

**XIV ENCONTRO INTERNACIONAL
DO CONPEDI BARCELOS -
PORTUGAL**

**GOVERNO DIGITAL, DIREITO E NOVAS
TECNOLOGIAS**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Napolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

G326

Governo digital, direito e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Ana Catarina Almeida Loureiro; Danielle Jacon Ayres Pinto; José Renato Gaziero Cella. – Barcelos, CONPEDI, 2025.

Inclui bibliografia

ISBN: 978-65-5274-207-0

Modo de acesso: www.conpedi.org.br em publicações

Tema: Direito 3D Law

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Internacionais. 2. Governo digital. 3. Direito e novas tecnologias. XIV Encontro Internacional do CONPEDI (3; 2025; Barcelos, Portugal).

CDU: 34



XIV ENCONTRO INTERNACIONAL DO CONPEDI BARCELOS - PORTUGAL

GOVERNO DIGITAL, DIREITO E NOVAS TECNOLOGIAS

Apresentação

No XIV Encontro Internacional do CONPEDI, realizado nos dias 10, 11 e 12 de setembro de 2025, o Grupo de Trabalho - GT “Governo Digital, Direito e Novas Tecnologias”, que teve lugar na tarde de 12 de setembro de 2025, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente no Instituto Politécnico do Cávado e do Ave - IPCA, em Barcelos, Portugal.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “Governo Digital, Direito e Novas Tecnologias”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. José Renato Gaziero Cella

INTELIGÊNCIA ARTIFICIAL NO POLICIAMENTO PREDITIVO: DESAFIOS ÉTICOS, JURÍDICOS E SOCIAIS EM PERSPECTIVA

ARTIFICIAL INTELLIGENCE IN PREDICTIVE POLICING: ETHICAL, LEGAL AND SOCIAL CHALLENGES IN PERSPECTIVE

Tatiana Nascimento Heim ¹
Cinthia Obladen de Almendra Freitas ²

Resumo

O desejo de prever o comportamento humano permeia diversas áreas da sociedade, incluindo a Segurança Pública. Neste contexto, a Inteligência Artificial é empregada para prever e prevenir crimes, incluindo a identificação de possíveis perpetradores. Dentre os benefícios, destacam-se a otimização de recursos, melhoria da eficiência operacional e a possibilidade de reduzir discriminações. No entanto, a previsão da identidade de perpetradores levanta desafios éticos e jurídicos, como o risco de vigilância excessiva e discriminação. Analisa-se os impactos de sistemas de Inteligência Artificial na predição criminal, focando na identificação de perpetradores. A pesquisa, baseada em revisão de literatura e abordagem dedutiva, conclui que prever perpetradores apresenta riscos jurídicos e sociais mais sensíveis do que os existentes na técnica de mapeamento geográfico de crimes, de modo que a qualidade dos dados é um fator essencial, visto que erros na coleta e no tratamento podem reforçar desigualdades e expor certos grupos a uma vigilância desproporcional. O artigo aponta desafios, dentre eles, a transparência dos algoritmos, frequentemente descritos como “caixas-pretas”, dificultando fiscalização e revisão de decisões. Assim, o policiamento preditivo pode perder eficácia à medida que intervenções alteram padrões criminais, tornando os dados históricos obsoletos. O uso excessivo dessa tecnologia sem uma base ética pode aprofundar desigualdades e prejudicar a relação entre polícia e comunidade. Portanto, transparência, padronização e supervisão contínua são essenciais para garantir uma aplicação justa e eficaz de sistemas de Inteligência Artificial, promovendo um modelo de segurança pública mais estratégico e equitativo.

including the identification of potential perpetrators. Among the benefits, the optimization of resources, improvement of operational efficiency and the possibility of reducing discrimination stand out. However, predicting the identity of perpetrators raises ethical and legal challenges, such as the risk of excessive surveillance and discrimination. The impacts of Artificial Intelligence systems on crime prediction are analyzed, focusing on the identification of perpetrators. The research, based on a literature review and a deductive approach, concludes that predicting perpetrators presents more sensitive legal and social risks than those existing in the geographic mapping technique of crimes, so that the quality of the data is an essential factor, since errors in collection and processing can reinforce inequalities and expose certain groups to disproportionate surveillance. The paper highlights challenges, among them, the transparency of algorithms, often described as black-boxes, making it difficult to monitor and review decisions. Predictive policing may therefore lose its effectiveness as interventions alter crime patterns, rendering historical data obsolete. The excessive use of this technology without an ethical basis may deepen inequalities and harm the relationship between police and the community. Therefore, transparency, standardization, and ongoing oversight are essential to ensure the fair and effective application of AI systems, promoting a strategic and equitable public security model.

Keywords/Palabras-claves/Mots-clés: Predictive policing, Ppublic security, Artificial intelligence, Law and new technologies, Societies

1 INTRODUÇÃO

O desejo de prever comportamentos humanos sempre permeou diversas áreas da sociedade, incluindo a Segurança Pública. Um exemplo remonta a 1829, quando um geógrafo italiano e um estatístico francês elaboraram os primeiros mapas que visualizavam dados criminais (Bachner, 2013).

Com o avanço das tecnologias da informação e a complexidade crescente dos conjuntos de dados, os sistemas computacionais se tornaram uma ferramenta relevante capaz de identificar padrões ocultos para prever condutas criminosas antes de sua ocorrência (Han *et al.*, 2012). Nesse contexto, surge o policiamento preditivo, entendido como um modelo orientado por inteligência que coleta e analisa dados criminais e sociodemográficos para identificar áreas ou indivíduos com maior propensão ao cometimento de crimes (Meijer; Wessels, 2019). Trata-se, portanto, de um modelo de policiamento orientado por inteligência, que prioriza a predição e, consequentemente, a prevenção em detrimento da reação aos eventos ocorridos.

