REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

O USO DA INTELIGÊNCIA ARTIFICIAL EM INVESTIGAÇÃO CRIMINAL: A POTENCIALIDADE PROBATÓRIA VERSUS GARANTIAS FUNDAMENTAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

THE USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATION: ITS EVIDENTIARY POTENTIAL VERSUS FUNDAMENTAL GUARANTEES IN THE BRAZILIAN LEGAL SYSTEM

Ciências Sociais Aplicadas • 19/11/2026

REGISTRO DOI: 10.70773/revistatopicos/794843913

Hilbert Paulino da Silva Santos[1]

Matheus Brito Carvalho[2]

Antônio Walter Gadelha Guimarães[3]

RESUMO

A Inteligência Artificial (IA) tem promovido transformações significativas no Direito e no Poder Judiciário. Seu uso na investigação criminal amplia as possibilidades de análise de dados e de modernização da persecução penal, No entanto, sua utilização suscita questionamentos acerca dos limites éticos e jurídicos da atuação estatal. Assim, o presente Artigo tem como objetivo geral analisar as diretrizes para a validade jurídica e os limites éticos do uso da IA na persecução penal, buscando-se a verificar se a eficiência investigativa justifica eventuais restrições aos direitos fundamentais do investigado. Busca-se também, a viabilidade jurídica e ética da criação de uma ferramenta de IA própria do Estado para as forças policiais brasileiras. Metodologicamente, o estudo caracteriza-se como uma pesquisa de natureza qualitativa, com objetivos exploratórios e descritivos, dentro da pesquisa, considera-se no ordenamento jurídico brasileiro, especialmente a Constituição Federal de 1988 e a Lei Geral de Proteção de Dados Pessoais (LGPD), e fundamenta-se nas contribuições doutrinárias de Aury Lopes Jr. e Gustavo Henrique Badaró. Prefacialmente, são examinadas as principais tecnologias de IA empregadas na persecução penal, com destaque para o policiamento preditivo e os riscos decorrentes dos vieses algorítmicos, em seguida, discute-se a ausência de neutralidade tecnológica, a seletividade penal e o racismo algorítmico. A pesquisa aborda, ainda, a admissibilidade da prova digital, a integridade dos dados e a cadeia de custódia, analisa-se também a relação entre a produção probatória por IA e o princípio da não autoincriminação. Ao final, pretende-se identificar parâmetros jurídicos e éticos para uma utilização responsável dessas tecnologias. Defende-se, como hipótese, a regulamentação técnica e a implementação de uma IA estatal destinada ao apoio operacional das investigações, sem substituir o juízo de valor dos

investigadores e dos agentes policiais, preservando-se o devido processo legal e as garantias fundamentais.
Palavras-chave: Inteligência Artificial; Processo Penal; Direito Constitucional.

ABSTRACT

Artificial Intelligence (AI) has promoted significant transformations in Law and the Judiciary, its use in criminal investigation expands the possibilities of data analysis and modernization of criminal prosecution. However, its use raises questions about the ethical and legal limits of state action. Thus, this article aims to analyze the guidelines for the legal validity and ethical limits of the use of AI in criminal prosecution, seeking to verify whether investigative efficiency justifies any restrictions on the fundamental rights of the investigated party. It also seeks the legal and ethical viability of creating a state-owned AI tool for the Brazilian police forces. Methodologically, the study is characterized as qualitative research, with exploratory and descriptive objectives. Within the research, the Brazilian legal system is considered, especially the 1988 Federal Constitution and the General Data Protection Law (LGPD), and it is based on the doctrinal contributions of Aury Lopes Jr. and Gustavo Henrique Badaró. Initially, the main AI technologies employed in criminal prosecution are examined, with emphasis on predictive policing and the risks arising from algorithmic biases. Then, the lack of technological neutrality, criminal selectivity, and algorithmic racism are discussed. The research also addresses the admissibility of digital evidence, data integrity, and the chain of custody, and analyzes the relationship between AI-powered evidence production and the principle against self-incrimination. Finally, the aim is to identify legal and ethical parameters for the responsible use of these technologies. As a hypothesis, the technical regulation and

implementation of a state AI intended to support the operational aspects of investigations is advocated, without replacing the value judgment of investigators and police officers, while preserving due process and fundamental guarantees.
Keywords: Artificial Intelligence; Criminal Procedure; Constitutional Law.

1. INTRODUÇÃO

A crescente utilização da Inteligência Artificial no sistema de justiça criminal promove transformações profundas na investigação e persecução penal, exigindo mecanismos automatizados para a análise massiva de dados e otimização das atividades policiais. Contudo, esse avanço tecnológico gera dilemas éticos e jurídicos ao tensionar limites constitucionais voltados à garantia das liberdades individuais. Diante dessa modernização, o estudo busca responder: qual o caminho a se seguir na utilização da Inteligência Artificial nas investigações criminais brasileiras sem comprometer princípios e garantias constitucionais, como o devido processo legal e a não autoincriminação?

Para responder a essa questão, a pesquisa tem como objetivo geral analisar as diretrizes e limites ético-jurídicos do uso de ferramentas de IA na persecução penal, verificando se a busca por eficiência investigativa justifica a mitigação de direitos do investigado, bem como a viabilidade de uma tecnologia própria e estatal. O estudo justifica-se nos âmbitos pessoal, social e científico diante do uso irreversível dessas ferramentas no Direito, da defasagem normativa processual e da necessidade de resguardar o cidadão contra vieses e opacidades algorítmicas, propondo um modelo público de código auditável centrado na soberania tecnológica.

Metodologicamente, trata-se de um estudo aplicado e de abordagem qualitativa, classificado como exploratório e descritivo. Utiliza-se o método hipotético-dedutivo aliado à hermenêutica constitucional, fundamentando-se em pesquisa bibliográfica e documental a partir da análise da Constituição Federal, da Lei Geral de Proteção de Dados, do Código de Processo Penal e de aportes da doutrina garantista.

O trabalho está estruturado em três seções principais. A primeira mapeia as tecnologias de IA na persecução penal, examinando seus reflexos e o risco do viés algorítmico. A segunda aborda os limites éticos da predição, analisando a seletividade penal, o racismo algorítmico e os riscos do Direito Penal do Inimigo. A terceira e última seção analisa a prova digital, a cadeia de custódia, a não autoincriminação, a crítica aos modelos opacos e a viabilidade jurídica e de governança de dados para uma Inteligência Artificial pública.

