JNT - FACIT BUSINESS AND TECHNOLOGY JOURNAL - ISSN: 2526-4281 - QUALIS B1
ANO 2025 – MÊS DE JUNHO - FLUXO CONTÍNUO – Ed. 63. Vol. 1. Págs. 61-78
DOI: 10.5281/zenodo.16423722

INTELIGÊNCIA ARTIFICIAL, PREVENÇÃO DE CRIMES E DIREITOS FUNDAMENTAIS: UMA ABORDAGEM CRIMINOLÓGICA

ARTIFICIAL INTELLIGENCE, CRIME PREVENTION AND FUNDAMENTAL RIGHTS: A CRIMINOLOGICAL APPROACH

Cirlene da Conceição PESSOA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: cirlenecpessoa@hotmail.com
ORCID: http://orcid.org/0009-0000-9212-1165

Sandra Renata Alves da SILVA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: srenata231@gmail.com
ORCID: http://orcid.org/0009-0006-8076-3703

Marcos Neemias Negrão REIS
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: marcos.reis@unitpac.edu.br
ORCID: http://orcid.org/0000-0002-6492-8460

RESUMO

O presente artigo analisa os impactos do uso da inteligência artificial (IA) na prevenção de crimes, à luz dos direitos fundamentais e sob uma abordagem criminológica crítica. A partir da constatação de que a sociedade contemporânea é profundamente marcada pela digitalização das relações sociais e pela crescente dependência de tecnologias algorítmicas, observa-se que sistemas de IA têm sido progressivamente incorporados às práticas de segurança pública, controle social e persecução penal. Ferramentas como policiamento preditivo, reconhecimento facial, análise de redes e rastreamento comportamental são frequentemente utilizadas sob o argumento de eficiência na prevenção criminal. No entanto, a utilização da IA no âmbito penal não está isenta de riscos. Estudos demonstram que algoritmos podem reproduzir e até amplificar discriminações estruturais, afetando especialmente grupos vulnerabilizados. Além disso, o caráter opaco das decisões automatizadas compromete princípios constitucionais como o devido processo legal, a ampla defesa, a dignidade da pessoa humana e a igualdade. A seletividade penal, historicamente denunciada pela criminologia crítica, ganha novas configurações na era da vigilância digital. Diante desse contexto, o artigo propõe uma reflexão sobre os limites éticos,

jurídicos e criminológicos da IA na prevenção criminal. Defende-se a necessidade de regulamentação robusta, com mecanismos de explicabilidade, transparência, auditoria algorítmica e accountability, de modo a compatibilizar inovação tecnológica com os pilares do Estado Democrático de Direito e a proteção dos direitos fundamentais.

Palavras-chave: Inteligência Artificial. Prevenção Criminal. Direitos Fundamentais. Criminologia Crítica. Discriminação Algorítmica.

ABSTRACT

This paper analyzes the impacts of using artificial intelligence (AI) in crime prevention, based on fundamental rights and under a critical criminological approach. Acknowledging that contemporary society is deeply shaped by the digitalization of social relations and the growing dependence on algorithmic technologies, it is observed that AI systems have been increasingly incorporated into public security practices, social control, and criminal justice. Tools such as predictive policing, facial recognition, network analysis, and behavioral tracking are commonly employed under the premise of greater efficiency in crime prevention. However, the use of AI in the criminal field is not without risks. Research shows that algorithms can reproduce and even amplify structural discrimination, disproportionately affecting vulnerable groups. Furthermore, the opacity of automated decisions compromises constitutional principles such as due process, the right to defense, human dignity, and equality. Penal selectivity, historically denounced by critical criminology, assumes new forms in the era of digital surveillance. Given this scenario, the paper proposes a reflection on the ethical, legal, and criminological boundaries of AI in crime prevention. It advocates for the need for robust regulation, including mechanisms of explainability, transparency, algorithmic auditing, and institutional accountability, aiming to align technological innovation with the core values of the Democratic Rule of Law and the protection of fundamental rights.

Keywords: Artificial intelligence. Cybercrime. Non-discrimination. Critical criminology. Fundamental rights.

INTRODUÇÃO

A contemporaneidade, marcada pela intensificação do uso de tecnologias digitais em todas as esferas da vida social e configurada como "sociedade em rede" que, segundo Castels (2005, p. 17), apresenta relações interpessoais, econômicas, políticas e jurídicas permeadas por fluxos informacionais constantes, mediados por dispositivos tecnológicos sofisticados. Nesse cenário, a inteligência artificial (IA) emerge como ferramenta influente, ofertando possibilidades inéditas de automatização, eficiência e antecipação de comportamentos. Contudo, sua capacidade disruptiva suscita profundas inquietações no campo do Direito, especialmente em sua aplicação à segurança pública e à prevenção de crimes cibernéticos.

