



Anais do Encontro Anual
da Rede de Pesquisa em
Governança da Internet
Maio de 2025

VIII ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET - REDE 2025

FICHA TÉCNICA

ANAIIS DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET-VOL. 8, ISSN 2675-1690

Editora

Kimberly Anastácio

Autoras (es)

Amanda Cunha e Mello Smith
Martins
Bianca Galvão Marques
Carla Alessandra Marques
Cinthia Obladen de Almendra
Freitas
Diná Santana Santos
Elizabeth Machado Veloso
João Pedro Bueno Ghizelini
José Humberto Fazano Filho
Pietra Milani Bizerril
Tatiana Nascimento Heim
Thiago Novaes

COMITÊ ORGANIZADOR

Núcleo de Coordenação da Rede de Pesquisa em Governança da Internet

Alexandre Arns Gonzales
Carolina Batista Israel
Diego Vicentin
Fernanda R. Rosa
Hemanuel Jhosé Alves Veras
Kimberly Anastácio
Maria Vitoria Pereira de Jesus
Nahema Falleiros
Nathan Paschoalini Ribeiro Batista
Rodolfo Avelino

Comitê Científico

Adriana Espindola
Alcides Peron
Alexandre Arns Gonzales
Ana Paula Camelo
Carolina Batista Israel
Diego Vicentin
Edson Spina
Fernanda Rosa
Flávio Wagner
Gills Villar-Lopes
Leonardo Cruz

Marta Kanashiro
Monica Arroyo
Nahema Falleiros
Rafael Dias
Rodolfo Avelino
Rodrigo Firmino

Moderadoras (es)

Carolina Batista Israel
Hemanuel Jhosé Alves Veras
Nahema Falleiros
Rodolfo Avelino

Debatedoras (es)

Alcides Eduardo dos Reis Peron
Amanda Cunha e Mello Smith
Martins
André Fernandes
Bianca Galvão Marques
Carla Alessandra Marques
Diná Santana Santos
Elizabeth Machado Veloso
Mariana Soares
Messias Guimarães
Nina da Hora
Pietra Milani Bizerril
Tatiana Nascimento Heim
Thiago Novaes

O VIII Encontro da Rede de Pesquisa em Governança da Internet e a publicação dos Anais resultantes deste encontro receberam apoio de: Comitê Gestor da Internet no Brasil - CGI.br, Internet Society - Capítulo Brasil e do Programa de Pós-graduação em Ciências Sociais da Universidade Estadual de Campinas (Unicamp), através de recursos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).



PREDIÇÃO CRIMINAL E INTELIGÊNCIA ARTIFICIAL: IMPLICAÇÕES JURÍDICAS E ÉTICAS

TATIANA NASCIMENTO HEIM E CINTHIA OBLADEN DE ALMENDRA FREITAS

SUMÁRIO

INTRODUÇÃO.....	5
DEFINIÇÃO DE INTELIGÊNCIA ARTIFICIAL.....	7
DEFINIÇÃO DE POLICIAMENTO PREDITIVO E SUAS ETAPAS	10
IMPLICAÇÕES E DESAFIOS DO USO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL NO POLICIAMENTO PREDITIVO	14
CONCLUSÃO	16



PREDIÇÃO CRIMINAL E INTELIGÊNCIA ARTIFICIAL: IMPLICAÇÕES JURÍDICAS E ÉTICAS

Tatiana Nascimento Heim¹

Cinthia Obladen de Almendra Freitas²

RESUMO

O desejo de prever o comportamento humano permeia diversas áreas da sociedade, incluindo a segurança pública. No contexto da segurança pública, a inteligência artificial é empregada para prever e prevenir crimes, incluindo a identificação de possíveis perpetradores. Dentre os benefícios desse uso, destacam-se a otimização de recursos, melhoria da eficiência operacional e a possibilidade de reduzir discriminações. O artigo analisa os desafios éticos e legais relacionados ao uso de sistemas de inteligência artificial (IA) na previsão de crimes, com especial atenção à identificação de possíveis perpetradores. A partir de uma abordagem dedutiva e de revisão bibliográfica, o estudo discute como a aplicação de modelos preditivos pode contribuir para a eficiência da segurança pública, ao mesmo tempo em que suscita preocupações quanto à transparência, responsabilização e respeito aos direitos fundamentais. Observa-se que a opacidade dos algoritmos, a possibilidade de discriminação algorítmica e os efeitos assimétricos de erros preditivos representam riscos relevantes à legitimidade das decisões automatizadas. Argumenta-se que métodos baseados em regressão, por operarem com valores contínuos, podem oferecer alternativas mais adequadas à classificação binária, desde que acompanhados de salvaguardas éticas e jurídicas. Conclui-se que a implementação responsável de sistemas de IA na segurança pública exige supervisão contínua, regulamentação apropriada e um diálogo interdisciplinar entre tecnologia, direito e sociedade.

PALAVRAS-CHAVE: Policiamento preditivo; sociedades; novas tecnologias; inteligência artificial; ética

¹ Pós-doutoranda no Programa de Pós-Graduação em Direito (PPGD) em Direito da Pontifícia Universidade Católica do Paraná (PUCPR), com pesquisa voltada à previsão de crimes e inteligência artificial. Doutora em regulação de cibersegurança pela Universidade de Twente, na Holanda. Bolsista da CAPES. Advogada. E-mail: tatiana.heim@gmail.com

² Doutora em Informática Aplicada pela Pontifícia Universidade Católica do Paraná (PUCPR). Professora Titular do Programa de Pós-Graduação em Direito (PPGD) da Escola de Direito da PUCPR. Membro Consultivo da Comissão de Proteção de Dados da OAB/PR. E-mail: cinthia@pucpr.br