2. ANÁLISE DAS TECNOLOGIAS DE IA NA PERSECUÇÃO PENAL

A presente seção tem como objetivo mapear e analisar o uso de ferramentas de Inteligência Artificial no processo e na persecução penal, examinando de que maneira tecnologias como o reconhecimento facial e o policiamento preditivo são incorporadas pelas instituições de segurança pública. Além de evidenciar o impacto desses recursos na modernização investigativa, o capítulo busca formular políticas e diretrizes metodológicas voltadas a mitigar os riscos de estereótipos, opacidade algorítmica e preconceitos estruturais, assegurando que o avanço tecnológico permaneça estritamente subordinado aos limites éticos e normativos do Estado Democrático de Direito.

2.1. Inteligência Artificial e a Modernização da Persecução Penal

A evolução tecnológica das últimas décadas promoveu profundas transformações nas estruturas sociais, econômicas e institucionais, repercutindo diretamente no sistema de justiça criminal. Nesse contexto, a Inteligência Artificial (IA) surge como uma ferramenta capaz de modernizar a persecução penal, especialmente no âmbito da investigação criminal, da produção probatória e da gestão processual. A utilização de algoritmos, sistemas de reconhecimento facial, análise preditiva e cruzamento automatizado de dados demonstra o avanço de mecanismos tecnológicos voltados ao aumento da eficiência estatal no combate à criminalidade. Entretanto, embora a implementação dessas tecnologias apresenta benefícios significativos, também levanta importantes debates acerca da preservação dos direitos fundamentais e das garantias processuais no Estado Democrático de Direito.

A Inteligência Artificial pode ser compreendida como um conjunto de sistemas computacionais desenvolvidos para simular capacidades cognitivas humanas, como aprendizado, raciocínio lógico, reconhecimento de padrões e tomada de decisões. Conforme apontam Piló e Brasil (2022), a IA vem sendo incorporada progressivamente ao Poder Judiciário e às instituições de persecução penal, sobretudo em razão da elevada carga de trabalho e da necessidade de maior celeridade na tramitação processual. Segundo os autores, o ambiente jurídico tornou-se fértil para a implementação de soluções tecnológicas, especialmente em atividades repetitivas e de análise massiva de dados.

No âmbito da persecução penal, a IA é utilizada principalmente como instrumento auxiliar na investigação criminal. Ferramentas de

reconhecimento facial, mineração de dados, análise de padrões comportamentais e cruzamento de informações digitais possibilitam a identificação mais rápida de suspeitos e a elucidação de crimes complexos. De acordo com Costa e Feller (2025), os algoritmos inteligentes são capazes de analisar grandes volumes de informações em curto espaço de tempo, identificando conexões que muitas vezes não seriam perceptíveis pela análise humana convencional. Dessa forma, a tecnologia contribui para a otimização dos recursos da polícia judiciária, reduzindo a morosidade investigativa e aumentando a eficiência operacional das instituições de segurança pública.

Além disso, a utilização da Inteligência Artificial demonstra relevante potencial no gerenciamento de provas digitais. Com a crescente digitalização das relações sociais, os meios de obtenção probatória passaram a envolver dados eletrônicos, comunicações virtuais, arquivos em nuvem, registros telefônicos e informações extraídas de dispositivos tecnológicos. Nesse cenário, a IA possibilita a organização, filtragem e análise automatizada de grandes quantidades de evidências digitais, auxiliando autoridades policiais e órgãos judiciais na construção do conjunto probatório. Conforme destacado por Souza (2024), a aplicação da IA no processo penal representa uma importante ferramenta para modernização investigativa, especialmente diante da complexidade dos crimes contemporâneos e da expansão da criminalidade digital.

Entretanto, embora os benefícios tecnológicos sejam evidentes, a expansão da IA na persecução penal também suscita relevantes preocupações jurídicas e constitucionais. Um dos principais problemas apontados pela doutrina refere-se ao risco de violação de direitos fundamentais, especialmente a privacidade, a intimidade e o

devido processo legal. O uso indiscriminado de sistemas de vigilância algorítmica e reconhecimento facial pode resultar em monitoramento excessivo da população, ampliando o poder de controle estatal sobre os indivíduos. Nesse sentido, Piló e Brasil (2022) afirmam que a expansão da intervenção estatal mediada por tecnologias inteligentes pode comprometer garantias processuais fundamentais e atingir diretamente a dignidade da pessoa humana.

Outro ponto amplamente debatido refere-se ao chamado viés algorítmico. Os sistemas de Inteligência Artificial operam a partir de bancos de dados e padrões estatísticos previamente alimentados, de modo que eventuais distorções sociais, raciais ou econômicas existentes nesses dados podem ser reproduzidas automaticamente pelos algoritmos. Assim, decisões automatizadas podem gerar discriminações indevidas, afetando especialmente grupos socialmente vulneráveis. Conforme ressaltado no estudo acerca da Portaria MJSP nº 961/2025, a ausência de mecanismos eficazes de auditoria algorítmica e transparência tecnológica pode aprofundar desigualdades e comprometer a legitimidade da persecução penal (Renz; Anschau; Zanatta, 2025).

Ademais, a utilização da IA no processo penal exige atenção quanto à licitude das provas obtidas por meios tecnológicos. O artigo 157 do Código de Processo Penal estabelece a inadmissibilidade das provas ilícitas, especialmente aquelas produzidas mediante violação de direitos fundamentais. Assim, ainda que a tecnologia proporciona maior eficiência investigativa, sua utilização não pode ultrapassar os limites constitucionais impostos pelo ordenamento jurídico brasileiro. A busca pela eficiência não pode justificar a flexibilização de garantias fundamentais, sob pena de comprometimento do próprio Estado Democrático de Direito.

