurados constitucionalmente.

A investigação criminal contemporânea passou a empregar tecnologias capazes de rastrear deslocamentos, analisar comunicações eletrônicas, monitorar redes sociais e identificar padrões comportamentais em larga escala. Embora tais mecanismos contribuam para o aumento da eficiência investigativa, sua utilização também amplia os riscos de interferência excessiva do Estado na esfera privada dos cidadãos.

A Constituição Federal de 1988 assegura expressamente a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como protege o sigilo das comunicações e dos dados, admitindo restrições apenas nas hipóteses previstas em lei e mediante observância das garantias constitucionais. Conforme destaca Sarlet (2023), os direitos fundamentais exercem importante função de limitação do poder estatal, impedindo que a busca por maior eficiência administrativa ou investigativa resulte em restrições desproporcionais às liberdades individuais.

VIGILÂNCIA EM MASSA E PROTEÇÃO DA PRIVACIDADE

Uma das principais preocupações relacionadas à utilização da inteligência artificial na investigação criminal refere-se à ampliação dos mecanismos de vigilância estatal. Os sistemas automatizados permitem o processamento contínuo de grandes volumes de informações provenientes de diversas fontes digitais, potencializando a capacidade de monitoramento das instituições públicas.

A integração de bancos de dados, sistemas de reconhecimento facial, ferramentas de geolocalização e mecanismos de mineração de dados possibilita a construção de perfis detalhados dos indivíduos e de suas atividades cotidianas. Embora tais recursos possam auxiliar

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

na prevenção e repressão de infrações penais, sua utilização indiscriminada pode comprometer direitos fundamentais relacionados à privacidade e à autodeterminação informativa.

O debate internacional acerca dos limites da vigilância estatal ganhou relevância após a divulgação de programas de monitoramento em larga escala conduzidos por órgãos de inteligência de diversos países. Esses episódios reforçaram a necessidade de mecanismos de controle democrático e transparência capazes de assegurar a compatibilidade entre as atividades de vigilância e a proteção dos direitos fundamentais no ambiente digital.

No contexto brasileiro, a crescente utilização de sistemas de reconhecimento facial e monitoramento urbano também desperta preocupações quanto à ausência de regulamentação específica para determinadas tecnologias, circunstância que amplia os riscos de utilização abusiva e dificulta a fiscalização dos critérios empregados pelos sistemas automatizados.

Conforme leciona Virgílio Afonso da Silva (2021), qualquer restrição a direitos fundamentais deve observar os critérios da proporcionalidade, necessidade e adequação. Assim, a utilização de tecnologias de monitoramento somente se legitima quando indispensável à consecução de finalidades constitucionalmente legítimas e realizada mediante estrita observância das garantias fundamentais.

VIESES ALGORÍTMICOS E SELETIVIDADE PENAL

Outro desafio relevante refere-se ao denominado viés algorítmico. Embora frequentemente apresentados como instrumentos objetivos e neutros, os algoritmos são desenvolvidos a partir de dados produzidos em contextos sociais específicos, podendo reproduzir padrões discriminatórios historicamente existentes.

Segundo Bioni (2021), os sistemas de inteligência artificial refletem as características dos dados utilizados em seu treinamento. Dessa forma, quando as bases de dados contêm distorções históricas ou práticas discriminatórias, os resultados produzidos pelos algoritmos tendem a reproduzir e potencializar essas desigualdades.

A preocupação torna-se particularmente relevante no âmbito da investigação criminal, uma vez que a utilização de dados historicamente influenciados por práticas seletivas pode direcionar a atuação estatal de maneira desproporcional contra determinados grupos sociais. Diversos estudos internacionais demonstraram que sistemas de reconhecimento facial apresentam índices de erro mais elevados na identificação de determinados segmentos populacionais, especialmente pessoas negras e mulheres.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

No contexto brasileiro, essa problemática adquire especial relevância em razão das desigualdades estruturais presentes no sistema penal. Conforme destaca Silvio Almeida (2021), o racismo estrutural influencia o funcionamento de diversas instituições sociais, produzindo efeitos que podem ser reproduzidos por sistemas automatizados quando inexistem mecanismos adequados de auditoria e fiscalização.

A seletividade penal, conforme ensina Zaffaroni (2015), corresponde à tendência histórica de concentração da atuação repressiva sobre grupos socialmente vulneráveis. Nesse cenário, sistemas de policiamento preditivo podem reforçar ciclos de vigilância direcionados a determinadas regiões ou populações, perpetuando padrões discriminatórios e comprometendo a igualdade material assegurada pela Constituição Federal.