Esta crescente sofisticação das infraestruturas digitais tem sido acompanhada por uma escalada dos delitos no ambiente virtual. Ataques a sistemas informacionais, fraudes eletrônicas, invasões de privacidade, crimes de ódio e violências digitais desafiam o Estado e suas instituições de controle. Diante desse quadro, a inteligência artificial é convocada como aliada estratégica para mapear riscos, prever condutas, identificar suspeitos e agir preventivamente. A promessa de um aparato repressivo mais ágil e inteligente, contudo, não se mostra imune a críticas, particularmente quando se observa o potencial dessas tecnologias para reproduzir ou amplificar discriminações estruturais preexistentes.

A utilização de IA para fins de prevenção criminal, especialmente quando fundamentada em dados históricos enviesados, pode reforçar padrões seletivos e estigmatizantes já identificados na atuação dos sistemas de justiça penal tradicionais. Casos em que algoritmos, treinados a partir de bancos de dados influenciados por discriminações raciais, sociais e de gênero, passam a identificar certos grupos populacionais como mais perigosos em detrimento de outros, não são incomuns. Essa realidade revela um paradoxo inquietante: a busca por maior eficiência na repressão criminal pode inadvertidamente legitimar formas automatizadas de exclusão e perseguição, em direta afronta ao princípio da igualdade.

Nesse ponto, o debate sobre o direito à não discriminação assume centralidade. No contexto constitucional brasileiro e no ordenamento jurídico internacional, esse direito ocupa lugar de destaque entre os direitos fundamentais,

sendo considerado cláusula pétrea e núcleo essencial da dignidade da pessoa humana.

A Constituição da República de 1988 preconiza a presunção de inocência como um de seus princípios no tocante à extensão das investigações e ao próprio processo acusatório de forma geral. Isso demonstra a preocupação de um Estado de Direito em não afligir garantias fundamentais individuais, mesmo quando se propõe uma observação mais ampliada, profunda e complexa do contexto delitivo.

A aplicação da IA neste ambiente, portanto, deve submeter-se a rigorosos critérios de controle, transparência e responsabilização, de modo a evitar que os avanços tecnológicos sejam utilizados para consolidar estruturas autoritárias ou práticas discriminatórias sob o pretexto da inovação.

Ademais, a questão da opacidade das decisões automatizadas merece atenção. Sistemas de IA operam, frequentemente, por meio de lógicas internas de difícil compreensão, mesmo para seus desenvolvedores, comprometendo o direito à ampla defesa, ao contraditório e ao devido processo legal, princípios estes que devem ser observados em todos os aspectos da prevenção criminal e da própria aplicação da norma punitiva.

Nesse cenário, a criminologia moderna desempenha um papel essencial ao oferecer instrumentos teóricos capazes de problematizar o uso da tecnologia na produção e gestão da criminalidade, sobretudo no que tange à prevenção delitiva. Neste sentido, Filho; Gimenes (2025, pág. 137), afirmam que:

> Enquanto a criminologia clássica vislumbra o crime como um enfrentamento da sociedade pelo criminoso (luta do bem contra o mal), numa forma minimalista do problema, a criminologia moderna observa o delito de maneira ampla e interativa, como um ato complexo em que os custos da reação social também são demarcados.

Será possível, portanto, compreender que a criminalidade cibernética não se restringe a um problema técnico a ser solucionado por algoritmos eficientes, mas configura uma questão política e social que exige reflexão ética, normativa e garantista.

O ordenamento jurídico brasileiro, neste particular, já possui de marcos legais que abordam ao tema. A Carta Magna consagra a igualdade como princípio

fundamental e veda qualquer forma de discriminação. Por outro lado, a Lei nº 13.709/18, denominada de Lei Geral de Proteção de Dados Pessoais (LGPD), por sua vez, estabelece critérios para o tratamento ético de informações pessoais, incluindo dispositivos sobre decisões automatizadas. Essas normas, contudo, demandam aplicação mais efetiva e interpretações que as atualizem frente aos desafios impostos pela inteligência artificial e pela digitalização dos mecanismos de controle social.

Paralelamente, observa-se no plano internacional um esforço crescente de regulamentação da IA, com destaque para o European AI Act, ou Regulamento Inteligência Artificial, que insere a Europa na vanguarda dos cuidados com o uso das inteligências artificiais, assim como as recomendações da Unesco e os relatórios da ONU sobre direitos digitais. Essas iniciativas reforçam a necessidade de criação de marcos normativos capazes de compatibilizar o uso da tecnologia com os valores democráticos e com os direitos humanos.