ABSTRACT

The desire to predict human behavior permeates various areas of society, including public security. In this context, artificial intelligence (AI) is employed to anticipate and prevent crimes, including the identification of potential perpetrators. Among the benefits of such use are resource optimization, improved operational efficiency, and the potential to reduce discrimination. This article analyzes the ethical and legal challenges related to the use of AI in crime prediction, with particular focus on the identification of possible offenders. Based on a deductive approach and literature review, the study discusses how predictive models may enhance the effectiveness of public security strategies, while also raising concerns about transparency, accountability, and the protection of fundamental rights. It is observed that algorithmic opacity, the risk of discriminatory outcomes, and the asymmetrical effects of prediction errors pose significant threats to the legitimacy of automated decisions. The article argues that regression-based methods, which operate with continuous values, may offer more suitable alternatives to binary classification, provided they are accompanied by ethical and legal safeguards. The study concludes that the responsible implementation of AI in public security requires ongoing oversight, appropriate regulation, and interdisciplinary dialogue among technology, law, and society.

KEY WORDS: Predictive policing; artificial intelligence; ethics

INTRODUÇÃO

A sociedade atual é guiada por dados. Ferramentas computacionais baseadas em dados processam, recuperam, organizam e geram informações, podendo até mesmo influenciar a tomada de decisões seja no setor público ou privado. Tem-se modelos baseados em algoritmos e dados que servem de apoio à tomada de decisão tanto para gestão quanto organização social, de modo que tais modelos têm por fundamento análises probabilísticas que permitem a identificação de padrões que podem ser associados a riscos. O risco, por sua vez, pode ser gerenciado, mitigado e redistribuído entre diferentes instituições, estabelecendo uma tomada de decisão, por exemplo, compartilhada (BLOUNT, 2023).

De acordo com Mackenzie (2015), vive-se imerso ao "desejo de prever" - que consiste na tentativa de compreender o comportamento humano e antecipar suas ações. Técnicas de Inteligência Artificial, tais como Aprendizagem de Máquina (*Machine Learning*) tornam-se ferramentas importantes nesse procedimento, utilizadas para prever comportamentos, preferências e ações de indivíduos ou grupos (MACKENZIE, 2015). Esse anseio de previsão se estende a todas as esferas da sociedade, incluindo a segurança pública.

Diante desse cenário, surgem novas abordagens tecnológicas para combater e prevenir a criminalidade. Entre essas inovações, destaca-se o uso de métodos e técnicas de Inteligência Artificial (IA) para prever padrões criminais e aprimorar a eficiência das forças de segurança. Modelos como o policiamento preditivo e o policiamento orientado por inteligência enfatizam a especialização, a eficiência e o uso de táticas cientificamente comprovadas, baseadas em análises de grandes volumes de dados quantitativos (JUNIOR, 2022).

A ideia de prever crimes e identificar criminosos antes que o delito ocorra não é nova e encontra paralelo na ficção científica, como no filme "*Minority Report*", baseado na obra de Philip K. Dick. No filme, em que um sistema avançado antecipa delitos antes de sua concretização, permitindo a intervenção policial antecipada (SARKAR, 2002). Embora ainda distantes desta realidade distópica, as tecnologias baseadas em IA aplicadas à segurança pública vêm se tornando cada vez mais sofisticadas, influenciando estratégias de policiamento preditivo e orientado por inteligência.

A utilização de modelos estatísticos na segurança pública pode contribuir para a redução de crimes. Nos Estados Unidos, alguns exemplos ilustram essa aplicação. Um exemplo, frequentemente citado ocorreu em 2003, o Departamento de Polícia de Richmond utilizou dados históricos para prever onde haveria disparos de armas de fogo na véspera de Ano Novo. Com base nessas previsões, os trajetos das patrulhas foram ajustados, resultando em uma redução de 47% nos disparos aleatórios, um aumento de 246% na apreensão de armas (MUGARI, 2021).

Nesse contexto, métodos e técnicas de IA podem potencializar a utilização de grandes volumes de dados, extraídos de repositórios institucionais e outras fontes, para estimar a probabilidade de crimes específicos (JUNIOR, 2022). O lado negativo do uso de sistemas de IA na predição de crimes está ligado a preocupações morais, éticas, falhas de tecnologia e aumento de custos (KAUFMANN, 2024). Ademais, a grande quantidade de coleta de dados também traz uma preocupação com a proteção de dados pessoais.

O policiamento preditivo pode prever quando e onde é mais provável que o crime venha a ocorrer até quem tem mais probabilidade de se envolver em atividades criminosas. O objetivo deste artigo é entender quais dilemas éticos e jurídicos podem emergir da aplicação de sistemas de Inteligência Artificial na predição de crimes.

O método de pesquisa adotado foi o dedutivo, que parte de teorias e conceitos existentes, para, a partir dessas fundamentações, chegar a novas conclusões ou *insights* sobre o tema em questão. A primeira etapa do processo metodológico consistiu em uma revisão de literatura detalhada, que envolveu a análise de estudos e publicações acadêmicas recentes e relevantes. Embora a pesquisa tenha um forte caráter teórico, a análise foi complementada com dados empíricos obtidos a partir de exemplos práticos. O artigo é resultado de projeto de pesquisa CAPES/PROCAD – SPCF (Segurança Pública e Ciências Forenses).

DEFINIÇÃO DE INTELIGÊNCIA ARTIFICIAL

A inteligência artificial (IA) possui diversas definições, que evoluíram conforme os avanços das pesquisas na área. O termo "inteligência artificial" foi cunhado por John McCarthy em 1955, no contexto de uma proposta para obter financiamento para uma escola de verão na Universidade de Dartmouth.³ O autor definiu a inteligência artificial como a ciência e a engenharia dedicadas ao desenvolvimento de máquinas e sistemas computacionais inteligentes. A principal finalidade da inteligência artificial seria replicar aspectos da inteligência humana (MCCARTHY, 2007). Essa concepção, de natureza antropocêntrica, enfatiza a simulação das habilidades mentais ou intelectuais humanas (WANG, 2019).