Dessa maneira, observa-se que a Inteligência Artificial possui significativo potencial para modernizar a persecução penal brasileira, oferecendo maior eficiência, agilidade e capacidade analítica às investigações criminais e ao sistema de justiça. Contudo, sua implementação deve ocorrer de forma cautelosa, equilibrando inovação tecnológica e proteção dos direitos fundamentais. A ausência de regulamentação específica, fiscalização adequada e mecanismos de transparência podem transformar ferramentas úteis em instrumentos de vigilância abusiva e restrição de garantias constitucionais. Portanto, a modernização tecnológica da persecução penal deve necessariamente estar subordinada aos princípios constitucionais da legalidade, proporcionalidade, dignidade da pessoa humana e devido processo legal, assegurando que o avanço tecnológico sirva à justiça sem comprometer as liberdades individuais.

2.2. O Policiamento Preditivo e o Risco do Viés Algorítmico

Uma das principais aplicações da IA na investigação criminal é o sistema de análise de dados. Por meio de técnicas como *machine learning*, entendido como um ramo da IA que permite o aprendizado a partir de dados para que se torne possível a realização de previsões ou decisões automáticas sem uma programação explícita, é possível examinar grandes volumes de informações provenientes de diversas fontes, como registros telefônicos, movimentação bancárias e dados extraídos de dispositivos eletrônicos.

Um ponto que deve ser destacado para a presente análise reside no policiamento preditivo. Essas ferramentas que fazem uso de dados antigos e históricos para indicação de de locais com maior

probabilidade de ocorrência de crimes podem, de forma paradoxal, institucionalizar o que a Criminologia Crítica denomina de seletividade penal. Em que, ao caso dos dados inseridos no sistema refletem um histórico de que determinadas zonas ou etnias enviesados de policiamento mais forte, a Inteligência Artificial tenderá a reproduzir e amplificar esses preconceitos.

Nesse sentido, Pereira e Oliveira (2024) advertem que o "viés algorítmico" não é uma falha técnica, mas muitas vezes um reflexo da base de dados utilizada. Para o direito Penal Garantista, o atual utilizado no sistema brasileiro, para aceitar uma prova ou uma suspeita baseada em um algoritmo apaco, acaba por ferir os princípios que regem a Constituição Federal e o Código de Processo Penal, especialmente o princípio da presunção de inocência, uma vez que a carga probatória passa a ser fundamentada em uma probabilidade calculada em estatística, e não em indícios concretos de autoridade e materialidade.

Ademais segundo Doneda e Almeida (2016) na revista *“o que é a governança de algoritmos?”* O uso de grandes bases de dados no contexto jurídico redefine a forma como decisões são tomadas, deslocando o foco da análise individual para padrões estatísticos e probabilísticos. Porém sob a perspectiva processual penal é necessário cautela na utilização desses mecanismos pois conforme destaca Badaró (2021), a obtenção e análise de provas devem respeitar rigorosamente os limites legais e constitucionais, sob pena de nulidade e violação de direitos fundamentais.

Outra tecnologia amplamente utilizada é o reconhecimento facial, que se baseia em algoritmos capazes de comparar imagens capturadas em tempo real com bancos de dados previamente

armazenados, no âmbito da persecução penal essa ferramenta tem sido aplicada na identificação de suspeitos e na localização de foragidos. Contudo essa utilização levanta preocupações relevantes quanto à precisão do sistema e a possibilidade de identificação equivocada, até porque sistemas automatizados podem operar como verdadeiras “caixas pretas” o que se torna problemático, pois a prova no processo penal deve ser submetida ao contraditório e à ampla defesa.

Por fim, se destaca os sistemas de vigilância inteligente, que integram câmeras, sensores e algoritmos de IA para monitoramento contínuo de ambientes, sendo capazes assim de detectar comportamentos considerados suspeitos. Dessa forma o mapeamento das tecnologias na persecução penal deixa evidente não apenas o potencial de aprimoramento da atividade investigativa, mas também a necessidade de compatibilização com as garantias processuais penais, de modo que a eficiência não se sobreponha aos direitos fundamentais devendo o seu uso ser rigorosamente controlado.

3. OS LIMITES ÉTICOS DA PREDIÇÃO

A presente seção tem como objetivo contextualizar e explicar os profundos riscos decorrentes do uso irresponsável e genérico da Inteligência Artificial na investigação e persecução criminal. Para tanto, o capítulo analisa criticamente como a aplicação de lógicas preditivas pode instrumentalizar de forma drástica a teoria do direito penal do inimigo, convertendo a atividade investigativa em um processo enviesado que enxerga o cidadão sob a ótica de inimigo do Estado, em nítida afronta às garantias constitucionais e ao modelo garantista de direito.

O avanço da Inteligência Artificial no âmbito da segurança pública e da persecução penal possibilitou o desenvolvimento de sistemas capazes de realizar análises preditivas sobre comportamentos humanos, padrões criminais e riscos de reincidência. A denominada "predição criminal" consiste na utilização de algoritmos alimentados por grandes bancos de dados para identificar tendências delitivas, mapear regiões com maior incidência de crimes e até mesmo indicar indivíduos considerados potencialmente perigosos. Embora tais mecanismos sejam frequentemente apresentados como instrumentos de modernização e eficiência investigativa, sua utilização levanta profundas questões éticas, jurídicas e sociais relacionadas aos limites da atuação estatal em um Estado Democrático de Direito (PILO E BRASIL. 2022).

A principal promessa da predição algorítmica é a capacidade de antecipar comportamentos criminosos e otimizar a atuação das instituições de segurança pública. Por meio do cruzamento automatizado de informações, os sistemas de Inteligência Artificial conseguem identificar padrões estatísticos e fornecer respostas rápidas às autoridades responsáveis pela investigação criminal. Nesse contexto, a tecnologia surge como ferramenta de apoio à prevenção de delitos, à distribuição estratégica de recursos policiais e à redução da criminalidade. Todavia, o problema ético central reside justamente na tentativa de transformar probabilidades estatísticas em fundamentos legítimos para vigilância, suspeição ou intervenção estatal.

A lógica preditiva desloca o foco tradicional do Direito Penal, baseado na responsabilização por fatos concretamente praticados, para uma perspectiva fundada em probabilidades futuras de comportamento. Em outras palavras, deixa-se de atuar

exclusivamente sobre condutas efetivamente realizadas para admitir intervenções baseadas em estimativas algorítmicas de risco. Esse fenômeno aproxima-se da ideia de um “Direito Penal preventivo”, no qual indivíduos passam a ser monitorados não pelo que fizeram, mas pelo que supostamente poderiam vir a fazer. Tal perspectiva representa significativo risco às garantias constitucionais, especialmente aos princípios da presunção de inocência, da dignidade da pessoa humana e do devido processo legal.