Entre seus benefícios estão a otimização de recursos, a eficiência operacional (Chan; Moses, 2016), a prevenção de discriminações (Selbst, 2017) e o fortalecimento institucional por meio da tomada de decisões estratégicas e alocação de efetivo policial (Chan; Moses, 2016). A flexibilidade e adaptabilidade também se destacam, visto que os sistemas podem ser atualizados com novos dados, mantendo políticas e decisões alinhadas com contextos dinâmicos (Abramowicz, 2006). As técnicas preditivas também podem contribuir para a legitimidade institucional (Koper *et al.*, 2014), uma vez que podem aprimorar a comunicação entre a polícia e os cidadãos e reduzir os efeitos colaterais negativos da atuação policial. Por fim, o uso de técnicas de predição impulsiona a inovação institucional (Abramowicz, 2006), estimulando o desenvolvimento de novas tecnologias e métodos para aprimorar a acurácia das previsões e promover avanços sistêmicos.

Adota-se uma concepção ampla de Inteligência Artificial (IA), compreendendo-a como sistemas computacionais, que demonstram comportamento inteligente com certo grau de autonomia. Adota-se, especificamente, a noção de Inteligência Artificial Fraca, focada em aplicações específicas por meio de técnicas computacionais voltadas à resolução de problemas específicos (HLEG, 2019).

Embora a IA tenha contribuído significativamente para o aprimoramento do policiamento preditivo, sua utilização também suscita importantes questões de ordem ética e legal. Assim, torna-se fundamental examinar não apenas os potenciais benefícios, mas também as implicações e os limites da aplicação de sistemas de IA neste contexto. Diante disso, este

artigo tem como objetivo examinar os benefícios e os desafios éticos, legais e sociais na aplicação de sistemas de IA na predição de crimes.

É importante frisar que na maior parte das vezes, os modelos de IA utilizados são de escopo restrito, o que resulta em uma variedade de modelos e aplicações específicas, que variam conforme a categoria do crime, os dados disponíveis e os critérios de previsão adotados (Kaur; Saini, 2024). Portanto, inicialmente, é necessário compreender como a predição criminal está estruturada. Isso é importante, em primeiro lugar, para identificar em quais pontos do processo preditivo incidem os principais desafios éticos e jurídicos; em segundo lugar, para avaliar com precisão qual é a contribuição efetiva dos sistemas de IA nesse contexto; e, por fim, para analisar criticamente se os objetivos de eficiência e prevenção são de fato alcançados ou se os modelos adotados geram novos problemas institucionais.

Metodologicamente, este artigo baseia-se em revisão de literatura e análise de conteúdo. Na primeira seção, examinam-se as implicações éticas da aplicação de sistemas de IA no policiamento preditivo a partir de publicações acadêmicas recentes e relevantes. Na sequência, busca compreender como está estruturado o policiamento preditivo, também com base em revisão bibliográfica. Para interpretar criticamente os dados textuais coletados, empregou-se a técnica de análise de conteúdo conforme sistematizada por Laurence Bardin (2011), que propõe a organização do material em categorias de sentido construídas com base nos critérios de exclusividade, exaustividade e relevância. Por fim, são integrados os principais achados teóricos e empíricos, com vistas a alcançar o objetivo geral. O artigo é resultado de projeto de pesquisa financiado pelo PROCAD – SPCF (Segurança Pública e Ciências Forenses) da CAPES.

2 IMPLICAÇÕES ÉTICAS, LEGAIS E SOCIAIS DA APLICAÇÃO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL NO POLICIAMENTO PREDITIVO

O uso crescente de métodos e técnicas de Inteligência Artificial na sociedade contemporânea apresenta uma série de desafios éticos e jurídicos. A distinção entre ética e direito é fundamental para compreender os parâmetros que orientam o desenvolvimento e a aplicação de sistemas de IA. A ética refere-se a sistemas internos de controle, baseados em princípios morais, enquanto o direito envolve normas externas impostas por autoridades competentes. Assim, enquanto a ética busca incorporar valores morais às práticas tecnológicas, o direito assegura a conformidade legal (Qian *et al.*, 2024). Tanto as dimensões éticas quanto jurídicas se entrelaçam com desafios sociais relevantes. Por isso, considerar os impactos sociais

constitui uma perspectiva complementar para compreender os efeitos do policiamento preditivo (Gstrein *et al.*, 2019).

No campo ético, a responsabilização (*accountability*) é um ponto crítico. Diante da complexidade dos sistemas baseados em IA, surgem dúvidas sobre quem deve ser responsabilizado juridicamente e moralmente por decisões automatizadas: desenvolvedores, operadores ou usuários. O desdobramento deste princípio é o estabelecimento de mecanismos institucionais, permitindo responsabilização efetiva e reparação adequada em caso de falhas (Goram; Veiel, 2021) (Siau; Wang, 2020). O viés (*bias*) algorítmico também merece atenção. Algoritmos podem reproduzir e amplificar preconceito preexistentes na base de dados, resultando em discriminação em setores sensíveis como a Segurança Pública. Estes vieses decorrem tanto de falhas técnicas, como dados não representativos, quanto de fatores estruturais. Mitigá-los exige curadoria ética baseada em dados, testes de equidade e ajustes nos parâmetros dos modelos de predição (Goram; Veiel, 2021) (Siau; Wang, 2020).