Seguindo esta linha de raciocínio, Alan Turing, em 1950, propôs o Teste de Turing, no qual um examinador interage com um computador por meio de perguntas e considera a máquina inteligente se não conseguir distinguir se as respostas provêm de um ser humano ou de uma máquina (RUSSEL, 2016). Tanto a definição de McCarthy quanto o Teste de Turing são marcos iniciais nas pesquisas de IA baseadas na premissa de que os sistemas computacionais poderiam replicar o funcionamento da mente humana.

No entanto quando se compara o cérebro humano com sistemas de AI se assume que a inteligência artificial pode alcançar uma estrutura semelhante à do cérebro composta por unidades de processamento que se assemelham aos neurônios (WANG, 2008). A crítica a estas definições se baseia no fato de que o cérebro humano

³ "It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable" (MCCARTHY, 2007, p. 2).

é extremamente complexo, e o avanço depende diretamente dos avanços na neurociência, o que torna esse progresso desafiador. Além disso, definir inteligência exclusivamente em termos de inteligência humana pode limitar o desenvolvimento da área. Por exemplo, a diferença entre desenvolver um *design* para "voar" ou "voar como um pássaro" faz refletir como a concepção de sistemas complexos. A segunda abordagem pode limitar a inovação, excluindo propostas que, embora eficazes, não reproduzem fielmente o modelo natural (WANG, 2019).

Além disso, o conceito de inteligência humana transformou-se ao longo do tempo, especificamente impulsionado pelo avanço da tecnologia. Por exemplo, no passado, a capacidade de se jogar xadrez era considerado o ápice da inteligência humana. No entanto, atualmente, após inúmeras pesquisas que levaram à vitória de sistemas de inteligência artificial sobre humanos, o xadrez deixou de ser um parâmetro definitivo de inteligência (TOOSI, 2021). Com o passar do tempo a inteligência artificial afastou-se da ideia antropocêntrica, focando no ideal de racionalidade (RUSSELL, 2016). Essa dimensão de racionalidade está vinculada a uma tendência que emergiu nos anos 1980, a qual se concentra em aspectos específicos da área de IA (TOOSI, 2021).

Nessa fase surge o conceito de Inteligência Artificial Fraca (*Weak or Narrow AI*), que tem como foco a realização de tarefas ou aplicações específicas. Exemplos disto incluem sistemas de diagnóstico médico, que auxiliam na identificação de doenças; carros autônomos, que utilizam IA para navegação; assistentes virtuais, que reconhecem comandos de voz; e software de análise financeira, como os utilizados por bancos para detecção de fraudes (GOERTZEL, 2019). Essa transição representou uma mudança de perspectiva, passando de sistemas que buscavam imitar o funcionamento do cérebro humano para modelos computacionais altamente especializados na resolução de problemas específicos (WANG, 2018).

A IA passou então a ser definida pelo conjunto de métodos que dela derivam, abrangendo provas de teoremas (*Theorem Proving*), busca heurística (*Heuristic Search*), redes neurais (*Neural Networks*), redes bayesianas (*Bayesian Networks*), mineração de dados (*Data Mining*) e aprendizado profundo (*Deep Learning*). Estes métodos são fundamentados em diferentes teorias e são aplicáveis a um ou mais ramos da IA. Assim muitos pesquisadores tendem a se identificar mais com esses ramos do que com o conceito amplo de IA (WANG, 2021; MAAS, 2021; PENNACHIN *et al.*, 2007). Essas tarefas distinguem-se de automação tradicional, uma vez que, demandam pro-

cessos cognitivos superiores, como raciocínio, estratégia, planejamento e tomada de decisão, características intrínsecas à inteligência humana (FREITAS, 2024).

No entanto, essa abordagem também é alvo de críticas por se distanciar do ideal de criar máquinas verdadeiramente pensantes, reduzindo a inteligência artificial à construção de ferramentas inteligentes. Marvin Minsky, respondendo a entrevista realizada pelo jornalista, argumentou que, desde a década de 1970, a área enfrenta um estancamento, uma vez que os computadores ainda carecem de senso comum. Embora a IA seja amplamente utilizada para tarefas, ela permanece incapaz de interpretar o contexto ao seu redor ou de engajar-se em diálogos significativos sobre experiências vividas. Esta limitação restringe sua eficácia em situações que demandam uma compreensão mais profunda e contextualizada, evidenciando os desafios ainda presentes no desenvolvimento de sistemas verdadeiramente inteligentes (MCHUGH, 2003).

Novos conceitos de IA vem surgindo com o objetivo de desenvolver sistemas computacionais capazes de replicar as funções cognitivas da mente humana (NATALE *et al*, 2020). O pressuposto seria que na IA Fraca (*Weak AI*) quando há uma alteração, no contexto ou na especificação do comportamento, esses sistemas geralmente requerem algum nível de reprogramação ou reconfiguração humana para manter seu desempenho. Isso contrasta fortemente com sistemas naturalmente inteligentes, como os humanos, que possuem uma ampla capacidade de adaptação a mudanças em seus objetivos ou circunstâncias. Desta forma, o conceito de "Inteligência Artificial Geral" (*General-purpose Artificial Intelligence* – GAI) surgiu como o oposto da IA Fraca (*Weak AI*), referindo-se aos sistemas capazes de estabelecer generalizações em contexto amplo (GOERTZEL, 2014).