PRESUNÇÃO DE INOCÊNCIA E DEVIDO PROCESSO LEGAL

A presunção de inocência constitui um dos pilares fundamentais do Estado Democrático de Direito. Prevista expressamente no artigo 5º, inciso LVII, da Constituição Federal, essa garantia estabelece que ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória.

O avanço da inteligência artificial trouxe novos desafios para a preservação desse princípio, especialmente em razão da utilização de sistemas de análise preditiva e classificação de risco. Tais ferramentas produzem inferências estatísticas baseadas em padrões de comportamento, criando preocupações quanto à possibilidade de antecipação de juízos de suspeita ou culpabilidade.

Segundo Ferrajoli (2002), o garantismo penal exige rigorosa limitação do poder punitivo estatal, assegurando proteção efetiva contra arbitrariedades e presunções indevidas de culpabilidade. Nessa perspectiva, a atividade investigativa deve fundamentar-se em elementos concretos e individualizados, não podendo apoiar-se exclusivamente em probabilidades estatísticas produzidas por sistemas automatizados.

Conforme sustenta Lopes Jr. (2024), a busca por eficiência investigativa não autoriza a flexibilização das garantias processuais asseguradas ao investigado. O perfilamento criminal automatizado, quando utilizado sem critérios adequados de controle e transparência, pode resultar em processos de criminalização antecipada e reforço de estigmatizações sociais incompatíveis com o devido processo legal.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Do mesmo modo, Badaró (2023) destaca que a investigação criminal deve observar rigorosamente os direitos fundamentais do investigado, sendo incompatível com medidas baseadas exclusivamente em suspeições genéricas ou probabilidades matemáticas desvinculadas de elementos concretos de prova.

RESPONSABILIDADE CIVIL DO ESTADO E CONTROLE DA INTELIGÊNCIA ARTIFICIAL

A utilização da inteligência artificial na investigação criminal também suscita discussões acerca da responsabilidade civil do Estado diante de falhas tecnológicas e erros algorítmicos. A Constituição Federal estabelece a responsabilidade objetiva estatal pelos danos causados por seus agentes, assegurando proteção aos indivíduos prejudicados por atuações administrativas ilegítimas.

Segundo Celso Antônio Bandeira de Mello (2023), a responsabilidade civil do Estado decorre da obrigação jurídica de reparar prejuízos causados por atividades administrativas que resultem em lesão a direitos individuais. Nesse contexto, erros decorrentes da utilização inadequada de sistemas de inteligência artificial podem gerar o dever de indenização quando ocasionarem danos aos cidadãos.

Tais falhas podem decorrer de erros técnicos, utilização de bancos de dados incorretos, vieses algorítmicos ou interpretações equivocadas produzidas pelos sistemas automatizados. Quando esses fatores resultam em abordagens indevidas, constrangimentos ilegais ou outras formas de violação de direitos, surge a obrigação estatal de reparar os prejuízos causados.

Conforme leciona Di Pietro (2023), a responsabilidade civil constitui importante instrumento de proteção dos administrados contra abusos e irregularidades praticados no exercício da função pública. Nesse sentido, mecanismos de responsabilização contribuem para o fortalecimento do controle democrático sobre a utilização de tecnologias inteligentes pelo Poder Público.

Além disso, a Resolução nº 332/2020 do Conselho Nacional de Justiça estabeleceu diretrizes para a utilização ética, transparente e responsável da inteligência artificial no âmbito do Poder Judiciário, destacando princípios como transparência, supervisão humana, não discriminação e respeito aos direitos fundamentais.

Dessa forma, embora a inteligência artificial apresente elevado potencial para modernizar a investigação criminal e ampliar a eficiência das instituições responsáveis pela persecução penal, sua utilização deve ocorrer em estrita observância aos limites constitucionais. Somente por meio da conjugação entre inovação tecnológica, controle democrático e proteção

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

dos direitos fundamentais será possível assegurar que essas ferramentas contribuam para o fortalecimento da justiça criminal sem comprometer os valores essenciais do Estado Democrático de Direito.

REGULAMENTAÇÃO E PERSPECTIVAS FUTURAS

O avanço da inteligência artificial nas últimas décadas provocou profundas transformações nas relações sociais, econômicas e institucionais, especialmente no âmbito da atuação estatal. A crescente utilização de algoritmos em atividades relacionadas à segurança pública e à investigação criminal passou a exigir reflexão jurídica mais aprofundada acerca dos limites constitucionais da tecnologia e da necessidade de regulamentação específica capaz de assegurar a proteção dos direitos fundamentais. Embora o ordenamento jurídico brasileiro já disponha de normas relacionadas à proteção de dados e ao ambiente digital, ainda não existe legislação abrangente e definitiva voltada exclusivamente à disciplina da inteligência artificial, circunstância que mantém relevantes debates no campo jurídico.