Ainda no plano ético, a utilização de classificações binárias, como “alto risco” e “baixo risco” — pode resultar em consequência assimétricas. 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, 2011). Para lidar com esta assimetria pode-se utilizar modelos baseados em regressão (*random forest*) que permitem ajustar tais erro, uma vez que esta técnica superestima os casos de risco (aumenta os falsos positivos) para garantir que erros mais graves — os falsos negativos — sejam minimizados (Berk, 2011).

A transparência e a explicabilidade dos algoritmos representam outro desafio. À medida que os algoritmos, especialmente os baseados em Aprendizagem Profunda (*Deep Learning*), se tornam mais complexos, sua lógica de funcionamento torna-se menos compreensível, sendo frequentemente caracterizados como “caixas-pretas” (*black-box*) devido à sua complexidade e opacidade (Ali *et al.*, 2023) (Goram; Veiel, 2021) (Siau; Wang, 2020) (Kaufman, 2021) (Mendonça Junior; Nunes, 2023) (Qian *et al.*, 2024). A falta de transparência decorre da dificuldade em compreender tanto os mecanismos operacionais dos algoritmos quanto os dados utilizados no treinamento de modelos (Cerrillo i Martinez, 2019).

Tal opacidade impede que predições incorretas sejam apontadas, sem a devida compreensão sobre as causas de erros e incertezas (Henz, 2021). Ademais, a dificuldade em se realizar auditoria, contestação ou revisão das decisões automatizadas, coloca em risco princípios como o devido processo legal (Henz, 2021). Ademais, como os algoritmos tem por

base estruturação dinâmica, a compreensão de seu funcionamento pode rapidamente se tornar obsoleta (Cerrillo i Martinez, 2019). Modelos alternativos, como "caixas-brancas" ou "cinzas" (*grey-box*), podem auxiliar e mitigar a opacidade, mas ainda podem enfrentar obstáculos práticos significativos, o que reforça a complexidade de tais sistemas (Ali, 2023).

No entanto, Hung e Yen (2021) argumentam que, embora teoricamente seja possível caminhar em direção a uma maior transparência algorítmica, essa possibilidade não se concretiza de forma simples ou automática. As limitações cognitivas dos usuários e os custos econômicos e técnicos envolvidos impõem desafios substanciais ao entendimento pleno desses modelos. Neste sentido, a transparência pode ser concebida como uma meta desejável, mas que pode esbarrar em obstáculos práticos significativos, o que reforça a complexidade envolvida na aplicação real desses sistemas.

Contudo, a opacidade destes sistemas gera limitações. Muitos profissionais que os utilizam — como policiais e promotores — não têm formação em Ciência da Computação (área do conhecimento humano que desenvolve e estuda a área de IA) ou Estatística ou Matemática, o que dificulta a compreensão e avaliação crítica de resultados. Esta assimetria de conhecimento pode comprometer a capacidade de avaliação crítica das recomendações emitidas por tais sistemas, tornando os operadores mais propensos a aceitar os resultados como tecnicamente corretos, mesmo sem compreender plenamente seus fundamentos ou limitações. A transparência é ainda comprometida por segredos comerciais que envolvem os algoritmos, criando barreiras à fiscalização pública (Helm; Hagendorff, 2021). A ausência de clareza sobre quais departamentos usam quais sistemas afeta, por consequência, a transparência da administração pública (Sabol; Baumann, 2022).

Outro questão é o viés racial. Estudos mostram que dados enviesados — decorrentes da atuação seletiva da polícia — podem levar à superestimação da criminalidade em comunidades com alta concentração de minorias raciais (Davis et al., 2022). Ademais, evidências empíricas sugerem que critérios raciais e étnicos influenciam a decisão sobre quais indivíduos são detidos e revistados, bem como quais bairros são alvo de patrulhamento. Dessa forma, a concentração policial em determinadas áreas tende a gerar uma representação desproporcional destes grupos nos registros criminais, uma vez que os crimes ocorridos nestes locais são mais frequentemente documentados devido à maior presença policial (Lum; Isaac, 2016). Isso, por sua vez, reforça os próprios dados que alimentam o modelo, criando um ciclo vicioso de hipervigilância seletiva e criminalização de determinados grupos sociais (Ensign et al., 2018). Este ciclo de reforço foi chamado por Ensign et al. (2018) de “*loop* de

retroalimentação” (*feedback loop*), no qual a presença policial aumenta os registros, o que por sua vez justifica mais policiamento.

Uma técnica utilizada na identificação de possíveis perpetradores é a Análise de Redes Sociais (*Social Network Analysis – SNA*) que examina as conexões entre indivíduos (Tayebi *et al.*, 2016) (Borgatti *et al.*, 2009) (Shapiro, 2017) (Susser, 2021) (Deeks, 2018). A Análise de Redes Sociais concentra-se nos aspectos estruturais das redes para detectar e interpretar padrões das entidades sociais. Deste modo, analisa uma rede composta por nós e arestas (ligações entre nós), buscando identificar propriedades distintas por meio de uma análise formal (Tayebi *et al.*, 2016). Esta abordagem permite compreender detalhadamente as interações entre os elementos (indivíduos) da rede e como essas interações podem influenciar comportamentos e dinâmicas sociais, incluindo a propagação de comportamentos delitivos. Isto levanta ‘srias preocupações éticas e legais sobre proporcionalidade.

O lado negativo é que este tipo de análise pode gerar a chamada “rede de vigilância secundária”, por meio da qual indivíduos que nunca tiveram contato com o sistema de justiça passam a ser monitorados simplesmente por estarem conectados a alguém que já teve, por exemplo, que já foi preso anteriormente. Tais indivíduos podem ser colocados sob rastreamento automático, sendo que o sistema pode disparar alertas em tempo real quando eles interagem com a polícia ou outros órgãos governamentais (Brayne, 2018).