Além disso, os sistemas de predição criminal operam a partir de dados previamente coletados e organizados por instituições estatais. Isso significa que os algoritmos reproduzem padrões históricos presentes nos bancos de dados utilizados em seu treinamento. Dessa forma, se o sistema penal já apresenta distorções estruturais, desigualdades sociais e seletividade repressiva, a Inteligência Artificial tende a replicar essas mesmas distorções em escala automatizada. Conforme apontam os estudos sobre IA e persecução penal, a tecnologia não atua de forma isolada ou neutra, mas condicionada pelas informações humanas que alimentam seus mecanismos de funcionamento (Renz; Anschau; Zanatta, 2025).

Outro aspecto ético relevante refere-se à opacidade algorítmica. Muitos sistemas utilizados na segurança pública funcionam como verdadeiras “caixas-pretas”, impossibilitando que operadores do Direito, investigados e até mesmo autoridades compreendam integralmente os critérios utilizados pela Inteligência Artificial para produzir determinadas conclusões. Essa ausência de transparência compromete diretamente o contraditório e a ampla defesa, uma vez que o indivíduo submetido à persecução penal muitas vezes não possui meios adequados para questionar tecnicamente os resultados produzidos pelo sistema automatizado.

A utilização indiscriminada de mecanismos preditivos também amplia o risco de vigilância massiva da população. O monitoramento constante de dados pessoais, deslocamentos, interações digitais e comportamentos cotidianos pode transformar a tecnologia em instrumento de controle social excessivo, incompatível com as liberdades civis asseguradas constitucionalmente. Nesse cenário, o combate à criminalidade não pode servir como justificativa para relativização permanente de direitos fundamentais, sobretudo porque a eficiência estatal deve permanecer subordinada aos limites éticos e jurídicos impostos pela Constituição. (LOPES JR., Aury.2023).

Dessa maneira, embora a Inteligência Artificial apresente potencial relevante para auxiliar políticas de segurança pública e investigação criminal, sua utilização preditiva exige cautela e regulamentação rigorosa. O desenvolvimento tecnológico não pode afastar o protagonismo humano nas decisões que envolvem liberdade, dignidade e responsabilização penal. A adoção de sistemas preditivos deve observar princípios de transparência, fiscalização, proporcionalidade e controle judicial, assegurando que a modernização tecnológica não resulte na institucionalização de práticas discriminatórias ou autoritárias incompatíveis com o Estado Democrático de Direito.

3.1. A Desmitificação da Neutralidade Tecnológica

Durante muito tempo, consolidou-se a ideia de que a tecnologia seria essencialmente neutra, funcionando apenas como instrumento técnico desprovido de valores, ideologias ou interesses sociais. No contexto da Inteligência Artificial aplicada à persecução penal, essa percepção contribuiu para a disseminação do entendimento de que decisões automatizadas seriam mais

objetivas, imparciais e eficientes do que aquelas produzidas exclusivamente por seres humanos. Contudo, o avanço dos estudos sobre algoritmos e sistemas inteligentes demonstrou que a tecnologia está longe de ser neutra, especialmente quando utilizada em áreas sensíveis como a segurança pública e o processo penal.

Os sistemas de Inteligência Artificial são desenvolvidos por seres humanos, programados com determinadas finalidades e alimentados por bancos de dados produzidos socialmente. Isso significa que os algoritmos reproduzem valores, escolhas institucionais, critérios estatísticos e padrões históricos existentes na sociedade. Dessa forma, eventual discriminação, desigualdade ou seletividade presente nos dados utilizados pelo sistema tende a ser incorporada e reproduzida automaticamente pelas ferramentas tecnológicas.

A ilusão da neutralidade tecnológica e algorítmica na persecução penal apoia-se frequentemente no falso argumento de que os sistemas computacionais e estatísticos operam com imparcialidade científica absoluta. Contudo, conforme adverte Silvio Almeida (2019, p. 47), *"a ciência tem o poder de produzir um discurso de autoridade, que poucas pessoas têm a condição de contestar, salvo aquelas inseridas nas instituições em que a ciência é produzida"*, conferindo uma aura de inquestionabilidade técnica a decisões que, no fundo, refletem vieses e escolhas institucionais. No contexto da Inteligência Artificial aplicada à segurança pública, essa suposta neutralidade mascarada de objetividade matemática acaba por blindar os algoritmos contra o escrutínio democrático, dificultando o controle de vieses discriminatórios e a ampla defesa do investigado.

No âmbito da persecução penal, essa problemática torna-se ainda mais grave, pois o sistema criminal historicamente opera de forma seletiva, concentrando sua atuação sobre determinados grupos sociais. Assim, ao utilizar dados oriundos de práticas policiais e judiciais marcadas por desigualdades estruturais, os algoritmos passam a reforçar os mesmos padrões discriminatórios já existentes. A aparência de objetividade tecnológica acaba mascarando decisões profundamente condicionadas por fatores sociais, econômicos e raciais.

Além disso, a crença na neutralidade algorítmica pode gerar excessiva confiança nos sistemas automatizados, reduzindo o senso crítico dos operadores do Direito diante dos resultados produzidos pela Inteligência Artificial. Muitas vezes, decisões fundamentadas em análises algorítmicas passam a ser aceitas como tecnicamente incontestáveis, mesmo quando existem falhas metodológicas, inconsistências estatísticas ou ausência de transparência quanto aos critérios utilizados pelo sistema. Essa situação cria um perigoso deslocamento da responsabilidade decisória, transferindo para a máquina uma legitimidade que ela não possui autonomamente.

Outro fator relevante refere-se à ausência de transparência nos mecanismos de funcionamento dos algoritmos. Em muitos casos, os sistemas utilizados por órgãos de segurança pública são protegidos por sigilo comercial ou possuem estruturas técnicas complexas que dificultam sua fiscalização externa. Consequentemente, torna-se extremamente difícil identificar como determinadas conclusões foram alcançadas, comprometendo a possibilidade de controle democrático sobre a atuação tecnológica do Estado.