A ideia de que a IA pode antecipar crimes antes de sua ocorrência, como sugere a lógica do "pré-crime", popularizada pela ficção científica e por algumas experiências policiais, deve ser confrontada com o princípio da presunção de inocência e com os limites do poder punitivo estatal. A predição comportamental, por mais acurada que se revele, não pode substituir o juízo de culpa e o processo penal regular. O risco reside na substituição do cidadão pelo "perfil de risco", transformando indivíduos em dados e decisões judiciais em probabilidades estatísticas.

Não se trata, contudo, de negar a utilidade da inteligência artificial na prevenção de crimes cibernéticos, mas de circunscrever claramente os contornos ético-jurídicos de sua atuação. A tecnologia deve servir à justiça, à igualdade e à dignidade humana — e não o contrário. Urge, portanto, fomentar o debate público e acadêmico sobre os limites da automação no campo penal, bem como investir em pesquisas interdisciplinares que integrem conhecimentos do Direito, da Criminologia, da Informática e das Ciências Sociais.

Este estudo parte do pressuposto de que a proteção dos direitos fundamentais, notadamente o direito à não discriminação, deve orientar qualquer política pública de prevenção criminal fundamentada em tecnologias digitais. A construção de uma justiça digital verdadeiramente democrática pressupõe o enfrentamento crítico dos

riscos do determinismo tecnológico e a elaboração de critérios normativos que estabeleçam limites claros ao uso da IA em contextos de poder punitivo.

Ao longo desta análise, será realizada uma investigação teórica e crítica do emprego da inteligência artificial na prevenção de crimes cibernéticos, com especial atenção às suas implicações sobre o direito à não discriminação. Serão discutidos os principais desafios éticos e jurídicos, bem como propostas regulatórias que busquem harmonizar inovação tecnológica com o respeito aos direitos humanos.

O presente trabalho também visa demonstrar a relevância da criminologia crítica para a compreensão dos processos de criminalização digital e da seletividade algorítmica. Concomitantemente, serão exploradas as possibilidades normativas oferecidas pela Constituição Federal, pela LGPD e por tratados internacionais no enfrentamento dessas novas formas de discriminação.

Em última análise, espera-se que esta pesquisa contribua para o fortalecimento de um modelo de prevenção criminal que seja tecnicamente eficiente, juridicamente responsável e, sobretudo, comprometido com os valores fundamentais do Estado Democrático de Direito.

A EVOLUÇÃO DA PREVENÇÃO CRIMINAL NA SOCIEDADE DIGITAL

Da Prevenção Tradicional à Prevenção Preditiva

Historicamente, a prevenção criminal sempre ocupou papel central nos modelos de controle social desenvolvidos. Desde os sistemas repressivos clássicos, pautados na punição como resposta ao delito consumado, até as abordagens preventivas contemporâneas que buscam antecipar o risco e neutralizá-lo antes que se concretize, observa-se uma transformação substancial nas formas de conceber o crime, o criminoso e o próprio papel do Estado. A emergência da sociedade da informação e a ascensão da lógica algorítmica como base para a tomada de decisões públicas inaugura uma nova etapa dessa trajetória: a da prevenção automatizada e preditiva.

Importante considerar que a prevenção criminal sempre esteve associada a modelos tradicionais de controle social, cuja atuação se dava, majoritariamente, no espaço físico e por meio de métodos baseados na observação humana, na repressão policial e no monitoramento comunitário. Esse modelo se estruturava tanto em ações

primárias, voltadas à redução de fatores criminógenos, como pobreza, marginalização e falta de acesso a direitos, quanto em ações secundárias, focadas na vigilância de grupos considerados de risco, geralmente determinados por critérios sociais, raciais e territoriais. Neste aspecto, Filho; Gimenes (2025, pág. 137) afirmam que:

> Enquanto a criminologia clássica vislumbra o crime como um enfrentamento da sociedade pelo criminoso (luta do bem contra o mal), numa forma minimalista do problema, a criminologia moderna observa o delito de maneira ampla e interativa, como um ato complexo em que os custos da reação social também são demarcados.

Com o avanço das tecnologias da informação e a consolidação da sociedade digital, assistiu-se a uma transição paradigmática em relação aos mecanismos de controle social. A prevenção, antes centrada na presença física e nas práticas tradicionais de policiamento, passa a ser mediada por dispositivos tecnológicos capazes de monitorar, cruzar e analisar grandes volumes de dados.