Ademais, outro conceito está aqui relacionado, é o conceito de IA Forte que define como objetivo computadores serem máquinas pensante equivalentes a uma mente humana (NATALE *et al*, 2020). A diferença entre agir de acordo como a mente humana e replicar funções cognitivas humanas reside na mesma linha de raciocínio trazida anteriormente sobre a diferença entre “voar” e “voar como um pássaro”. Embora seja possível simular a mente humana - objeto da Inteligência Artificial Geral -, para agir de forma verdadeiramente humana, seria necessário a experiência social mediada pela comunicação. Em outras palavras, a máquina precisaria ser reconhecida e tratada por outros (humanos e outras máquinas) como um ser humano, algo extremamente difícil de se alcançar na prática (WANG, 2018).

Considerando todas as discussões e definições apresentadas, este artigo adota uma concepção ampla de Inteligência Artificial. Essa definição não restringe a IA a uma única tecnologia, mas a compreende como um termo guarda-chuva, abrangendo diversos ramos, métodos, técnicas e aplicações. Além disso, reconhece que o conceito de IA está em constante evolução, adaptando-se aos avanços tecnológicos e contextuais. Por fim, essa perspectiva não equipara a IA à mera imitação da inteligência humana, mas a entende como um campo dinâmico e multifacetado, capaz de transcender essa comparação. Esse conceito é extraído pelo Grupo de Peritos de Alto Nível em Inteligência Artificial da Comissão Europeia, como apresentado e discutido por FREITAS (2024, p. 5):

O conceito de inteligência artificial (IA) aplica-se a sistemas que apresentam um comportamento inteligente, analisando o seu ambiente e tomando medidas —com um determinado nível de autonomia— para atingir objetivos específicos. Os sistemas baseados em inteligência artificial podem estar puramente confinados ao “software”, atuando no mundo virtual (por exemplo: assistentes de voz, programas de análise de imagens, motores de busca, sistemas de reconhecimento facial e de discurso), ou podem estar integrados em dispositivos físicos (por exemplo: robôs avançados, automóveis autônomos, veículos aéreos não tripulados ou aplicações da Internet das coisas) (HLEG, 2019).⁴

É importante destacar que este conceito se refere à Inteligência Artificial Fraca. Ele é adotado neste artigo, pois a expressão “sistemas de IA” diz respeito a qualquer componente que utilize métodos e técnicas de IA em sua estrutura. Nesse contexto, sistemas de IA envolvem tanto programas de computador (software) quanto componentes físicos (*hardware*). No entanto, o que realmente define um sistema de IA não é o processamento realizado pelo *hardware*, mas sim a escolha dos métodos e técnicas aplicadas para resolver um problema específico (FREITAS, 2024, p. 6).

DEFINIÇÃO DE POLICIAMENTO PREDITIVO E SUAS ETAPAS

O policiamento preditivo é um termo guarda-chuva que engloba uma variedade de técnicas e processos com a finalidade prevenir, responder e fazer previsões sobre a ocorrência de crimes (MCDANIEL, 2021). A polícia preditiva pode ser entendida como a coleta e análise de dados sobre crimes para identificar e fazer previsões estatísticas sobre indivíduos ou áreas geoespaciais com maior probabilidade de atividade criminal,

⁴ HLEG - High-Level Expert Group on Artificial Intelligence. A definition of AI: Main capabilities and scientific disciplines. European Commission, Brussels, 2019.

a fim de ajudar no desenvolvimento de estratégias e táticas de intervenção e prevenção policial (MEIJER et al, 2019). Trata-se do policiamento orientado pela inteligência, pois foca na prevenção em vez de se concentrar apenas nos eventos ocorridos (BACHNER, 2013).

Há várias vantagens de se utilizar o policiamento preditivo. A literatura indica que as principais vantagens são a otimização de recursos e aumento da eficiência. Ademais, a aplicação dessas ferramentas analíticas fortalece a capacidade das agências de segurança pública na tomada de decisões estratégicas, especialmente no que se refere ao deslocamento e à distribuição do efetivo policial (CHAN, 2016). Essa abordagem parte da premissa de que tanto criminosos quanto vítimas seguem padrões de comportamento recorrentes, os quais podem indicar tendências criminais. Além disso, fatores como localização geográfica e temporal desempenham um papel fundamental na dinâmica criminal, pois influenciam diretamente as decisões dos infratores em relação à escolha do local, do alvo e à avaliação do risco de captura (PERRY, 2013).

Em termo gerais, a criminologia se baseia a ideia de previsão de crimes na premissa de que tanto criminosos quanto vítimas exibem padrões comportamentais recorrentes, essa metodologia busca identificar tendências criminais e otimizar as ações preventivas (PERRY, 2013). Dentro desse viés teórico o policiamento preditivo pode ser entendido como a coleta e análise de dados criminais para identificar padrões e fazer previsões estatísticas sobre indivíduos ou áreas geoespaciais (MEIJER, 2019). Mugari *et al* argumenta que dado o avanço tecnológico o conceito de previsão criminal precisa capturar a essência das novas ferramentas e métodos disponíveis. Portanto, sugere que o conceito de policiamento preditivo seja entendido como um modelo de policiamento que utiliza dados históricos de crimes e dados sociodemográficos de fontes diversas para prever crimes futuros, por meio de aplicativos computacionais sofisticados (MUGARI, 2021). Trata-se de um modelo de policiamento orientado pela inteligência, que prioriza a prevenção em vez de se concentrar apenas nos eventos ocorridos (BACHNER, 2013).