A desmistificação da neutralidade tecnológica revela, portanto, que a Inteligência Artificial não pode ser tratada como instrumento puramente objetivo ou infalível. Pelo contrário, trata-se de tecnologia construída socialmente, sujeita a erros, vieses e condicionamentos institucionais. Por essa razão, sua utilização na persecução penal exige permanente fiscalização jurídica, ética e democrática, garantindo que os sistemas tecnológicos permaneçam subordinados aos direitos fundamentais e às garantias constitucionais.

3.2. Seletividade Penal e o Racismo Algorítmico

O debate acerca da Inteligência Artificial na persecução penal torna-se especialmente relevante quando analisado sob a perspectiva da seletividade penal e do racismo algorítmico. O sistema penal brasileiro historicamente apresenta forte seletividade social e racial, concentrando a repressão estatal sobre grupos marginalizados, especialmente pessoas negras, pobres e residentes de regiões periféricas. Nesse contexto, a incorporação de sistemas automatizados de vigilância e predição criminal pode não apenas reproduzir, mas também intensificar desigualdades estruturais já existentes.

O chamado racismo algorítmico ocorre quando sistemas de Inteligência Artificial produzem resultados discriminatórios em razão dos dados utilizados em seu treinamento ou da própria lógica estatística adotada pelos algoritmos. Como os bancos de dados utilizados pelas tecnologias de segurança pública são construídos a partir de práticas históricas de policiamento e persecução penal, acabam refletindo padrões seletivos anteriormente estabelecidos pelas instituições estatais. Assim, indivíduos pertencentes a grupos

historicamente criminalizados tornam-se mais frequentemente identificados como suspeitos, monitorados ou submetidos à vigilância estatal.

Um dos exemplos mais debatidos refere-se aos sistemas de reconhecimento facial utilizados por órgãos de segurança pública. Diversos estudos internacionais e nacionais demonstram que esses mecanismos apresentam índices significativamente maiores de erro quando aplicados a pessoas negras. Isso ocorre porque muitos algoritmos são treinados predominantemente com bancos de imagens compostos por pessoas brancas, reduzindo a precisão da identificação em relação a outros grupos raciais. Como consequência, aumentam os riscos de abordagens policiais indevidas, prisões injustas e constrangimentos ilegais.

Além do reconhecimento facial, sistemas de análise preditiva também podem reforçar práticas discriminatórias. Regiões periféricas e comunidades historicamente mais policiadas tendem a gerar maior volume de registros criminais, fazendo com que os algoritmos identifiquem tais locais como áreas de “alto risco”. A partir disso, intensifica-se o policiamento nessas regiões, produzindo novos registros e alimentando continuamente o próprio ciclo seletivo do sistema penal. Cria-se, assim, uma dinâmica de retroalimentação algorítmica da seletividade criminal.

A incorporação de sistemas automatizados de predição criminal e reconhecimento facial pelas forças de segurança pública não ocorre no vácuo, mas sobre um terreno institucional historicamente seletivo. Como aponta Silvio Almeida (2019, p. 44-45), o imaginário punitivo e a construção do estereótipo do criminoso *"não poderia se sustentar sem um sistema de justiça seletivo, sem a criminalização*

da pobreza e sem a chamada 'guerra às drogas', que, na realidade, é uma guerra contra os pobres e, particularmente, contra as populações negras". Nesse sentido, quando a Inteligência Artificial é alimentada por bases de dados geradas por essa engrenagem de controle punitivo, o algoritmo absorve e automatiza o racismo estrutural, transformando vieses históricos em "previsões científicas" e aprofundando as marcas da seletividade penal.

A problemática torna-se ainda mais grave diante da aparente legitimidade científica atribuída às decisões automatizadas. O discurso da objetividade tecnológica muitas vezes oculta práticas discriminatórias estruturais, dificultando a identificação dos vieses presentes nos sistemas utilizados. Diferentemente do preconceito humano explícito, o racismo algorítmico opera de forma silenciosa, técnica e estatisticamente mascarada, conferindo aparência de neutralidade a práticas profundamente excludentes.

Nesse sentido, os debates contemporâneos sobre Inteligência Artificial e processo penal demonstram que a modernização tecnológica não elimina problemas históricos do sistema de justiça criminal, podendo inclusive aprofundá-los caso não existam mecanismos adequados de controle e fiscalização. A adoção de tecnologias inteligentes no âmbito da segurança pública deve estar acompanhada de auditorias independentes, transparência algorítmica, fiscalização democrática e observância rigorosa dos direitos fundamentais.

Portanto, o enfrentamento da seletividade penal e do racismo algorítmico exige o reconhecimento de que a tecnologia não atua de forma neutra ou desvinculada das estruturas sociais. A Inteligência Artificial aplicada à persecução penal precisa ser

submetida a limites éticos e jurídicos capazes de impedir a automatização de discriminações históricas. Somente por meio de regulamentação adequada, controle institucional e compromisso efetivo com a igualdade material será possível utilizar os avanços tecnológicos sem comprometer os princípios fundamentais do Estado Democrático de Direito.

3.3. A Teoria do Direito Penal do Inimigo

A expansão do uso da Inteligência Artificial na investigação criminal também pode ser analisada sob a perspectiva da teoria do Direito Penal do Inimigo, formulada por Günther Jakobs. Segundo essa teoria, determinados indivíduos considerados perigosos ao Estado deixam de ser tratados como cidadãos titulares de direitos e passam a ser vistos como verdadeiros “inimigos”, legitimando-se medidas excepcionais de controle e vigilância.