Do ponto de vista jurídico, destaca-se a preocupação com a proteção de dados pessoais e privacidade. Aqui a privacidade está sendo entendida como um direito individual, voltado a limitar interferências arbitrárias e desproporcionais do Estado na integridade do espaço pessoal e da liberdade de expressão (Gstrein *et al.*, 2019). Portanto, uma vez que a IA opera com grandes volumes de dados pessoais e sensíveis, isto impõe riscos de tratamento indevido e vazamento de dados. A coleta inadequada ou o uso excessivo de dados pessoais pode gerar vigilância desproporcional e afastamento dos cidadãos dos serviços públicos (Brayne, 2018). Assim, a compatibilização entre inovação e direitos fundamentais demanda transparência e definição de limites claros para o tratamento de dados pessoais (Goram; Veiel, 2021) (Siau; Wang, 2020).

Para além disto, a própria lógica preditiva pode tensionar princípios fundamentais, como o da presunção de inocência, deslocando o foco da responsabilização para uma antecipação de culpabilidade, do “inocente até que se prove o contrário” para o “culpado até que se prove o contrário” (Gstrein *et al.*, 2019).

No plano social, 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. Além disto, deve-se examinar criticamente a cultura de coleta, interpretação, compartilhamento e exclusão de dados, especialmente dos dados pessoais e sensíveis — aspectos importantes para a confiança institucional. (Gstrein *et al.*, 2019).

Adicionalmente, a dependência excessiva de soluções técnicas também pode enfraquecer o vínculo entre a polícia e a comunidade, transformando agentes em operadores de sistemas, distantes das práticas baseadas em confiança, legitimidade e responsabilidade institucional. Isso pode agravar desigualdades e comprometer a missão social do policiamento como um todo (Bachner, 2013).

Outro desafio significativo reside na ausência de uma metodologia unificada para mensurar a predição. Mesmo quando se busca realizar predições mais precisas, não há critérios claros para definir o grau de sucesso obtido (Berk, 2008). Esta questão se torna especialmente relevante na formulação de políticas públicas, em que formas de padronização são essenciais para garantir a eficácia e a legitimidade das medidas adotadas (Lum; Nagin, 2017).

A participação da sociedade e o compartilhamento de informações com os agentes de patrulha tornam-se elementos essenciais para fortalecer a legitimidade da polícia e compreender as demandas sociais (Lum; Koper, 2017). Isto porque a atuação policial passa a envolver não apenas a antecipação de comportamentos delitivos, mas também a preservação da credibilidade institucional e a manutenção da confiança pública (Lum; Nagin, 2017).

Considerando-se o exposto, tem-se que as implicações éticas, legais e sociais dos sistemas de IA aplicados ao policiamento preditivo não são meras externalidades do processo tecnológico, mas sim componentes estruturais que moldam sua legitimidade, eficácia e aceitação pública. Entender tais implicações em sua complexidade é essencial para orientar políticas públicas mais justas, transparentes e sensíveis às dinâmicas sociais contemporâneas.

3 ESTRUTURA DO POLICIAMENTO PREDITIVO

Compreender a estrutura do policiamento preditivo é importante para avaliar os efeitos da aplicação de sistemas de IA sobre as práticas de segurança pública. A análise realizada nesta seção baseia-se em revisão de literatura especializada e na técnica de análise de conteúdo conforme sistematizada por Laurence Bardin (2011, p. 44). Esta abordagem permite examinar discursos e textos relevantes a partir da identificação de núcleos de sentido, organizados em categorias analíticas construídas com base nos critérios de exclusividade, exaustividade e

relevância. Com isso, busca-se mapear os componentes centrais da predição criminal, visando compreender suas implicações práticas e normativas.

Deste modo, a revisão de literatura foi dividida em três principais eixos: (1) Coleta e Processamento de Dados, (2) Produção de Previsões e (3) Implementação, com base nos modelos teóricos propostos por Brantingham (2017), Perry (2013), Berk (2008), Brayne (2018) e Carleton *et al.* (2020), de modo que tais autores dividem as etapas do policiamento preditivo conforme apresentado no Quadro 1.

Quadro 1 – Etapas do Policiamento Preditivo. Fonte: as autoras.

Categoria	Brantingham 2017	Perry 2013	Berk 2008	Brayne 2018	Carleton <i>et al.</i> 2020
Coleta de Dados	✓	✓	✓	✓	✓
Administração de Dados	–	–	✓	–	–
Análise de Dados	✓	✓	✓	✓	✓
Produção de Previsões	✓	✓	✓	✓	✓
Intervenção Policial	–	✓	✓	✓	–
Resposta / Feedback	–	✓	✓	✓	✓

Parte-se da premissa que Brantingham (2017) concebe o policiamento preditivo como um procedimento em três etapas: (1) coleta de dados, (2) aplicação de métodos algorítmicos e (3) uso das previsões. E, o modelo de policiamento preditivo proposto por Perry (2013) é estruturado em quatro fases principais interconectadas e contínuas, a saber: (1) coleta de dados, (2) análise de dados, (3) operações policiais e (4) resposta criminal. Este modelo visa antecipar comportamentos criminosos com base na análise de dados históricos e contextuais, permitindo aos órgãos de Segurança Pública tomarem medidas preventivas. Dentro da fase de coleta de dados, Perry (2013) inclui a *fusão de dados (data fusion)*, que é a combinação de informações de diferentes fontes para formar uma visão mais ampla e precisa do comportamento criminal. O objetivo da pesquisa do autor é examinar as medidas preditivas que já estão em uso e identificar tecnologias promissoras que podem ser aplicadas no futuro.