O policiamento preditivo pode ser categorizado em quatro tipos principais, conforme o objeto da previsão. A primeira categoria envolve métodos destinados a identificar locais e horários com maior probabilidade de ocorrência de crimes, com base na análise de padrões históricos. A segunda refere-se à previsão de ofensores, ou seja, à identificação de indivíduos com maior propensão a cometer delitos futuros. A terceira

categoria abrange técnicas voltadas à inferência da identidade de perpetradores de crimes já ocorridos, por meio da correlação de dados contextuais e comportamentais. Por fim, a quarta categoria contempla métodos que buscam determinar pessoas ou grupos com maior risco de vitimização, possibilitando a adoção de medidas preventivas mais eficazes (PERRY, 2013).

Em comparação com as previsões espaço-temporais de crimes, os métodos voltados para a identificação de indivíduos ainda são muito menos desenvolvidos (PERRY, 2013). Enquanto modelos estatísticos e algoritmos já conseguem apontar com relativa precisão onde e quando crimes podem ocorrer, prever quem os cometerá continua sendo um desafio significativamente maior. De acordo com Ferguson (2017), os programas voltados à predição de perpetradores não derivaram diretamente da lógica do policiamento preditivo tradicional, mas desenvolveram-se de forma paralela, influenciados por modelos de saúde pública (FERGUSON, 2017). A predição da identidade de perpetradores visa identificar indivíduos com maior probabilidade de cometer crimes no futuro ou de ter cometido crimes no passado (PERRY, 2013).

O policiamento preditivo consiste na coleta e análise de dados criminais com a finalidade de identificar padrões e realizar previsões estatísticas sobre atividades criminais em áreas geográficas ou indivíduos com maior propensão ao envolvimento em atividades criminosas. Mugari *et al.* (2021, p. 4) enfatizam que, diante do avanço tecnológico, é imprescindível que o conceito de previsão criminal acompanhe a complexidade e a sofisticação das ferramentas e métodos atualmente disponíveis. Assim, o policiamento preditivo é compreendido como um modelo de atuação baseado em dados históricos e sociodemográficos oriundos de fontes diversas, com vistas à antecipação de delitos mediante o uso de sistemas computacionais (MUGARI *et al.*, 2021, p.6). Tal abordagem desloca o foco reativo tradicional para uma atuação preventiva e baseada em inteligência.

A análise preditiva, em termos simplificados, visa transformar dados pretéritos em informações relevantes para a tomada de decisões em tempo real e para a previsão de eventos futuros (BACHNER, 2013, p. 9), valendo-se de conhecimentos provenientes de áreas como estatística, matemática e ciência da computação (HAN; PEI; TONG, 2000, p. 23). Tradicionalmente, os processos preditivos envolviam análise manual de dados, com foco em riscos localizados. A IA, entretanto, permite que essas análises sejam realizadas de forma mais rápida, eficiente e em grande escala (MCDANIEL,

2021). Os modelos de IA, geralmente de escopo restrito, são adaptados conforme o tipo de crime, a natureza dos dados e os critérios adotados para previsão.

Segundo Freitas e Barddal (2019, p. 110), a análise preditiva fundamenta-se em técnicas de Aprendizagem de Máquina (*Machine Learning*), com algoritmos ajustados para tarefas específicas que envolvem a generalização. Esta é definida como a capacidade de um modelo extrair padrões subjacentes dos dados e aplicar esse conhecimento a dados não observados (FREITAS *et al*, 2019, p.110). O desempenho de modelos preditivos está diretamente relacionado à quantidade e à qualidade dos dados originais. Conforme Han, Kamber e Pei (2011, p. 5), o uso desses modelos se justifica em cenários nos quais: (a) o processamento manual é inviável diante do volume e da complexidade das regras, ou (b) é vantajosa a descoberta de padrões ainda desconhecidos nos dados.

A polícia preditiva pode ser dividida em três etapas principais: (1) coleta de dados de diferentes tipos, (2) aplicação de métodos algorítmicos para prever a ocorrência de crimes em determinado contexto e (3) uso das previsões pela polícia para embasar decisões estratégicas e táticas no campo (BRANTINGHAM, 2017).

A metodologia preditiva aplicada à segurança pública se baseia principalmente em dados empíricos, representando uma ruptura com abordagens tradicionais que focam na causalidade e formulação de hipóteses (MEIJER *et al*, 2019). Em vez de buscar compreender as causas individuais do crime, a ênfase está na identificação de padrões e correlações a partir de grandes volumes de dados (*big data*) (CUSTERS, 2021). Nesse contexto, os modelos estatísticos não realizam previsões determinísticas, mas sim estimam as probabilidades de ocorrência de delitos, o que exige conjuntos de dados extensos, precisos e limpos (ANDREJEVIC, 2017).

As principais fontes desses dados incluem históricos de crimes — como tipo, local, horário e perfil demográfico dos envolvidos — além de dados sociais complementares, como informações econômicas, demográficas e até interações em redes sociais (PERRY, 2013). O cruzamento dessas informações permite identificar correlações inesperadas, como demonstrado por Dario *et al.* (2015), que observaram aumento na atividade criminosa em Ventura, Califórnia, durante dias favoráveis ao surfe, especialmente no período da tarde (DARIO, 2015). A eficácia dos modelos, portanto, depende diretamente da qualidade dos dados utilizados, o que representa tanto um desafio técnico quanto uma vulnerabilidade operacional (PERRY, 2013).

Além dos dados, os algoritmos desempenham um papel central no policiamento preditivo. De acordo com Freitas (2021), um algoritmo é uma sequência finita de ações que podem ser executadas para resolver um determinado problema (FREITAS, 2021). No contexto da polícia preditiva, os algoritmos seguem uma metodologia analítica estruturada: processam automaticamente grandes volumes de dados históricos para identificar variáveis estatisticamente correlacionadas a desfechos específicos, como homicídios ou reincidência criminal (HAMILTON, 2021).