> *O Direito penal do cidadão é o Direito de todos, o Direito penal do inimigo é daqueles que o constituem contra o inimigo: frente ao inimigo, é só coação física, até chegar & guerra. Esta coação pode ficar limitada em um duplo sentido. Em primeiro lugar, o Estado, não necessariamente, excluirá o inimigo de todos os direitos. Neste sentido, o sujeito submetido à custodia de segurança fica incólume em seu papel de proprietário de coisas. E, em segundo lugar, o Estado não tem por que fazer tudo o que é permitido fazer, mas pode conter-se, em especial, para não fechar a porta a um posterior acordo de paz. Mas isto em nada altera o fato de que a medida executada contra o inimigo não significa nada, mas só coage. O Direito penal do cidadão mantém a vigencia da norma, o Direito penal do inimigo (em sentido amplo: incluindo o Direito das medidas de seguranca) combate perigos; com toda certeza existem múltiplas formas intermediárias.*

Nesse cenário, o uso indiscriminado de sistemas de monitoramento inteligente, reconhecimento facial e policiamento preditivo podem intensificar práticas incompatíveis com o Estado Democrático de Direito. Isso ocorre porque a IA, ao operar por padrões estatísticos e previsões probabilísticas, tende a identificar indivíduos com base em perfis de risco, e não necessariamente em condutas concretas.

Tal lógica aproxima-se da ideia de antecipação da tutela penal criticada pelo garantismo penal, pois desloca a persecução criminal do fato efetivamente praticado para uma presunção de periculosidade construída algoritmicamente. Em outras palavras, o indivíduo passa a ser monitorado ou investigado não pelo que fez, mas pelo que o sistema entende que ele potencialmente poderá fazer.

Conforme leciona Aury Lopes Jr. (2023), o processo penal não pode admitir mecanismos incompatíveis com a presunção de inocência e com o devido processo legal. A investigação criminal deve estar fundamentada em indícios concretos e juridicamente válidos, e não em meras inferências estatísticas produzidas por sistemas automatizados opacos.

Além disso, a ausência de transparência dos algoritmos utilizados pelas forças de segurança dificulta o exercício do contraditório e da ampla defesa, uma vez que o investigado pode sequer compreender os critérios utilizados para sua inclusão em determinada análise de risco.

Portanto, a utilização da Inteligência Artificial no âmbito da persecução penal deve observar limites constitucionais rígidos, evitando que a tecnologia seja utilizada como instrumento de expansão de um modelo de Direito Penal preventivo e autoritário incompatível com os princípios fundamentais do ordenamento jurídico brasileiro.

4. A PROVA DIGITAL NO ORDENAMENTO JURÍDICO BRASILEIRO

A presente seção tem como objetivo demonstrar e exemplificar formas adequadas de utilização da Inteligência Artificial na produção de provas digitais, evidenciando como a tecnologia pode ser empregada na persecução penal sem violar direitos fundamentais ou comprometer a integridade da cadeia de custódia. Para tanto, o capítulo examina os mecanismos técnicos e normativos necessários para que a modernização probatória ocorra em estrita harmonia com as salvaguardas constitucionais e o devido processo legal.

A crescente digitalização das relações sociais transformou profundamente a forma como as informações são produzidas, armazenadas e compartilhadas na sociedade contemporânea. Nesse cenário, a prova digital passou a ocupar posição de destaque no âmbito do processo penal brasileiro, especialmente em razão da expansão dos crimes cibernéticos e da utilização de meios tecnológicos na prática de infrações penais. Mensagens eletrônicas, registros telefônicos, e-mails, arquivos em nuvem, dados de geolocalização, imagens de câmeras de segurança e conteúdos extraídos de dispositivos eletrônicos tornaram-se elementos cada vez mais frequentes nas investigações criminais e nos processos judiciais.

A prova digital pode ser compreendida como toda informação armazenada, transmitida ou produzida em meio eletrônico capaz de demonstrar a existência de um fato juridicamente relevante. Diferentemente das provas tradicionais, a prova digital possui características próprias, como volatilidade, facilidade de alteração, grande capacidade de armazenamento e necessidade de conhecimentos técnicos específicos para sua obtenção e preservação. Tais peculiaridades exigem cuidados rigorosos quanto à coleta, armazenamento e análise do material probatório, especialmente para garantir sua autenticidade, integridade e confiabilidade.

No ordenamento jurídico brasileiro, embora não exista um código específico destinado exclusivamente à disciplina da prova digital, diversos dispositivos legais oferecem fundamentos normativos para sua utilização. A Constituição Federal assegura a inviolabilidade da intimidade, da vida privada, do sigilo das comunicações e do devido processo legal, estabelecendo limites à atuação estatal na obtenção

de dados eletrônicos. Além disso, o Código de Processo Penal disciplina a admissibilidade das provas e veda expressamente a utilização de provas ilícitas, especialmente aquelas obtidas mediante violação de direitos fundamentais.

Com o avanço das tecnologias da informação, surgiram importantes legislações voltadas à regulamentação do ambiente digital. O Marco Civil da Internet representou importante avanço ao estabelecer princípios, garantias e deveres relacionados ao uso da internet no Brasil, disciplinando questões relativas à proteção de dados, guarda de registros eletrônicos e fornecimento de informações mediante ordem judicial. Posteriormente, a Lei Geral de Proteção de Dados (LGPD) fortaleceu a tutela da privacidade e da proteção de dados pessoais, impondo limites ao tratamento de informações digitais tanto pelo setor privado quanto pelo poder público.

A relevância da prova digital tornou-se ainda mais evidente diante do crescimento da criminalidade virtual e da utilização de meios eletrônicos na prática de crimes tradicionais. Atualmente, grande parte das investigações criminais depende da análise de dispositivos eletrônicos e registros digitais, permitindo o rastreamento de comunicações, movimentações financeiras, localização geográfica e interações em redes sociais. Conforme apontam os estudos sobre inteligência artificial e investigação criminal, o ambiente digital passou a fornecer um volume significativo de material probatório, exigindo novas técnicas investigativas e mecanismos tecnológicos de análise de dados.(LOPES JR.2023)

Nesse contexto, a Inteligência Artificial também passou a desempenhar papel relevante na análise da prova digital. Ferramentas baseadas em algoritmos e machine learning são

utilizadas para organizar grandes quantidades de dados, identificar padrões de comportamento, realizar cruzamento automatizado de informações e auxiliar autoridades na identificação de elementos relevantes para a investigação criminal. Essa modernização tecnológica contribui para maior eficiência investigativa, especialmente em crimes complexos envolvendo organizações criminosas, lavagem de dinheiro e delitos cibernéticos.