Berk (2008), por sua vez, apresenta metodologia que foca especificamente no uso de algoritmos e de técnicas de *Narrow Artificial Intelligence* em modelos preditivos e justiça criminal. A metodologia é dividida em cinco etapas: (1) coleta de dados, (2) administração de dados, (3) análise de dados, (4) decisões e (5) ações. Uma das diferenças centrais da metodologia de Berk é a introdução da fase de administração de dados (*data management*), que não é abordada diretamente por Perry. Essa etapa envolve a organização, o armazenamento e a governança de dados, garantindo que eles sejam acessíveis e precisos.

No mesmo sentido, Brayne (2018) entende que as etapas da polícia preditiva são: (1) coleta, (2) análise, (3) intervenção e (4) resposta. A primeira etapa envolve a coleta de dados, que pode incluir desde os tipos básicos de dados criminais presentes em relatórios oficiais até dados ambientais mais complexos, como sazonalidade, composição dos bairros ou variáveis ambientais associadas ao crime, por exemplo, terrenos baldios, parques, escolas e caixas eletrônicos. A segunda etapa é a análise de dados — um termo abrangente que inclui métodos que vão desde cálculos aritméticos básicos até as mais variadas abordagens algorítmicas.

A terceira etapa considerada por Brayne (2018) é denominada de intervenção policial, por meio da qual as previsões de crime são distribuídas a policiais e supervisores para que decidam onde alocar os agentes em campo. A quarta etapa, “resposta ao alvo”, refere-se à reação dos indivíduos sob vigilância policial, sendo avaliada em termos de desistência (a polícia intervém e a pessoa não comete o crime) ou deslocamento (a polícia intervém e a pessoa procura outro local para cometer o crime).

Focando em Aprendizagem de Máquina (*Machine Learning*), Carleton *et al.* (2020) entende que os passos para realizar uma predição são: (1) Inserir dados, (2) analisar dados, (3) identificar padrões, (4) fazer previsões e (5) armazenar os resultados.

Este artigo se propõe a cumprir três principais eixos: a) Coleta e Processamento de Dados, b) Produção de Previsões e c) Implementação. Os eixos abrangem o fenômeno estudado e estão alinhados aos modelos teóricos e serão utilizados como base para descrever o funcionamento do policiamento preditivo. Assim, a categorização proposta favorece uma análise mais clara, coesa e funcional do *corpus* empírico, sendo cada eixo conceituado de acordo com o Quadro 2, conforme a descrição dos autores citados no Quadro 1.

A seguir, examina-se a estrutura operacional do policiamento preditivo, com foco na coleta e no processamento de dados, bem como na produção de previsões. Ao descrever estas etapas, busca-se compreender os mecanismos técnicos que fundamentam os modelos baseados em Inteligência Artificial aplicados à segurança pública para, posteriormente, identificar os principais pontos de vulnerabilidade ética e legal que emergem ao longo deste processo.

Quadro 2 – Conceitos das Etapas do Policiamento Preditivo. Fonte: as autoras.

Eixo Analítico	Descrição Geral	Elementos Específicos
1. Coleta e Processamento de Dados	Abrange a coleta, organização, fusão e administração dos dados utilizados nos sistemas de policiamento preditivo.	- Coleta de dados criminais e contextuais - Organização e padronização dos dados - Fusão de dados de diferentes fontes - Administração e governança dos dados
2. Desenvolvimento de Previsões	Refere-se à aplicação de técnicas estatísticas e computacionais para extrair padrões e produzir inferências sobre comportamentos ou ocorrências futuras.	- Escolha de variáveis relevantes - Modelagem matemática ou computacional - Testagem e calibração dos modelos - Geração de outputs
3. Implementação	Compreende a aplicação prática das previsões geradas, guiando as operações policiais e avaliando suas consequências.	- Planejamento tático com base nas previsões - Intervenções dirigidas (patrulhamento, visitas, abordagens) - Avaliação da resposta (deslocamento, desistência)

3.1 Coleta e Processamento de Dados

Os dados constituem a base da aplicação de métodos preditivos. E, dos estudos realizados, depreende-se que tais modelos se fundamentam em dados empíricos que orientam tanto a construção quanto a aplicação dos resultados das previsões. A lógica do policiamento preditivo está em alimentar modelos estatísticos com grandes volumes de dados, identificando características relevantes para gerar generalizações estatísticas que possam sustentar decisões preventivas. Nesta perspectiva, trata-se menos de prever eventos específicos e mais de estimar probabilidades com base em padrões observados (Helm; Hagendorff, 2021).

Os modelos preditivos dependem, portanto, de dados precisos, limpos e utilizáveis (Ferguson, 2017). A diversidade de formatos - que pode incluir números, textos, sons, imagens e até o silêncio - exige técnicas robustas de coleta e processamento (Kitchin, 2016). Falhas nesta etapa afetam diretamente a performance dos algoritmos e geram vulnerabilidades no sistema (Ferguson, 2017). A coleta de dados envolve etapas como seleção, limpeza (*data cleaning*), integração e preparação dos dados para uso nos algoritmos (Han *et al.*, 2000). As fontes primárias incluem registros históricos de crimes, a exemplo de dados sobre tipo, local e horário dos delitos, bem como características dos envolvidos (Perry, 2013). Além disto, são incorporados dados sociais, por exemplo: condições econômicas, ambiente familiar (Hamilton,

2021) e uso de substâncias, conforme apontado por Cottle *et al.* (2001) no estudo sobre reincidência juvenil.