A Constituição Federal de 1988 estabelece diversos princípios que funcionam como limites à atuação tecnológica do Estado, especialmente os direitos à privacidade, à intimidade, à dignidade da pessoa humana, ao devido processo legal e à presunção de inocência. Assim, mesmo diante da ausência de regulamentação específica sobre inteligência artificial aplicada à investigação criminal, a utilização dessas tecnologias permanece condicionada à observância dos parâmetros constitucionais.

A REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO BRASIL

Sarlet (2023) afirma que o desenvolvimento tecnológico não pode resultar na flexibilização das garantias fundamentais, especialmente quando o poder público passa a utilizar instrumentos capazes de ampliar significativamente sua capacidade de controle social. Segundo o autor, a modernização administrativa e tecnológica deve ocorrer em consonância com os princípios democráticos e com a proteção das liberdades individuais.

Nesse contexto, destaca-se a importância da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), considerada atualmente o principal instrumento normativo brasileiro relacionado ao tratamento automatizado de informações pessoais. A legislação estabeleceu princípios fundamentais para a utilização de dados pessoais, dentre eles finalidade, adequação, necessidade, transparência, segurança e responsabilização. Embora não trate especificamente

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

da inteligência artificial, possui grande relevância para o tema, uma vez que os sistemas algorítmicos dependem diretamente da coleta e do processamento de dados pessoais.

A LGPD também introduziu importante mecanismo de proteção relacionado às decisões automatizadas. O artigo 20 assegura ao titular dos dados o direito de solicitar revisão de decisões tomadas exclusivamente com base em tratamento automatizado de dados pessoais, previsão que assume especial relevância diante da crescente utilização de sistemas inteligentes capazes de identificar suspeitos, mapear padrões comportamentais e classificar indivíduos por meio de grandes bases de dados.

Além da LGPD, merece destaque o Projeto de Lei nº 2.338/2023, atualmente em tramitação no Congresso Nacional, que busca estabelecer princípios, diretrizes e mecanismos de governança para o desenvolvimento e a utilização da inteligência artificial no Brasil. Inspirado em modelos regulatórios internacionais, especialmente na experiência europeia, o projeto adota abordagem baseada na classificação de riscos, impondo controles mais rigorosos para sistemas considerados de alto risco, incluindo aqueles empregados em segurança pública e investigação criminal.

Também merece destaque a Resolução nº 332/2020 do Conselho Nacional de Justiça, que estabelece diretrizes éticas para o uso da inteligência artificial no âmbito do Poder Judiciário, enfatizando princípios como transparência, supervisão humana, segurança, igualdade e não discriminação.

EXPERIÊNCIAS INTERNACIONAIS DE REGULAMENTAÇÃO

A discussão internacional acerca da regulamentação da inteligência artificial intensificou-se nos últimos anos em razão da expansão acelerada das tecnologias algorítmicas e de seus potenciais impactos sobre os direitos fundamentais. Nesse cenário, diferentes modelos regulatórios foram desenvolvidos por Estados e organismos internacionais, refletindo distintas concepções acerca da relação entre tecnologia, liberdade e poder estatal.

A União Europeia consolidou-se como uma das principais referências mundiais em regulamentação digital. Após a implementação do Regulamento Geral de Proteção de Dados (GDPR), o bloco avançou na construção de normas específicas para inteligência artificial, culminando na aprovação do *AI Act*. O regulamento europeu adota sistema baseado na análise de riscos, classificando determinadas tecnologias como reconhecimento facial, monitoramento biométrico e policiamento preditivo como sistemas de alto risco, sujeitos a rigorosos mecanismos de controle, transparência e supervisão humana.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Nos Estados Unidos, por outro lado, prevalece modelo regulatório mais descentralizado e flexível, caracterizado pela ausência de legislação federal abrangente sobre inteligência artificial. Apesar disso, o emprego de sistemas algorítmicos por órgãos de segurança pública tem sido alvo de críticas relacionadas à reprodução de discriminações raciais e à ocorrência de erros em tecnologias de reconhecimento facial.

Em sentido diverso, a China desenvolveu um dos modelos mais amplos de vigilância tecnológica contemporânea, utilizando sistemas de reconhecimento facial, monitoramento digital e rastreamento populacional em larga escala. Tal modelo tem sido objeto de críticas por organismos internacionais de direitos humanos, especialmente em razão dos potenciais impactos sobre a privacidade, a liberdade individual e a autonomia dos cidadãos.