No paradigma clássico da prevenção criminal a função da norma penal era essencialmente preventiva, mas operava segundo uma lógica racional e proporcional, em que a pena deveria funcionar como um desestímulo à prática de delitos. Já no Séc. XIX, com a criminologia positivista, há um deslocamento do foco da conduta para o sujeito: o criminoso passa a ser entendido como portador de características patológicas ou degenerativas, e a prevenção criminal assume um caráter biopolítico, visando neutralizar o "perigo" que certos indivíduos representariam para a ordem social.

Com o advento do Séc. XX, e, mais distintamente, com o desenvolvimento da criminologia crítica e da sociologia do desvio, a concepção de prevenção transcende sua acepção meramente protetiva para ser compreendida também como uma complexa manifestação de controle social seletivo. Essa operacionalização ocorre tanto em níveis simbólicos quanto institucionais.

A Escola de Chicago, com suas pioneiras análises sobre a desorganização social e a ecologia urbana, e teóricos como Foucault, que desvelaram os dispositivos disciplinares e os mecanismos de vigilância, foram instrumentais na desnaturalização das práticas preventivas. Suas contribuições elucidaram os vínculos intrínsecos

dessas práticas com as estruturas de poder e as estratégias de exclusão social, revelando a dimensão política e social subjacente à sua aplicação.

É nesse contexto que se insere a atual reconfiguração da prevenção criminal na era digital, evidenciando a consolidação de um modelo tecnocrático de prevenção, altamente dependente de bases de dados massivas e da análise algorítmica de comportamentos. Trata-se de uma mudança paradigmática: a prevenção deixa de ser apenas um instrumento político-jurídico baseado em evidências normativas e passa a se orientar por modelos estatísticos, padrões probabilísticos e inferências automatizadas. Essa mudança implica uma série de riscos e desafios que serão considerados e observados ao longo desta análise.

Inteligência Artificial Aplicada à Prevenção de Crimes

A integração da inteligência artificial (IA) no âmbito da segurança pública emerge como uma das mais impactantes transformações nas arquiteturas contemporâneas de controle social. Longe de se configurar meramente como um subsídio instrumental, a IA ascende, de fato, a uma posição de instância decisional indireta. Sua influência permeia e reconfigura as práticas investigativas, as estratégias de policiamento ostensivo, os modelos de gestão de riscos e, notavelmente, a própria construção dos sujeitos tidos como suspeitos.

Esse avanço tecnológico se desenvolve, paradoxalmente, em meio a um discurso tecnocrático que enfaticamente celebra a suposta objetividade algorítmica. Tal retórica, no entanto, tende a ocultar as complexas dinâmicas de poder, os interesses corporativos subjacentes e as desigualdades estruturais intrinsecamente imbricadas nas próprias concepções e implementações dessas tecnologias.

Conforme explicitam Chaves Júnior *et al,* ao citarem Navarro (2023, pág. 8), ao conceituar e delimitar a Inteligência Artificial, afirmam que:

> Pode-se delimitar a inteligência artificial como a capacidade das máquinas de mimetizar as habilidades humanas. Isto quer dizer que as máquinas, em alguma medida, imitam o processo cognitivo humano, após um processo de aprendizado baseado em dados que fornecem generalizações sobre dado assunto.

A utilização de algoritmos tem sido a base do funcionamento da Inteligência Artificial. Como reiteram Chaves Júnior *et al* (2023, pág. 8), “um sistema de IA

impende uma sequência de instruções que especifique as diferentes ações a serem executadas pelo computador a fim de resolver um determinado problema".

O funcionamento dos sistemas de inteligência artificial, especialmente aqueles baseados em *machine learning* (aprendizado de máquina) e *deep learning* (aprendizado profundo), depende da análise de grandes conjuntos de dados (*big data*), que alimentam algoritmos programados para identificar padrões, estabelecer correlações e produzir inferências.

No campo da prevenção criminal, essa capacidade de previsão tem sido utilizada para mapear zonas de risco, indicar áreas de policiamento intensificado, identificar potenciais suspeitos e até mesmo para orientar decisões judiciais sobre liberdade provisória, fiança e penas alternativas. Trata-se de uma mudança de paradigma: a decisão sobre quem deve ser vigiado, abordado ou punido não parte apenas da autoridade estatal direta, mas de modelos estatísticos automatizados, frequentemente indecifráveis mesmo para seus programadores.