Casos como o analisado por Dario *et al.* (2015), que encontrou correlação entre criminalidade e condições favoráveis ao surfe em Ventura – Califórnia - EUA, mostram como variáveis aparentemente desconexas podem se tornar relevantes para os modelos. Isso reforça a importância da abrangência, qualidade e representatividade de bases de dados. Este tipo de estudo demonstra que fatores ambientais (extrínsecos - clima) podem ter impacto sobre a segurança pública e, também, mostra a importância de analisar dados de forma contextualizada.

Ademais, o paradoxo do policiamento preditivo - quando a ação policial bem-sucedida altera os padrões criminais e compromete as previsões futuras - mostra que os dados são voláteis. Quando a intervenção policial resulta em uma redução significativa da criminalidade, as previsões tornam-se ineficazes, uma vez que os dados utilizados para prever crimes já não são mais aplicáveis, porque as próprias previsões alteram os padrões de comportamento de criminoso futuro (Helm; Hagendorff, 2021) (Farrington, 1987).

Em síntese, a etapa de coleta e processamento de dados é primordial para o policiamento preditivo. Sua qualidade, abrangência e representatividade influenciam diretamente a validade das análises e a eficácia das decisões baseadas em previsões. Contudo, ela também representa uma fonte relevante de riscos e limitações, especialmente diante da natureza mutável dos dados e da complexidade de suas interpretações.

3.2 Desenvolvimento de Previsões

Este item não aborda o desenvolvimento algorítmico de modelos de previsão, visto que foge ao escopo do presente artigo, o qual tem foco nos aspectos jurídicos, éticos e sociais do policiamento preditivo. Assim, entende-se que o motor do policiamento preditivo está no conjunto de métodos e técnicas aplicados nos algoritmos. E. existem diversos métodos que podem ser aplicados no desenvolvimento de modelos voltados à previsões (Bachner, 2013), podendo-se utilizar algoritmos que seguem metodologia analítica específica (Ferguson, 2017), consistindo em instruções automatizada para processar dados e produzir saídas (Dencik *et al.*, 2018).

Cabe comentar algo sobre algoritmos, que de acordo com Freitas (2021), podem ser entendidos como uma sequência finita de ações que podem ser executadas para resolver um problema específico. Para serem eficazes, devem ser precisos, mecânicos, eficientes e corretos, compostos por instruções, raciocínio e operações (atribuição, aritmética, lógica e relacional).

Com o tempo, a utilização de algoritmos evoluiu de escalas simples, baseadas em conhecimento empírico e correlação entre duas variáveis (por exemplo: idade e criminalidade), para análises de regressão mais complexas e, mais recentemente, para a Aprendizagem de Máquina (*Machine Learning*) (Dencik, 2018). Segundo Freitas e Barddal (2019) estas técnicas permitem a personalização de algoritmos que são aplicados para executar tarefas preditivas com capacidade de generalização, ou seja, de extrair padrões dos dados passados e prever, com precisão, dados desconhecidos.

3.3 Implementação de Modelos Preditivos

Após a coleta e análise de dados, o próximo passo é a implementação dos modelos. A implementação de modelos preditivos dependerá, em grande medida, dos objetivos e das técnicas utilizadas (Abramowicz, 2006), sendo marcada por sua orientação à inteligência policial e foco preventivo (Bachner, 2013).

A adoção destes modelos exige uma adaptação institucional ampla. A criação de manuais operacionais contribui para traduzir os modelos preditivos e o conhecimento técnico em práticas concretas, ao mesmo tempo em que aumenta a transparência das ações (Lum; Koper, 2017). Contudo, para que estes instrumentos sejam eficazes, é necessário reconfigurar os sistemas de responsabilização, supervisão, gestão e liderança, integrando a lógica orientada por dados à estrutura organizacional. Os sistemas preditivos influenciam o comportamento dos agentes ao se relacionarem com mecanismos de recompensa, punição, promoção e reconhecimento, portanto, rever a inserção de tais modelo na estrutura organizacional é fundamental. Isto posto, diante de que se tem estruturas organizacionais frequentemente complexas e contraditórias, entrelaçadas com a cultura institucional, as expectativas sociais e as rotinas operacionais (Lum; Koper, 2017).

A efetiva incorporação dos resultados preditivos às decisões policiais requer ferramentas que tornem essas informações inteligíveis e aplicáveis. Isso demanda capacitação contínua das equipes envolvidas, para que interpretem os resultados com criticidade e adequação ao contexto. Além disto, os modelos devem ser constantemente monitorados, assegurando sua atualização diante de mudanças regulatórias, institucionais ou sociais. Paralelamente, é necessário fomentar uma cultura organizacional baseada em dados, que promova a colaboração intersetorial e reduza a predominância de decisões baseadas apenas na intuição ou na experiência empírica (Abramowicz, 2006).

Além dos desafios técnicos e normativos, a implementação de sistemas de IA nas instituições policiais envolve obstáculos operacionais. Barreiras como a resistência cultural de

agentes, a falta de treinamento e a adaptação a novos processos dificultam a aceitação da tecnologia. Frequentemente, o aumento da supervisão e das exigências de relatórios é percebido negativamente pelos próprios policiais, reforçando a importância de apoio gerencial consistente (Koper, 2014).

Em síntese, a implementação de modelos preditivos exige mais do que ajustes técnicos: envolve transformações organizacionais, capacitação contínua, transparência e engajamento com a sociedade. A eficácia desta etapa depende da articulação entre tecnologia, estrutura institucional e confiança pública, destacando-se a necessidade de monitoramento constante e adaptação às dinâmicas sociais e institucionais.