Os fatores com maior capacidade preditiva são selecionados e ponderados, resultando em uma equação algorítmica que orienta o modelo. A evolução desses sistemas foi de regras simples e associações binárias para modelos mais sofisticados, como regressões estatísticas complexas e, mais recentemente, técnicas de aprendizado de máquina. Este último avanço é significativo, pois permite que os algoritmos melhorem sua performance à medida que acumulam experiência e processam continuamente novos dados (JENGA, 2023).

Após a coleta e análise dos dados, a aplicação prática das previsões enfrenta desafios relevantes que podem comprometer sua eficácia. A implementação de tecnologias de inteligência artificial na polícia envolve dificuldades técnicas e institucionais, como a resistência cultural de agentes acostumados a métodos tradicionais, a falta de capacitação adequada e falhas operacionais que geram frustração entre os usuários. Além disso, o tempo necessário para adaptação e para que os resultados comecem a se concretizar pode alimentar percepções negativas dentro da própria corporação, especialmente diante do aumento da supervisão e das exigências de relatórios (KOPER, 2014). Nesse cenário, o engajamento ativo e o apoio contínuo da gestão tornam-se elementos cruciais para a consolidação e o sucesso das iniciativas preditivas.

IMPLICAÇÕES E DESAFIOS DO USO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL NO POLICIAMENTO PREDITIVO

No entanto, o uso crescente da IA no policiamento suscita importantes questões éticas e legais. Inicialmente é relevante distinguir os dois conceitos para compreensão do seu uso. A ética corresponde a sistemas internos de controle, estruturados a partir de princípios morais que regulam o comportamento da tecnologia e orientam a resolução de conflitos decorrentes de seu uso. O direito, por sua vez, consiste em mecanismos externos de imposição, definidos por normas e regulamentos elaborados

por autoridades competentes, com a finalidade de assegurar a conformidade legal no desenvolvimento e utilização da IA. Enquanto o direito se volta ao cumprimento obrigatório de deveres impostos, a ética busca assegurar que valores morais sejam incorporados às práticas que envolvem a inteligência artificial (QIAN, 2024). Ambas as esferas são complementares na busca por um uso justo e transparente da IA (KAUFMANN, 2024).

A transparência e a explicabilidade de algoritmos é um dos desafios. Muitos sistemas operam como "caixas-pretas" devido a sua opacidade, dificultando a compreensão de seus mecanismos decisórios (ALI *et al.*, 2023). A opacidade impede que previsões incorretas sejam identificadas, sem uma compreensão clara das causas sobre erros e incertezas. Modelos alternativos, como "caixas-brancas" ou "cinzas", podem auxiliar e mitigar a opacidade, mas ainda podem enfrentar obstáculos práticos significativos, o que reforça a complexidade de tais sistemas (HUNG, 2021).

A responsabilização (*accountability*) é outro aspecto relevante. A complexidade dos sistemas de IA levanta dúvidas sobre quem deve responder por danos, se os desenvolvedores, operadores, usuários ou outros agentes envolvidos. Para isso, mecanismos institucionais devem ser criados, assegurando rastreabilidade das decisões e condições de responsabilização e reparação (GORAM, 2021; SIAU *et al.*, 2020).

Outros desafios cruciais referem-se ao viés (*bias*) e à discriminação algorítmica. Os algoritmos podem reproduzir e intensificar preconceitos existentes nos dados de treinamento, gerando decisões discriminatórias. Estes vieses decorrem tanto de problemas técnicos — como a representatividade inadequada dos dados — quanto de questões estruturais associadas às desigualdades sociais preexistentes. A mitigação do viés algorítmico requer práticas éticas de governança de dados, testes contínuos de equidade e correção dos parâmetros modelados (GORAM, 2021; SIAU *et al.*, 2020; KAUFMAN, 2021; JUNIOR, 2023; NUNES, 2023; NAH, 2024).

No tocante à privacidade os modelos preditivos exigem conformidade com legislações de proteção de dados pessoais. A predição de crimes, de forma geral, depende do tratamento massivo de dados pessoais e sensíveis, o que pode resultar em vazamentos ou vigilância excessiva de indivíduos, inclusive levando ao afastamento de cidadãos dos serviços públicos (GORAM, 2021).

A implementação de sistemas de IA na área policial enfrenta resistências institucionais, falta de capacitação e dificuldades técnicas (KOPER *et al.*, 2014, p. 215). Isso

inclui a resistência cultural de oficiais que podem ter preferência por métodos tradicionais, problemas técnicos que podem causar frustração entre os usuários e a falta de treinamento adequado. Frequentemente, é necessário um período de adaptação antes que resultados positivos se manifestem, o que pode intensificar a percepção negativa pelos próprios policiais devido ao aumento da supervisão e das exigências de relatórios (KOPER *et al.*, 2014, p. 215-218). Além disso, a ênfase no uso exclusivo de sistemas de IA de métodos altamente técnicos pode reforçar a imagem da polícia como especialistas científicos, em vez de agentes acessíveis à comunidade. Portanto, é importante o equilíbrio entre as perspectivas tecnológica e humana (BACHNER, 2013).

Do ponto de vista técnico, também é necessário ponderar o possível custo social associado à aplicação de modelos preditivos. Quando um modelo preditivo classifica indivíduos em categorias binárias, como "alto risco" ou "baixo risco" de cometer crimes, pode-se aplicar uma função de perda simétrica, que trata igualmente falsos positivos e negativos (BERK, 2011). Normalmente, este tipo de simetria não é aplicável em sistemas complexos, a exemplo de políticas públicas de segurança. No entanto, se utilizadas tais classificações podem acarretar consequências assimétricas. Por exemplo, um falso positivo — rotular indevidamente alguém como de "alto risco" — pode gerar efeitos como vigilância excessiva, estigmatização e violação de direitos. Já um falso negativo — deixar de identificar um risco elevado — pode resultar na não prevenção de um crime (BERK, 2010). Para lidar com esta assimetria pode se utilizar modelos baseados em regressão (*random forest*) que permite ajustar esses erros: ele superestima os casos de risco (aumenta os falsos positivos) para garantir que erros mais graves — os falsos negativos — sejam minimizados (BERK, 2010).