Todavia, o uso da prova digital também levanta importantes debates jurídicos e constitucionais. Um dos principais desafios refere-se à preservação da cadeia de custódia da prova digital. Em razão da facilidade de manipulação e alteração dos arquivos eletrônicos, torna-se indispensável a adoção de procedimentos técnicos capazes de garantir a autenticidade e integridade do material coletado. A ausência de preservação adequada pode comprometer a confiabilidade da prova e resultar em sua invalidação judicial.

Além disso, a obtenção de provas digitais frequentemente envolve restrições a direitos fundamentais, especialmente à privacidade e ao sigilo das comunicações. A coleta indiscriminada de dados, o acesso irregular a dispositivos eletrônicos e o monitoramento excessivo de indivíduos podem configurar violações constitucionais, tornando ilícita a prova produzida. Dessa forma, o uso de meios tecnológicos na persecução penal deve observar rigorosamente os princípios da proporcionalidade, legalidade e necessidade, evitando abusos estatais e práticas incompatíveis com o Estado Democrático de Direito.(Renz; Anschau; Zanatta, 2025).

Outro ponto de destaque refere-se à dificuldade de equilíbrio entre eficiência investigativa e garantias processuais. Embora as tecnologias digitais ampliem significativamente a capacidade

investigativa do Estado, também aumentam os riscos de vigilância excessiva, monitoramento em massa e utilização abusiva de dados pessoais. Por essa razão, a doutrina e a jurisprudência vêm reconhecendo a necessidade de regulamentação mais específica acerca da produção, preservação e admissibilidade das provas digitais no processo penal brasileiro.

Dessa maneira, a prova digital consolidou-se como instrumento indispensável à persecução penal contemporânea, refletindo as transformações tecnológicas da sociedade moderna. Contudo, sua utilização exige cautela, responsabilidade e observância rigorosa das garantias constitucionais. O avanço tecnológico não pode ocorrer em detrimento dos direitos fundamentais, sendo imprescindível que o ordenamento jurídico brasileiro desenvolva mecanismos eficazes de regulamentação e controle, assegurando que a modernização investigativa ocorra em conformidade com os princípios do devido processo legal, da ampla defesa e da dignidade da pessoa humana.

4.1. Cadeia de Custódia e Integridade de Dados

A crescente utilização de provas digitais produzidas ou analisadas por sistemas de Inteligência Artificial torna indispensável a observância rigorosa da cadeia de custódia prevista nos artigos 158-A a 158-F do Código de Processo Penal brasileiro.

> *Art. 158-A. Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte. (Incluído pela Lei nº 13.964, de 2019)*
>
> *§ 1º O início da cadeia de custódia dá-se com a preservação do local de crime ou com procedimentos policiais ou periciais nos quais seja detectada a existência de vestígio. (Incluído pela Lei nº 13.964, de 2019)*
>
> *§ 2º O agente público que reconhecer um elemento como de potencial interesse para a produção da prova pericial fica responsável por sua preservação. (Incluído pela Lei nº 13.964, de 2019)*
>
> *§ 3º Vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal. (Incluído pela Lei nº 13.964, de 2019)*

A cadeia de custódia consiste no conjunto de procedimentos destinados a preservar a integridade e a autenticidade dos vestígios coletados durante a investigação criminal, assegurando que não ocorram adulterações, perdas ou contaminações das provas produzidas.

No contexto da Inteligência Artificial, essa preocupação ganha maior relevância, pois os sistemas automatizados operam a partir de grandes volumes de dados digitais, muitas vezes manipulados por softwares complexos e de difícil auditabilidade. Assim, qualquer falha no armazenamento, processamento ou compartilhamento

dessas informações pode comprometer a confiabilidade da prova digital.

Segundo Gustavo Badaró (2021), a validade da prova penal depende não apenas de sua obtenção lícita, mas também da preservação de sua integridade durante todas as fases da persecução penal. A ausência de controle adequado sobre a cadeia de custódia pode gerar nulidade probatória e violação ao devido processo legal.

Além disso, o uso de Inteligência Artificial exige mecanismos técnicos capazes de garantir rastreabilidade, transparência e auditabilidade dos dados utilizados pelos algoritmos. Isso porque a defesa deve possuir condições de verificar como determinada conclusão automatizada foi produzida.

Nesse sentido, a preservação da cadeia de custódia digital constitui requisito indispensável para a admissibilidade das provas derivadas de sistemas de IA, funcionando como instrumento de proteção das garantias constitucionais do investigado e de legitimidade da atividade investigativa estatal.

4.2. O Princípio da Não Autoincriminação e a Produção de Prova por IA

O princípio da não autoincriminação, consagrado pela expressão latina *nemo tenetur se detegere*, assegura ao investigado o direito de não produzir prova contra si mesmo. Trata-se de garantia fundamental prevista implicitamente na Constituição Federal de 1988 e expressamente reconhecida no artigo 8º da Convenção Americana sobre Direitos Humanos.

Com o avanço da Inteligência Artificial aplicada à persecução penal, surgem novos desafios relacionados à proteção desse direito fundamental. Ferramentas capazes de acessar dispositivos eletrônicos, analisar padrões comportamentais, interpretar dados biométricos e processar informações pessoais em larga escala podem resultar em formas indiretas de autoincriminação.

Um exemplo relevante refere-se à utilização de tecnologias de reconhecimento facial e extração automatizada de dados de celulares e computadores apreendidos. Nessas hipóteses, discute-se até que ponto o investigado pode ser compelido a fornecer senhas, biometria facial ou impressões digitais para desbloqueio de dispositivos eletrônicos.

Aury Lopes Jr. (2023) sustenta que o investigado não possui dever de colaborar ativamente com a própria incriminação, sendo incompatível com o sistema acusatório qualquer medida coercitiva destinada à obtenção compulsória de prova autoincriminatória. Além disso, a utilização de algoritmos para construção de perfis comportamentais e análise preditiva de condutas pode ampliar excessivamente o poder investigativo estatal, colocando em risco direitos fundamentais relacionados à privacidade, intimidade e liberdade individual.

Dessa forma, a aplicação da Inteligência Artificial na investigação criminal deve respeitar os limites constitucionais impostos pelo princípio da não autoincriminação, garantindo que o avanço tecnológico não comprometa direitos historicamente conquistados no âmbito do processo penal democrático.