4 SÍNTESE DOS EIXOS E IMPLICAÇÕES

Objetiva-se, a partir do que foi discutido no item 3, integrar os principais achados teóricos e empíricos relativos à aplicação de sistemas de IA no policiamento preditivo, seguindo-se os mesmos três eixos analíticos: (1) Coleta e Processamento de Dados, (2) Desenvolvimento de Predições e (3) Implementação. Esta estrutura permite identificar, de forma sistemática, os benefícios operacionais, os desafios éticos e as implicações jurídicas associados a cada etapa do processo. O Quadro 3 sintetiza essas dimensões e serve de base para a discussão subsequente.

Quadro 3- Eixos e implicações. Fonte: As autoras.

Etapa	Benefícios Operacionais	Riscos Éticos	Implicações Jurídicas e Institucionais
Coleta e Processamento de Dados	- Organização de dados - Ganho de escala	- Coleta sem consentimento - Enviesamento	- Regulação - Proteção de dados - Governança de dados
Desenvolvimento de Predições	- Previsibilidade - Alocação eficiente	- Opacidade - Discriminação algorítmica	- Transparência - Explicabilidade
Implementação e Decisão	- Ação rápida - Prevenção	- Estigmatização - Uso excessivo da força	- Controle institucional - Protocolos públicos

A análise das etapas revela contrastes importantes entre os benefícios e os riscos éticos-jurídicos ao longo do ciclo de aplicação de sistemas de IA. A etapa de Coleta e Processamento de Dados, embora operacionalmente mais consolidada, traz consigo riscos éticos relacionados à coleta indiscriminada de dados, especialmente dados pessoais e sensíveis, ao viés estrutural e ao uso de dados sensíveis sem consentimento. Trata-se de um ponto em que a conformidade com legislações de proteção de dados não é apenas desejável, mas obrigatória,

a exemplo da Lei Geral de Proteção de Dados Pessoais (LGPD), no Brasil, e o *General Data Protection Regulation* (GDPR), na União Europeia. Contudo, é também neste eixo que surgem oportunidades para o aprimoramento da eficiência institucional, por meio da integração de bases de dados, melhoria na qualidade informacional e identificação de padrões antes invisíveis à atuação policial tradicional.

A fase de Desenvolvimento de Previsões, por exemplo, concentra os maiores desafios técnicos e normativos. A opacidade algorítmica, a falta de explicabilidade e a possibilidade de discriminação tornam esta etapa crítica do ponto de vista do controle institucional e da responsabilização. Ainda que esta fase proporcione ganhos substanciais em termos de previsão e antecipação de riscos, ela exige rigorosos mecanismos de supervisão, auditoria e transparência para evitar danos estruturais à justiça e aos direitos fundamentais.

A fase de Implementação se distingue por representar não apenas um ponto de aplicação prática dos resultados dos modelos de predição, mas também o momento em que os efeitos sociais, jurídicos e simbólicos atrelados ao uso de sistemas de IA se materializam. É nesta etapa que se exige mais do que regulamentação. Torna-se imprescindível uma remodelação institucional, com ajustes nos sistemas de supervisão, capacitação, responsabilização e comunicação com a sociedade. O uso de modelos preditivos neste estágio requer protocolos públicos, engajamento comunitário e mecanismos de contestação acessíveis. A ausência destes elementos pode amplificar estigmas sociais, aprofundar desigualdades e comprometer a legitimidade da atuação policial.

Em síntese, enquanto as fases iniciais apresentam riscos ligados à base técnica e ao tratamento de dados, a etapa de implementação revela-se como o núcleo mais sensível, exigindo transformação organizacional ampla e sustentada. Ainda assim, a aplicação de sistemas de IA no policiamento preditivo traz oportunidades relevantes de eficiência, precisão e inovação, desde que seja acompanhada de salvaguardas éticas robustas e governança normativa transparente e democrática.

5 CONCLUSÃO

A aplicação de sistemas de IA na predição criminal representa um avanço significativo na forma como a segurança pública pode ser planejada e executada. O presente estudo buscou analisar os benefícios e os desafios éticos e sociais, bem como as implicações jurídicas de tais sistemas diante da necessidade de se ter ferramenta tecnológica, porém com embasamento jurídico e ético, tendo por base a análise das etapas do policiamento preditivo. A categorização proposta em três eixos — Coleta e Processamento de Dados, Produção de Previsões e

Implementação — mostrou-se adequada para articular diferentes modelos teóricos e oferecer uma visão coesa e crítica do fenômeno.

Entre as principais descobertas, destaca-se que os maiores riscos éticos se concentram na fase de produção de predições, especialmente devido à opacidade algorítmica, enquanto a fase de implementação exige, além de regulamentação, transformações institucionais profundas. Ao mesmo tempo, os sistemas de IA oferecem oportunidades concretas de aumento de eficiência, desde que acompanhados de salvaguardas éticas, controle social e transparência.

Como recomendação normativa, ressalta-se a necessidade de elaboração de diretrizes públicas claras sobre a aplicação de sistemas de IA em segurança pública, incluindo exigências de auditabilidade, critérios de explicabilidade dos modelos e mecanismos de contestação acessíveis. Institucionalmente, é imperativo reestruturar os sistemas de supervisão, capacitação e responsabilização das forças policiais, promovendo uma cultura orientada por dados, mas ancorada em valores democráticos.