CONCLUSÃO

A aplicação de sistemas de Inteligência Artificial na previsão criminal representa um avanço significativo na forma como a segurança pública pode ser planejada e executada. Observou-se que, embora os modelos preditivos possam oferecer ganhos em eficiência e otimização de recursos na segurança pública, seu uso também está associado a riscos decorrentes, por exemplo, da opacidade de algoritmos, possibilidade de discriminação algorítmica e impactos assimétricos decorrentes de erros preditivos.

Além dos desafios técnicos, o uso de IA em contextos policiais suscita importantes preocupações éticas e jurídicas. A ausência de transparência nos sistemas de IA

compromete a legitimidade das decisões automatizadas, dificultando mecanismos de auditoria e responsabilização. Da mesma forma, o uso de bases de dados enviesadas ou mal estruturadas pode intensificar desigualdades sociais já existentes, especialmente em contextos nos quais a classificação de indivíduos em categorias de risco influencia a alocação de ações policiais. O artigo também destacou que, em vez de classificações dicotômicas, modelos que operam com valores contínuos, como os de regressão, tendem a oferecer maior precisão e flexibilidade para o apoio à tomada de decisão. Ainda assim, esses modelos também devem estar ancorados em princípios éticos claros, legislação adequada e participação ativa da sociedade civil.

Frente a esse cenário, a adoção de sistemas de IA no policiamento deve ser guiada por princípios de governança ética, respeito aos direitos fundamentais e participação social. Também se faz necessário fomentar a capacitação técnica e ética dos agentes envolvidos, bem como incentivar o desenvolvimento de modelos mais explicáveis e passíveis de controle público.

Dessa forma, conclui-se que a aplicação de sistemas de IA na previsão criminal requer uma abordagem cautelosa, multidisciplinar e continuamente supervisionada. A efetividade destas tecnologias está condicionada não apenas à sua sofisticação técnica, mas principalmente ao modo como são concebidas, aplicadas e reguladas. Somente mediante um equilíbrio entre inovação tecnológica e salvaguardas ético-jurídicas será possível promover uma segurança pública mais justa, eficiente e compatível com os direitos fundamentais.

REFERÊNCIAS

ALI, Sajid *et al.* Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence. **Information Fusion**, v. 99, p. 101-805, 2023.

ANDREJEVIC, Mark. Digital citizenship and surveillance| To Pre-empt a thief. **International Journal of Communication**, v. 11, p. 18-18, 2017.

BACHNER, Jennifer. Predictive policing: preventing crime with data and analytics. IBM Center for the Business of Government, Washington, 2013.

BERK, Richard. Asymmetric loss functions for forecasting in criminal justice settings. **Journal of Quantitative Criminology**, v. 27, p. 107-123, 2011.

BRANTINGHAM, P. Jeffrey. The logic of data bias and its impact on place-based predictive policing. **Ohio St. J. Crim. L.**, v. 15, p. 473, 2017.

BLOUNT, Kelly. **Applying Existing Legal Frameworks to Predictive Policing with Artificial Intelligence: Gaps, Tensions, and Individual Harms**. University of Luxembourg, Luxembourg, 2023. Disponível em: <https://orbilu.uni.lu/handle/10993/60344> . Acesso 10 março 2025.

CHAN, Janet; BENNETT MOSES, Lyria. Is big data challenging criminology?. **Theoretical criminology**, v. 20, n. 1, p. 21-39, 2016.

CUSTERS, Bart. Profiling and predictions: challenges in cybercrime research datafication. **Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches**, p. 63-79, 2021.

DARIO, Lisa M. et al. **The point break effect: an examination of surf, crime, and transitory opportunities**. *Criminal Justice Studies*, v. 28, n. 3, p. 257-279, 2015.

FREITAS, Cinthia Obladen. O Direito e a Inteligência Artificial como não-Coisa. **Conpedi Law Review**, v. 10, n. 1, 2024.

FREITAS, Cinthia Obladen de Almendra; BARDDAL, Jean Paul. Análise preditiva e decisões judiciais: controvérsia ou realidade? **Revista Democracia Digital e Governo Eletrônico**, Florianópolis, v. 1, n. 18, p. 107-126, 2019. p. 110.

FREITAS, Cinthia Obladen de Almendra. **A obscuridade dos algoritmos e a revisão da tomada de decisão automatizada diante de segredos comerciais e industriais**. In: WACHOWICZ, Marcos; CORTIANO, Marcelle. (Org.). **Sociedade informacional & propriedade intelectual**. 1. ed. Curitiba: GEDAI Publicações/UFPR, 2021. v. 1, p. 221-245.

MCHUGH, Josh. *Why A.I. is brain-dead*. Wired, 20 ago. 2003. Disponível em: <https://www.wired.com/2003/08/why-a-i-is-brain-dead/>. Acesso em: 9 maio 2025.

GOERTZEL, Ben. Artificial general intelligence: concept, state of the art, and future prospects. **Journal of Artificial General Intelligence**, v. 5, n. 1, p. 1, 2014.

GOERTZEL, Ben. **Artificial general intelligence**. New York: Springer, 2007; SEARLE, John. Minds, Brains, and Programs. 1980; WANG, Pei. On defining artificial intelligence. **Journal of Artificial General Intelligence**, v. 10, n. 2, p. 1-37, 2019.