PERSPECTIVAS FUTURAS E MECANISMOS DE CONTROLE

A utilização legítima da inteligência artificial na investigação criminal exige a criação de mecanismos jurídicos capazes de assegurar compatibilidade entre inovação tecnológica e proteção dos direitos fundamentais. Embora os sistemas algorítmicos possam contribuir para a eficiência investigativa, sua utilização indiscriminada representa riscos significativos à privacidade, à igualdade, ao contraditório e ao devido processo legal.

Entre os principais mecanismos defendidos pela doutrina contemporânea destaca-se a supervisão humana obrigatória sobre decisões automatizadas. Nessa perspectiva, a inteligência artificial deve atuar como instrumento auxiliar da atividade investigativa, sem substituir integralmente a análise humana em procedimentos capazes de afetar direitos individuais.

Outro elemento fundamental refere-se à transparência algorítmica. Sistemas utilizados pelo poder público devem ser auditáveis, verificáveis e passíveis de controle jurisdicional, permitindo a identificação de falhas, vieses discriminatórios e eventuais violações de direitos fundamentais.

Nesse contexto, ganha relevância a auditoria algorítmica, instrumento destinado à avaliação periódica dos sistemas de inteligência artificial, com o objetivo de assegurar conformidade técnica, legal e constitucional. Paralelamente, torna-se indispensável a capacitação contínua dos agentes públicos responsáveis pela utilização dessas ferramentas, garantindo compreensão adequada de seus limites e potencialidades.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

A Recomendação sobre a Ética da Inteligência Artificial, publicada pela UNESCO em 2021, reforça a necessidade de observância dos direitos humanos, da proporcionalidade, da diversidade, da não discriminação e da supervisão humana na implementação de sistemas inteligentes.

Dessa forma, a construção de um modelo regulatório equilibrado exige a conjugação entre regulamentação adequada, transparência, auditoria, supervisão humana e respeito aos limites constitucionais. Somente mediante a adoção desses mecanismos será possível compatibilizar o desenvolvimento tecnológico com a preservação das garantias fundamentais que caracterizam o Estado Democrático de Direito.

CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objetivo analisar os impactos jurídicos decorrentes da utilização da inteligência artificial na investigação criminal, examinando sua compatibilidade com os direitos e garantias fundamentais assegurados pela Constituição Federal de 1988. Para tanto, foram estudadas as principais aplicações dessas tecnologias no âmbito da persecução penal, os riscos associados à sua utilização e os desafios regulatórios decorrentes da crescente incorporação de sistemas algorítmicos às atividades de segurança pública.

Inicialmente, verificou-se que a inteligência artificial passou a desempenhar papel cada vez mais relevante na investigação criminal contemporânea, especialmente em razão de sua capacidade de processar grandes volumes de dados, identificar padrões de comportamento, realizar reconhecimento facial e auxiliar na análise de informações complexas. Nesse contexto, tais tecnologias apresentam potencial significativo para aumentar a eficiência investigativa e contribuir para o aprimoramento das atividades estatais voltadas à prevenção e repressão de infrações penais.

Todavia, a pesquisa demonstrou que a utilização dessas ferramentas também suscita importantes preocupações jurídicas e constitucionais. A ampliação da capacidade de monitoramento estatal, o emprego de sistemas de reconhecimento facial, a utilização de mecanismos de policiamento preditivo e o tratamento massivo de dados pessoais evidenciam riscos relacionados à privacidade, à proteção de dados, à igualdade, à presunção de inocência e ao devido processo legal.

A hipótese formulada foi confirmada. Constatou-se que a inteligência artificial pode constituir importante instrumento de apoio à investigação criminal, desde que sua utilização ocorra dentro de limites jurídicos rigorosos e sob mecanismos efetivos de fiscalização,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

transparência e controle. Em sentido contrário, a ausência de regulamentação adequada e de supervisão humana pode favorecer a reprodução de vieses discriminatórios, o fortalecimento da seletividade penal e a ocorrência de violações aos direitos fundamentais.

Os estudos analisados demonstraram que sistemas algorítmicos não são instrumentos neutros, uma vez que seus resultados dependem diretamente da qualidade e das características dos dados utilizados em seu treinamento. Dessa forma, falhas técnicas, vieses estatísticos e distorções históricas presentes nas bases de dados podem produzir resultados discriminatórios, comprometendo a confiabilidade das tecnologias empregadas na investigação criminal.