Entre as aplicações mais difundidas destaca-se o chamado policiamento preditivo, cujas bases epistemológicas estão na criminologia ambiental e na análise espacial da criminalidade. Softwares como o PredPol e o HunchLab, utilizados em cidades dos Estados Unidos e da Europa, baseiam-se em dados históricos de ocorrências policiais para indicar com antecedência onde e quando determinados crimes têm maior probabilidade de ocorrer.

Embora apresentados como instrumentos neutros e científicos, observa-se que esses sistemas operam com forte viés territorial, direcionando ações policiais de forma desproporcional para comunidades específicas, reforçando o ciclo de hiper criminalização de populações historicamente marginalizadas. É como afirmam Silva; Barbosa (2023, pág. 7):

> O risco de propagação e sedimentação de vieses discriminatórios é ainda mais preocupante ao se considerar que os algoritmos, depois de criados e programados por seres humanos, podem aprender e prever resultados com base nos dados aos quais têm acesso.

Um exemplo notório da aplicação tecnológica em questão reside no reconhecimento facial em tempo real. Essa tecnologia tem sido amplamente difundida como uma solução pretensamente eficaz para a identificação de indivíduos

foragidos e sujeitos suspeitos em ambientes de grande circulação, como eventos públicos, instalações esportivas, terminais aeroportuários e espaços urbanos monitorados. Contudo, esta tecnologia tem consistentemente revelado índices de erro preocupantes, particularmente no que concerne ao reconhecimento de mulheres negras e pessoas não brancas, o que levanta sérias implicações para a equidade e a não discriminação.

Segundo apontam Chaves Júnior *et al* (2023, pág. 12), parte do viés utilizado pelas tecnologias de identificação facial são oriundos de seus próprios programadores:

> Uma pesquisa publicada pelo AI Now Institute, instituto de pesquisa que estuda as implicações sociais da inteligência artificial, constatou que a ausência de diversidade dentro das equipes vem contribuindo para a criação de sistemas falhos e que perpetuam preconceitos de gênero e raça. Apenas 15% dos pesquisadores de IA do Facebook e, 10% do Google, são mulheres. As mulheres representam apenas 18% dos graduados em ciência da computação nos Estados Unidos.

Estudos realizados pelo MIT Media Lab demonstraram que, em alguns casos, os sistemas de reconhecimento facial apresentaram taxas de erro superiores a 30% para mulheres negras, ao passo que o erro para homens brancos era inferior a 1%. Essa disparidade revela não apenas limitações técnicas, mas também problemas estruturais de representatividade nos dados utilizados para o treinamento dos algoritmos, reforçando o argumento de que os sistemas de IA refletem os preconceitos do mundo social que os produz. Segundo Goode (2018, pág. 01), há evidentes imprecisões quanto à identificação de gênero:

> O gênero foi identificado erroneamente em menos de um por cento dos homens de pele mais clara; em até sete por cento das mulheres de pele mais clara; até 12% dos homens de pele mais escura; e até 35 por cento em mulheres de pele mais escura.

No Brasil, experiências similares vêm sendo adotadas de forma crescente por estados e municípios, muitas vezes sem qualquer base normativa específica ou mecanismos de controle institucional. A ausência de transparência, participação democrática e auditoria independente na aquisição e implementação dessas tecnologias evidencia uma grave lacuna regulatória, que coloca em risco direitos fundamentais consagrados constitucionalmente. O uso da IA, nesses termos, deixa de

ser uma ferramenta a serviço da justiça e se transforma em um instrumento opaco de ampliação do poder punitivo.

RISCOS, DESAFIOS E IMPACTOS DA IA SOBRE OS DIREITOS FUNDAMENTAIS

A incorporação de tecnologias de inteligência artificial no sistema de justiça criminal e na segurança pública não pode ser tratada apenas como um avanço técnico, mas como um processo que modifica as estruturas de responsabilização, os modos de exercício do poder punitivo e, sobretudo, o equilíbrio entre segurança e liberdade em uma sociedade democrática.

A seguir, serão analisados dois eixos fundamentais de impacto: o viés algorítmico e a discriminação estrutural, e a opacidade algorítmica e os desafios ao devido processo legal.

Viés Algorítmico e a Reprodução de Discriminações Estruturais

Um dos riscos mais proeminentes associados à implementação da inteligência artificial em contextos de justiça criminal é o fenômeno do viés algorítmico. Este se refere à propensão de sistemas computacionais reproduzirem, perpetuarem ou, inclusive, intensificarem disparidades sociais, raciais, territoriais e de gênero preexistentes. Contrariamente à percepção de neutralidade tecnológica, os algoritmos são constructos humanos, treinados com dados históricos, e, por conseguinte, intrinsecamente carregam as especificidades dos contextos sociais nos quais foram desenvolvidos.