Quanto às limitações, reconhece-se que a análise ora desenvolvida é predominantemente teórica e normativa, e que a aplicação prática de modelos de predição pode variar significativamente conforme o contexto sociopolítico e os recursos institucionais de cada país ou região. Como caminhos para futuras pesquisas, sugere-se o aprofundamento empírico da avaliação de modelos de predição voltados ao policiamento preditivo já em uso, a análise comparativa de experiências internacionais e a investigação de instrumentos regulatórios mais eficazes para equilibrar inovação tecnológica e proteção de direitos fundamentais.

REFERÊNCIAS

ABRAMOWICZ, Michael. Predictive decisionmaking. **Va. L. Rev.**, v. 92, p. 1-65, 2006.

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

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

BARDIN, Laurence. *Análise de Conteúdo*. Lisboa: Edições 70, 2011.

BERK, Richard. Forecasting methods in crime and justice. **Annual Review of Law and Social Science**, v. 4, n. 1, p. 219-238, 2008.

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

BORGATTI, Stephen P. *et al.* Network analysis in the social sciences. **Science**, v. 323, n. 5916, p. 892-895, 2009.

- BRANTINGHAM, P. Jeffrey. The logic of data bias and its impact on place-based predictive policing. **Ohio State Journal of Criminal Law**, v. 15, p. 473, 2017.
- BRAYNE, Sarah. The criminal law and law enforcement implications of big data. **Annual Review of Law and Social Science**, v. 14, n. 1, p. 293-308, 2018.
- CARLETON, Benjamin; CUNNINGHAM, Brittany; THORKILDSEN, Zoë. **The Use of Predictive Analytics in Policing**. Arlington, VA: CNA, 2020.
- CERRILLO I MARTINEZ, Agusti. How can we open the black box of public administration? Transparency and accountability in the use of algorithms. **Rev. Catalana Dret Pub.**, v. 58, p. 13, 2019.
- CHAN, Janet; MOSES, Lyria Bennett. Is big data challenging criminology? **Theoretical Criminology**, v. 20, n. 1, p. 21-39, 2016.
- COTTLE, Cindy C.; LEE, Ria J.; HEILBRUN, Kirk. The prediction of criminal recidivism in juveniles: A meta-analysis. **Criminal justice and behavior**, v. 28, n. 3, p. 367-394, 2001.
- 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.
- DAVIS, Jeremy et al. Five ethical challenges facing data-driven policing. **AI and Ethics**, v. 2, n. 1, p. 185-198, 2022.
- DEEKS, Ashley S. Predicting enemies. **Virginia Law Review**, v. 104, n. 8, p. 1529-1592, 2018.
- DENCIK, Lina et al. **Data scores as governance: Investigating uses of citizen scoring in public services**. Cardiff: Data Justice Lab, 2018.
- ENSIGN, Danielle et al. **Runaway feedback loops in predictive policing**. In: Conference on fairness, accountability and transparency, PMLR, 2018, p. 160-171.
- FARRINGTON, David P. Predicting individual crime rates. **Crime and Justice**, v. 9, p. 53-101, 1987.
- FERGUSON, Andrew Guthrie. Policing predictive policing. **Wash. UL Rev.**, v. 94, p. 1109, 2017.
- 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.

GSTREIN, Oskar J.; BUNNIK, Anno; ZWITTER, Andrej J. Ethical, legal and social challenges of Predictive Policing. **Católica Law Review**, v. 3, n. 3, p. 77-98, 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.

HAN, Jiawei; KAMBER, Micheline; PEI, Jian. **Data mining: concepts and techniques**, Waltham: Morgan Kaufmann Publishers, 2012.

HAN, Jiawei; PEI, Jian; TONG, Hanghang. **Data mining: concepts and techniques**. Morgan kaufmann, 2000.

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

HELM, Paula; HAGENDORFF, Thilo. Beyond the prediction paradigm: challenges for AI in the struggle against organized crime. **Law & Contemp. Probs.**, v. 84, p. 1, 2021.

HENZ, Patrick. Ethical and legal responsibility for artificial intelligence. *Discover Artificial Intelligence*, v. 1, n. 1, p. 2, 2021.

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.

KAUR, Manpreet; SAINI, Munish. Role of Artificial Intelligence in the crime prediction and pattern analysis studies published over the last decade: a scientometric analysis. **Artificial Intelligence Review**, v. 57, n. 8, p. 202, 2024.

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.

KITCHIN, Rob. **The data revolution: big data, open data, data infrastructures & their consequences**. Los Angeles: SAGE Publications Ltd., 2016.

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.

LUM, Kristian; ISAAC, William. To predict and serve? **Significance**, v. 13, n. 5, p. 14-19, 2016.

LUM, Cynthia M.; KOPER, Christopher S. **Evidence-based policing**: Translating research into practice. Oxford: Oxford University Press, 2017.

LUM, Cynthia; NAGIN, Daniel S. Reinventing american policing. **Crime and Justice**, v. 46, n. 1, p. 339-393, 2017.

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

MENDONÇA JUNIOR, Claudio do Nascimento; 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.

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

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.

SABOL, William J.; BAUMANN, Miranda L. Forecasting and criminal justice policy and practice. **American Journal of Criminal Justice**, v. 47, n. 6, p. 1140-1165, 2022.

SELBST, Andrew D. Disparate impact in big data policing. **Georgia Law Review**, v. 52, p. 109, 2017.

SHAPIRO, Aaron. Reform predictive policing. **Nature**, v. 541, n. 7638, p. 458-460, 2017.

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.

SUSSER, Daniel. **Predictive policing and the ethics of preemption**. The ethics of policing: New perspectives on law enforcement, p. 268-292, 2021.

TAYEBI, Mohammad A. et al. **Social network analysis in predictive policing**. Springer International Publishing, 2016.