5. CONSIDERAÇÕES FINAIS

O presente estudo debruçou-se sobre a utilização da Inteligência Artificial no âmbito da investigação e persecução penal no ordenamento jurídico brasileiro, analisando as profundas tensões entre a busca estatal por maior eficiência probatória e o respeito inafastável às garantias e direitos fundamentais assegurados pela Constituição Federal de 1988. O ponto central da investigação consistiu em identificar de que forma e por quais caminhos o uso dessas tecnologias pode ocorrer no âmbito policial sem comprometer princípios estruturantes do processo penal democrático, como o devido processo legal, a presunção de inocência, a ampla defesa e o direito contra a autoincriminação.

Em resposta à problemática proposta, conclui-se que o caminho constitucionalmente hígido para a utilização de ferramentas inteligentes na atividade investigativa pressupõe a edição de uma regulamentação normativa e técnica específica, combinada com a viabilidade da criação e implementação de uma Inteligência Artificial pública e estatal. Confirma-se, assim, a hipótese aventada de que a tecnologia deve atuar estritamente como instrumento de suporte operacional das forças de segurança, voltada ao processamento massivo de informações, triagem documental e automação de rotinas repetitivas, sendo vedada qualquer substituição do juízo de valor e da valoração probatória que cabem exclusivamente aos policiais e às autoridades judiciárias. A eficiência investigativa não justifica a mitigações de direitos do investigado, nem a aceitação de modelos opacos de “caixa-preta”, de modo que a validade das provas tecnológicas exige transparência algorítmica, código auditável, controle humano e estrita preservação da cadeia de custódia e das regras de proteção de dados pessoais.

Apesar de alcançar os objetivos delineados, este trabalho reconhece limitações decorrentes da acelerada evolução tecnológica e da dinamicidade do debate legislativo no cenário nacional. Como lacunas e desdobramentos para investigações futuras, aponta-se a necessidade de acompanhar os impactos práticos de eventuais legislações específicas sobre IA que venham a ser promulgadas no Brasil, bem como a realização de estudos empíricos sobre a eficiência real e os índices de erro dos sistemas de reconhecimento facial e policiamento preditivo aplicados na segurança pública brasileira. Abre-se, assim, espaço para novas construções teóricas que aprofundem os limites de governança de dados na segurança pública e a efetividade dos mecanismos institucionais de auditoria algorítmica independente.

Por fim, compreende-se que o desafio do uso da Inteligência Artificial na investigação criminal não consiste em impedir o avanço tecnológico, mas em estabelecer condições para que sua utilização seja compatível com os princípios que orientam o Estado Democrático de Direito. O aperfeiçoamento dos mecanismos de transparência, controle institucional e proteção de dados, aliado à capacitação dos profissionais responsáveis por sua utilização, mostra-se necessário para reduzir os riscos de abusos e assegurar maior confiabilidade à atividade investigativa. Assim, a efetividade da persecução penal deve ser compreendida não apenas pela rapidez na apuração dos fatos, mas também pela observância dos direitos fundamentais e pela legitimidade dos meios empregados na busca pela verdade processual.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Silvio Luiz de. **Racismo estrutural.** São Paulo: Sueli Carneiro; Pólen, 2019. (Feminismos Plurais).

BADARÓ, Gustavo Henrique. Processo Penal. 3. ed. São Paulo: **Revista dos Tribunais,** 2021.

BRASIL. **Código de Processo Penal. Decreto-Lei nº 3.689,** de 3 de outubro de 1941. Brasília, DF: Presidência da República, 1941.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988.

BRASIL. **Lei Geral de Proteção de Dados Pessoais.** Brasília, DF: Presidência da República, 2018.

COSTA, Mauir Victor da Silva da; FELLER, Thiago de Almeida. O uso da inteligência artificial na investigação criminal. **Revista Ibero-Americana de Humanidades, Ciências e Educação,** São Paulo, v. 11, n. 11, 2025.

DONEDA, Danilo; ALMEIDA, Virgílio A. F. **O que é a governança de algoritmos? Revista de Direito Civil Contemporâneo,** v. 8, 2016.

JAKOBS, Günther; MELIÁ, Manuel Cancio. **Direito Penal do Inimigo. 2. ed.** Porto Alegre: Livraria do Advogado, 2012.

LOPES JR., Aury. **Direito Processual Penal. 20.** ed. São Paulo: Saraiva, 2023.

MAGRANI, Eduardo. **A internet das coisas.** Rio de Janeiro: FGV Editora, 2019.

PILÓ, Xenofontes Curvelo; BRASIL, Deilton Ribeiro. **A utilização da inteligência artificial no Direito Penal e seus reflexos nas garantias e direitos fundamentais. Revista EJEF,** Belo Horizonte, ano 1, n. 1, jul./dez. 2022.

RENZ, Érica Talia; ANSCHAU, Joice; ZANATTA, Leticia Gheller. **Segurança pública e inteligência artificial: uma análise crítica da Portaria MJSP nº 961/2025 na investigação criminal. XVIII Mostra de Iniciação Científica** – MIC-DIR, 2025.

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: A Modern Approach. 3. ed.** Upper Saddle River: Prentice Hall, 2010.

SOUZA, Giulianne Quintale Covelo de. **O impacto da inteligência artificial na investigação criminal. 2024. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Pontifícia Universidade Católica de São Paulo,** São Paulo, 2024.

Trabalho de Conclusão de Curso apresentado no Centro Universitário Santo Agostinho (UNIFSA), no Curso de Direito, Teresina-PI, 10 de setembro de 2026.

[1] Bacharelando do Curso de Direito do Centro Universitário Santo Agostinho (UNIFSA). E-mail: acesse o artigo original para visualizar o e-mail

[2] Bacharelando do Curso de Direito do Centro Universitário Santo Agostinho (UNIFSA). E-mail: acesse o artigo original para visualizar o e-mail

[3] Professor do Centro Universitário Santo Agostinho - UNIFSA. Mestre em Economia pela Universidade Federal do Ceará (2010). Possui graduação em Ciências Contábeis pela Universidade Estadual do Ceará (1999) e graduação em Direito pela Universidade Federal do Ceará (1998). Exerce o cargo de Delegado de Polícia Civil do Estado do Piauí desde. E-mail: acesse o artigo original para visualizar o e-mail