Se os conjuntos de dados que subsidiam o treinamento desses sistemas forem resultantes de práticas discriminatórias – tais como abordagens policiais seletivas, prisões arbitrárias ou procedimentos judiciais que refletem iniquidades –, os algoritmos tenderão a replicar esses padrões de exclusão, conferindo-lhes uma aparência de cientificidade e legitimidade.

No cenário brasileiro, onde a seletividade penal tem operado historicamente com base em recortes raciais e socioeconômicos, a utilização de dados para alimentar algoritmos de segurança pública impõe a necessidade de uma análise crítica e criteriosa. Não é incomum que comunidades periféricas, caracterizadas por

vulnerabilidade socioeconômica e pela presença estatal predominantemente repressiva, sejam categorizadas como "áreas de risco" por sistemas automatizados.

Tal classificação as torna alvos preferenciais da vigilância estatal, resultando em uma dinâmica na qual a IA, em vez de mitigar distorções históricas, pode operar como uma "tecnologia da suspeição", aprofundando o estigma sobre populações já em situação de vulnerabilidade.

Além da dimensão territorial, o viés algorítmico manifesta-se de forma acentuada na dimensão racial, particularmente em tecnologias de reconhecimento facial. Estudos conduzidos em contextos como Estados Unidos, Reino Unido e Brasil demonstram consistentemente que sistemas de identificação automatizada exibem taxas significativamente elevadas de erro na detecção de rostos de indivíduos negros, asiáticos e indígenas, em comparação com rostos de pessoas brancas. Esse fenômeno, consolidado como *algorithmic bias*, transcende meras falhas técnicas, revelando desigualdades profundas nas bases de dados utilizadas e nos critérios de treinamento dos algoritmos. A consequência direta é a geração de falsos positivos, que submetem indivíduos inocentes à suspeita com base unicamente em sua aparência ou localização.

Este panorama desafia diretamente o princípio da igualdade material, basilar da Constituição Federal de 1988, bem como o direito à não discriminação, previsto em instrumentos jurídicos internacionais de direitos humanos, como o Pacto Internacional sobre Direitos Civis e Políticos e a Convenção Interamericana contra o Racismo. A implementação de tecnologias de IA que produzam efeitos discriminatórios, ainda que por via indireta, deve ser categorizada como uma violação de direitos fundamentais.

Torna-se imperativo, portanto, que qualquer política pública de segurança que incorpore a inteligência artificial seja submetida a rigorosos testes de impacto antidiscriminatório, acompanhados de auditorias independentes, promovendo a participação social e assegurando um controle institucional efetivo.

Opacidade Algorítmica e os Desafios ao Devido Processo Legal

Outro desafio crítico inerente à aplicação da inteligência artificial (IA) no domínio da segurança pública reside na opacidade dos sistemas algorítmicos. Essa

característica intrínseca inviabiliza ou, no mínimo, dificulta o pleno exercício dos direitos processuais fundamentais. Uma parcela significativa dos algoritmos empregados por instituições públicas, ou adquiridos de fornecedores privados, opera com arquiteturas complexas, muitas vezes baseadas em métodos de aprendizado de máquina não supervisionado.

Nesses cenários, os próprios critérios de decisão são ininteligíveis até mesmo para os especialistas que os desenvolveram. Esse fenômeno, frequentemente denominado "caixa-preta algorítmica", impõe severas restrições à transparência e à legitimidade do processo decisório em âmbito penal.

O devido processo legal, conforme salvaguardado pelo artigo 5º, inciso LIV, da Constituição Federal, e ainda em obediência ao princípio da ampla defesa e contraditório, postula que todo cidadão submetido ao julgamento da autoridade estatal possui o direito de conhecer as razões subjacentes às decisões que o afetam, bem como o direito de contestá-las de forma abrangente e informada.

Contudo, quando vereditos judiciais, medidas cautelares, ações de policiamento ou pareceres técnicos são fundamentados em algoritmos cujos critérios não são acessíveis publicamente ou sequer compreensíveis, o contraditório se converte em uma mera formalidade. O indivíduo é então reduzido à condição de objeto de cálculos probabilísticos, privado da capacidade de compreender ou refutar a lógica que o conduziu à condição de suspeito.

Tal opacidade não compromete apenas o contraditório e a ampla defesa, mas também subverte o próprio princípio da legalidade penal. Ao se substituir a tipicidade penal, edificada sobre normas claras e previamente estabelecidas, por sistemas de predição de risco alicerçados em modelos estatísticos, incorre-se no risco de transmutar o juízo jurídico em cálculo técnico. Essa inversão de lógica desloca o epicentro da decisão do magistrado ou da autoridade policial para o programador ou a corporação tecnológica, instituindo uma nova forma de terceirização do poder punitivo, alheia aos mecanismos democráticos de controle e responsabilização.