GORAM, Mandy; VEIEL, Dirk. Ethical Behavior and Legal Regulations in Artificial Intelligence (Part Two): Representation of Law and Ethics in Intelligent Systems. In: **Machine Law, Ethics, and Morality in the Age of Artificial Intelligence**. IGI Global Scientific Publishing, 2021. p. 27-46.

HAMILTON, Melissa. Predictive policing through risk assessment. In: **Predictive policing and artificial intelligence**. Routledge, 2021. p. 58-78.

HAN, Jiawei; PEI, Jian; KAMBER, Micheline. *Data Mining: Concepts and Techniques*. 3. ed. Amsterdam: Morgan Kaufmann, 2011.

HLEG - HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE. **A definition of AI: Main capabilities and scientific disciplines**. European Commission, Brussels, 2019.

HUNG, Tzu-Wei; YEN, Chun-Ping. On the person-based predictive policing of AI. **Ethics and Information Technology**, v. 23, p. 165-176, 2021.

JENGA, Karabo; CATAL, Cagatay; KAR, Gorkem. Machine learning in crime prediction. **Journal of Ambient Intelligence and Humanized Computing**, v. 14, n. 3, p. 2887-2913, 2023.

JUNIOR, Ilson Oliveira; DOS SANTOS, Franck Cione Coelho. **Inteligência Artificial e Policiamento Preditivo: Possibilidades de inovação tecnológica para a Polícia Militar do Paraná no enfrentamento aos crimes violentos contra o patrimônio com emprego de explosivos**. Brazilian Journal of Technology, v. 5, n. 1, p. 030-062, 2022.

JUNIOR, Claudio do Nascimento Mendonça; NUNES, Dierle José Coelho. Desafios e oportunidades para a regulação da inteligência artificial: a necessidade de compreensão e mitigação dos riscos da IA. **Revista Contemporânea**, v. 3, n. 07, p. 7753-7785, 2023.

KAUFMAN, Dora. Inteligência Artificial e os desafios éticos: a restrita aplicabilidade dos princípios gerais para nortear o ecossistema de IA. **PAULUS: Revista de Comunicação da FAPCOM**, v. 5, n. 9, 2021

KAUFMANN, Mareile. AI in policing and law enforcement. In: **Handbook on Public Policy and Artificial Intelligence**. Edward Elgar Publishing, 2024. p. 295-306.

KOPER, Christopher S.; LUM, Cynthia; WILLIS, James J. Optimizing the use of technology in policing: Results and implications from a multi-site study of the social, organizational, and behavioral aspects of implementing police technologies. **Policing: A Journal of Policy and Practice**, v. 8, n. 2, p. 212-221, 2014.

MACKENZIE, Adrian. The production of prediction: What does machine learning want? **European Journal of Cultural Studies**, v. 18, n. 4-5, p. 429-445, 2015.

MCCARTHY, John et al. What is artificial intelligence. 2007.

MAAS, Matthijs M. AI, **Governance Displacement, and the (De) Fragmentation of International Law**, 2021. Disponível em: <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3806624> , acesso em 20 fev 2025.

MCDANIEL, John LM; PEASE, Ken. **Predictive policing and artificial intelligence**. Routledge, Taylor & Francis Group, 2021.

MEIJER, Albert; WESSELS, Martijn. Predictive policing: Review of benefits and drawbacks. **International journal of public administration**, v. 42, n. 12, p. 1031-1039, 2019.

MUGARI, Ishmael; OBIOHA, Emeka E. Predictive policing and crime control in the

United States of America and Europe: Trends in a decade of research and the future of predictive policing. **Social Sciences**, v. 10, n. 6, p. 234, 2021.

NATALE, Simone; BALLATORE, Andrea. Imagining the thinking machine: Technological myths and the rise of artificial intelligence. **Convergence**, v. 26, n. 1, p. 3-18, 2020.

PENNACHIN, Cassio; GOERTZEL, Ben. Contemporary approaches to artificial general intelligence. *In*: GOERTZEL, B.; PENNACHIN, C. **Artificial general intelligence**. Berlin, Heidelberg: Springer, 2007. p. 1-30.

PERRY, Walt L. Predictive policing: The role of crime forecasting in law enforcement operations. **Rand Corporation**, 2013.

PERRY, Walt L.; SAUNDERS, Jessica; HUNT, Priscillia; HOLLYWOOD, John S. Predictions put into practice: A quasi-experimental evaluation of Chicago's predictive policing pilot. **Journal of Experimental Criminology**, v. 12, p. 347-371, 2016.

QIAN, Yuzhou; SIAU, Keng L.; NAH, Fiona F. Societal impacts of artificial intelligence: Ethical, legal, and governance issues. **Societal impacts**, v. 3, p. 100040, 2024.

RUSSELL, Stuart J.; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. Pearson, 2016.

SARKAR, Sameer P.; ADSHEAD, Gwen. What price security? A review of Steven Spielberg's Minority report. **Journal of the American Academy of Psychiatry and the Law Online**, v. 30, n. 4, p. 568-570, 2002.

SIAU, Keng; WANG, Weiyu. Artificial intelligence (AI) ethics: ethics of AI and ethical AI. **Journal of Database Management (JDM)**, v. 31, n. 2, p. 74-87, 2020.

TOOSI, Amirhosein et al. A brief history of AI: how to prevent another winter (a critical review). **PET clinics**, v. 16, n. 4, p. 449-469, 2021.

WANG, Pei. On defining artificial intelligence. **Journal of Artificial General Intelligence**, v. 10, n. 2, p. 1-37, 2019.

WANG, Pei. "What Do You Mean by" AI"?.*" AGI*. Vol. 171. 2008.

WANG, Pei; LIU, Kai; DOUGHERTY, Quinn. Conceptions of artificial intelligence and singularity. **Information**, v. 9, n. 4, p. 79, 2018.