Também se verificou que o ordenamento jurídico brasileiro ainda apresenta lacunas normativas quanto à utilização da inteligência artificial em atividades de segurança pública e persecução penal. Embora a Lei Geral de Proteção de Dados represente importante avanço na tutela dos direitos relacionados ao tratamento de informações pessoais, permanece necessária a construção de disciplina normativa mais específica para regular o emprego de sistemas algorítmicos pelo poder público.

Nesse cenário, destacam-se as discussões legislativas em torno do Projeto de Lei nº 2.338/2023, bem como as experiências internacionais desenvolvidas por diferentes ordenamentos jurídicos, especialmente pela União Europeia, que tem adotado modelos regulatórios fundamentados na classificação de riscos, na transparência algorítmica e na proteção dos direitos fundamentais.

Diante desse panorama, conclui-se que a utilização legítima da inteligência artificial na investigação criminal exige a observância dos princípios da proporcionalidade, necessidade, transparência, supervisão humana e controle jurisdicional. Além disso, revela-se indispensável a implementação de mecanismos de auditoria algorítmica, fiscalização institucional e capacitação técnica dos agentes públicos responsáveis pela utilização dessas ferramentas.

Por fim, conclui-se que a inteligência artificial não deve ser compreendida como tecnologia incompatível com o processo penal democrático, mas como instrumento que demanda utilização responsável, regulamentada e constitucionalmente limitada. O desafio contemporâneo consiste em compatibilizar inovação tecnológica e proteção dos direitos fundamentais, assegurando que o desenvolvimento dessas ferramentas contribua para o fortalecimento da justiça criminal sem comprometer os valores que sustentam o Estado Democrático de Direito.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REFERÊNCIAS

ALMEIDA, Silvio Luiz de. *Racismo estrutural*. São Paulo: Jandaíra, 2021.

BADARÓ, Gustavo Henrique Righi Ivahy. *Processo penal*. 11. ed. São Paulo: Thomson Reuters Brasil, 2023.

BANDEIRA DE MELLO, Celso Antônio. Curso de direito administrativo. 36. ed. São Paulo: Malheiros, 2023.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2021.

BRASIL. Conselho Nacional de Justiça. *Resolução nº 332, de 21 de agosto de 2020*. Dispõe sobre ética, transparência e governança na produção e no uso de inteligência artificial no Poder Judiciário. Brasília, DF: CNJ, 2020. Disponível em: https://atos.cnj.jus.br. Acesso em: 12 fev. 2026.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br. Acesso em: 12 fev. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 mar. 2026.

BRASIL. Senado Federal. *Projeto de Lei nº 2.338/2023*. Dispõe sobre o uso da Inteligência Artificial no Brasil. Brasília, DF: Senado Federal, 2023. Disponível em: https://www25.senado.leg.br. Acesso em: 16 mar. 2026.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 2018.

DI PIETRO, Maria Sylvia Zanella. *Direito administrativo*. 36. ed. Rio de Janeiro: Forense, 2023.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados*. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

FERRAJOLI, Luigi. *Direito e razão: teoria do garantismo penal*. 6. ed. São Paulo: Revista dos Tribunais, 2002.

HILDEBRANDT, Mireille. *Law for computer scientists and other folk*. Oxford: Oxford University Press, 2020.

LOPES JR., Aury. *Direito processual penal*. 21. ed. São Paulo: SaraivaJur, 2024.

LYON, David. *Surveillance studies: an overview*. Cambridge: Polity Press, 2007.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data: a revolution that will transform how we live, work and think*. London: John Murray, 2013.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

MILLER, Tim. Explanation in artificial intelligence: insights from the social sciences. [S.l.], 2017. Disponível em: https://arxiv.org/abs/1706.07269. Acesso em: 7 abr. 2026.

PECK, Patrícia. *Direito digital*. 7. ed. São Paulo: Saraiva, 2022.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 14. ed. Porto Alegre: Livraria do Advogado, 2023.

SILVA, Virgílio Afonso da. *Direitos fundamentais: conteúdo essencial, restrições e eficácia*. 3. ed. São Paulo: Malheiros, 2021.

TURING, Alan. Computing machinery and intelligence. *Mind*, Oxford, v. 59, n. 236, p. 433-460, 1950.

UNESCO. *Recommendation on the ethics of artificial intelligence*. Paris: UNESCO, 2021. Disponível em: https://unesdoc.unesco.org. Acesso em: 18 maio 2026.

ZAFFARONI, Eugenio Raúl. *Em busca das penas perdidas: a perda de legitimidade do sistema penal*. 5. ed. Rio de Janeiro: Revan, 2015.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.