Adicionalmente, a ausência de explicabilidade algorítmica engendra um substancial problema de *accountability* pública. O cidadão permanece alheio aos motivos pelos quais foi submetido à vigilância, classificado ou sancionado; o agente público carece de plena compreensão da ferramenta que emprega; e o desenvolvedor

do algoritmo se exime de responsabilidade, alegando que a máquina "aprendeu sozinha".

Essa cadeia de opacidade fragiliza os fundamentos do Estado de Direito e impõe a urgência na formulação de uma nova arquitetura normativa, capaz de assegurar que qualquer decisão que impacte direitos fundamentais possa ser integralmente compreendida, questionada e revisada por intermédio de instrumentos jurídicos apropriados.

A integração da inteligência artificial no sistema de justiça criminal, neste caso, se desacompanhada de mecanismos robustos de transparência, supervisão independente, controle jurisdicional e participação social, representa uma grave ameaça à racionalidade garantista do direito penal.

A legitimação da vigilância e da punição não pode se apoiar em instrumentos tecnocientíficos inescrutáveis ao debate público. Imprescindível, dessa forma, reafirmar que a centralidade da pessoa humana, com seus direitos e garantias fundamentais, deve sobrepor-se a qualquer pretensão de eficiência algorítmica.

PARÂMETROS ÉTICOS, JURÍDICOS E CRIMINOLÓGICOS PARA O USO DA IA NA PREVENÇÃO CRIMINAL

A incorporação da inteligência artificial nos sistemas de prevenção e repressão criminal exige, de maneira inadiável, a formulação de parâmetros éticos e jurídicos que assegurem sua compatibilidade com os princípios constitucionais e, crucialmente, com a dignidade da pessoa humana.

A ausência de regulação específica, ou a existência de normativas fragmentadas e insuficientes, pode abrir margem para abusos institucionais, discriminação automatizada e a consolidação de um modelo de justiça opaco, tecnocrático e excludente. Por isso, é fundamental que o uso de IA em segurança pública esteja sujeito a regras claras, controles públicos rigorosos e instrumentos efetivos de responsabilização.

Do ponto de vista normativo, a transparência algorítmica deve ser tratada como condição de validade para a utilização de qualquer tecnologia que produza efeitos jurídicos relevantes. Isso significa garantir que as decisões baseadas em IA sejam compreensíveis, auditáveis e passíveis de contestação. Conforme pontua

Pasquale (2015, p. 11), a opacidade, "por mais que possa estar ligada à complexidade técnica dos sistemas, não pode ser tolerada quando está em jogo o exercício do poder punitivo".

A exigência de explicabilidade, já reconhecida em legislações como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e no projeto do AI Act, deve também ser incorporada ao ordenamento jurídico brasileiro, ampliando as garantias processuais em face de decisões automatizadas.

Outro ponto essencial é a implementação de auditorias algorítmicas independentes e regulares, com a finalidade de detectar eventuais padrões discriminatórios, falhas operacionais e distorções nos resultados. Tais auditorias devem ser conduzidas por entidades técnicas autônomas, com participação da sociedade civil, e os seus resultados devem ser publicamente acessíveis. Essa prática é indispensável para assegurar a *accountability* institucional, evitando que eventuais danos causados por decisões algorítmicas sejam naturalizados ou acobertados sob o argumento da complexidade técnica. Conforme salientam Buolamwini; Gebrou (2018, p. 77), "a avaliação rigorosa desses sistemas é crucial para identificar e mitigar vieses".

Além dos mecanismos normativos e institucionais, é necessário estabelecer um marco ético para o uso de IA em segurança pública. Esse marco deve priorizar a proteção dos direitos humanos, reconhecer os riscos da seletividade penal digital e estabelecer limites objetivos ao uso de tecnologias preditivas. O princípio da precaução, muitas vezes utilizado no campo ambiental, pode e deve ser aplicado aqui: em caso de dúvida razoável quanto à legalidade ou potencial discriminatório de um sistema, deve-se optar por sua não implementação até que seja devidamente verificado e validado.

No plano criminológico, urge incorporar uma perspectiva crítica à análise da IA. A tecnologia, por si só, não é redentora nem neutra: ela é moldada por interesses políticos, econômicos e sociais. A prevenção criminal automatizada, se não for pensada a partir de uma ética da responsabilidade, corre o risco de aprofundar o que Foucault (2014) chamou de "sociedade disciplinar" agora expandida e silenciosamente operante sob a forma de vigilância digital.

Reafirmar os princípios do garantismo penal, da não discriminação e da centralidade da pessoa humana é, portanto, não apenas uma exigência jurídica, mas um imperativo ético diante dos novos desafios colocados pela era da inteligência artificial.

CONSIDERAÇÕES FINAIS

A emergência e a consolidação da inteligência artificial como ferramenta de prevenção criminal transformam radicalmente a relação entre Estado, tecnologia e indivíduo. Ao mesmo tempo em que a IA oferece promessas de maior eficiência na segurança pública, ela também expõe as estruturas do sistema penal a novos riscos, especialmente quando aplicada sem controle, sem transparência e sem critérios éticos bem definidos. A tecnologia, nesse contexto, não é um instrumento neutro: é parte de um arranjo de poder que pode tanto promover justiça quanto reforçar desigualdades, dependendo das escolhas políticas e normativas que a estruturam.

Ao longo deste artigo, procurou-se demonstrar que o uso da inteligência artificial na prevenção de crimes exige uma abordagem crítica, que ultrapasse os discursos tecnicistas e enfrente os impactos concretos sobre os direitos fundamentais. O viés algorítmico, a opacidade das decisões automatizadas, a criminalização estatística de territórios e a fragilização do devido processo legal não são meras falhas de sistema, mas sintomas de uma racionalidade punitiva que tende a se sofisticar, sem necessariamente se tornar mais justa. A seletividade penal, historicamente denunciada pela criminologia crítica, encontra nas tecnologias digitais um novo campo de reprodução e ocultação.

Nesse sentido, é urgente que o contexto normativo brasileiro avance no aperfeiçoamento de instrumentos legais sólidos, inspirado em experiências internacionais, mas sensível às especificidades do contexto nacional. Tais instrumentos devem incluir a exigência de explicabilidade, mecanismos de auditoria externa, responsabilização civil e administrativa, além de espaços institucionais de controle social. A construção de uma justiça digital verdadeiramente democrática passa, necessariamente, pelo reconhecimento de que a proteção dos direitos fundamentais deve estar no centro de qualquer inovação tecnológica aplicada ao campo penal.

Por fim, reafirma-se que a inteligência artificial, quando submetida a princípios constitucionais e orientada por uma ética humanista e garantista, pode sim colaborar para uma sociedade mais segura e justa. No entanto, seu uso irrestrito, sem fiscalização e guiado exclusivamente por métricas de eficiência, representa um risco civilizatório, capaz de corroer as bases do Estado Democrático de Direito. A tarefa que se impõe aos juristas, criminólogos e operadores do sistema de justiça é, portanto, dupla: dominar criticamente os fundamentos técnicos da nova era digital e assegurar que, mesmo diante da mais avançada tecnologia, os direitos humanos não sejam negociáveis.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais - LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: **Intersectional Accuracy Disparities in Commercial Gender Classification.** In: Proceedings of the 1st Conference on Fairness, Accountability and Transparency, New York, NY, USA, 23–24 fev. 2018. Proceedings of Machine Learning Research, v. 81, p. 77–91, 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a.html. Acesso em: 30 maio. 2025.

CHAVES JÚNIOR, José Eduardo; et al. **Inteligência artificial e vieses algorítmicos.** Revista Brasileira de Direito, Passo Fundo, v. 19, n. 2, p. 1-24, maio-ago. 2023. Disponível em: https://doi.org/10.26512/rbd.v19i2.4768. Acesso em: 30 maio. 2025.

FILHO, Nestor Sampaio P.; GIMENES, Eron V. **Criminologia** - 15ª Edição 2025. 15. ed. Rio de Janeiro: SRV, 2025.

GOODE, Lauren. **Software de reconhecimento facial é tendencioso para homens brancos, pesquisa descobre**. 2018. The Verge. Acesso em 31 maio 2025. Disponível em https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error.

PASQUALE, Frank A. **The Black Box Society: The Secret Algorithms That Control Money and Information.** Cambridge, MA: Harvard University Press, 2015. 319-320 p. ISBN 978-0674368279

SILVA, Isabela Maria Soares; BARBOSA, Letícia Mendes. Inov(ação): discriminação algorítmica racial e as inteligências artificiais no Brasil. **Revista do CAAP**, Belo Horizonte, v. 28, n. 2, p. 1–30, 2024. DOI: 10.69881/rcaap.v28i2.49200. Disponível em: https://periodicos.ufmg.br/index.php/caap/article/view/49200. Acesso em: 30 maio. 2025.