

VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

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 Naspolini - 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

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Caio Augusto Souza Lara; Claudia Maria Da Silva Bezerra; José Carlos Francisco dos Santos. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia

ISBN: 978-65-5274-160-8

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

Tema: Direito Governança e Políticas de Inclusão

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VIII Encontro Virtual do CONPEDI (2; 2025; Florianópolis, Brasil).

CDU: 34



VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Os artigos contidos nesta publicação foram apresentados no Grupo de Trabalho Direito, Governança e Novas Tecnologias I durante o VIII Encontro Virtual do Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, realizado nos dias 24 a 28 de junho de 2025, sob o tema geral “Direito, Governança e Políticas de Inclusão”. Trata-se da oitava experiência de encontro virtual do CONPEDI em mais de três décadas de existência.

A apresentação dos trabalhos abriu caminho para uma importante discussão, em que os pesquisadores do Direito puderam interagir em torno de questões teóricas e práticas, levando-se em consideração a temática central grupo. Essa temática traz consigo os desafios que as diversas linhas de pesquisa jurídica enfrentam no tocante ao estudo dos referenciais teóricos do tema governança e seus impactos no universo tecnológico.

A publicação reúne pesquisas que exploram os impactos jurídicos, éticos e sociais da inteligência artificial e das tecnologias digitais sobre o Estado Democrático de Direito, com foco especial na proteção de direitos fundamentais. As discussões abrangem temas como o uso de IA na Defensoria Pública e na dosimetria da pena, o risco de vieses algorítmicos no policiamento preditivo, e os limites constitucionais da automação decisória. Também são abordadas as responsabilidades civis dos agentes de IA, a regulação do mercado de criptoativos, a proteção de dados sensíveis (como prontuários médicos), e a necessidade urgente de regulamentar ilícitos eleitorais e obras autorais geradas por IA. A interseção entre transparência, governança algorítmica e acesso à justiça é outro eixo central, com reflexões

tecnologia, com base em autores como Douglas Rushkoff, e sugere caminhos para um novo paradigma regulatório que una inovação, equidade, sustentabilidade e respeito aos direitos humanos.

Na coletânea que agora vem a público, encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-graduação em Direito, nos níveis de Mestrado e Doutorado, com artigos rigorosamente selecionados, por meio de dupla avaliação cega por pares (double blind peer review). Dessa forma, todos os artigos ora publicados guardam sintonia direta com este Grupo de Trabalho.

Agradecemos a todos os pesquisadores pela sua inestimável colaboração e desejamos uma ótima e proveitosa leitura!

Caio Augusto Souza Lara

Claudia Maria Da Silva Bezerra

José Carlos Francisco dos Santos

POLICIAMENTO PREDITIVO E VIÉS ALGORÍTMICO: RISCOS, IMPLICAÇÕES JURÍDICAS E DESAFIOS PARA OS DIREITOS FUNDAMENTAIS

PREDICTIVE POLICING AND ALGORITHMIC BIAS: RISKS, LEGAL IMPLICATIONS AND CHALLENGES FOR FUNDAMENTAL RIGHTS

Dierick Bernini Marques Costa ¹

Daniel Vitor Silva Queiroz ²

Eduardo Pítrez de Aguiar Corrêa ³

Resumo

O presente artigo analisa criticamente os impactos do policiamento preditivo sobre os direitos fundamentais no processo penal, a partir de uma abordagem interdisciplinar que articula fundamentos técnicos, jurídicos e institucionais. A crescente utilização de sistemas de inteligência artificial na segurança pública, com destaque para ferramentas baseadas em machine learning e análise de big data, tem possibilitado a adoção de sistemas de policiamento preditivo voltados à antecipação de crimes com base em padrões estatísticos. Todavia, esses sistemas, ao se apoiarem em bases de dados historicamente enviesadas, tendem a reproduzir e até reforçar desigualdades estruturais preexistentes, como o racismo, o classismo e a seletividade penal. A pesquisa adota uma metodologia qualitativa, exploratória e analítico-crítica, com base em revisão bibliográfica e análise de documentos internacionais. Conclui-se que, embora o uso da inteligência artificial possa representar um avanço na eficiência das políticas públicas de segurança, sua aplicação no processo penal exige marcos regulatórios claros e mecanismos institucionais eficazes de controle, a fim de garantir que a inovação tecnológica não ocorra em detrimento dos direitos fundamentais e da legalidade democrática.

Palavras-chave: Policiamento preditivo, Inteligência artificial, Viés algorítmico, Direitos fundamentais, Governança algorítmica

Abstract/Resumen/Résumé

This article critically analyzes the impacts of predictive policing on fundamental rights in

security, with emphasis on tools based on machine learning and big data analysis, has enabled the adoption of predictive policing systems aimed at anticipating crimes based on statistical patterns. However, these systems, by relying on historically biased databases, tend to reproduce and even reinforce preexisting structural inequalities, such as racism, classism, and criminal selectivity. The research adopts a qualitative, exploratory, and analytical-critical methodology, based on a literature review and analysis of international documents. It is concluded that, although the use of artificial intelligence may represent an advance in the efficiency of public security policies, its application in criminal proceedings requires clear regulatory frameworks and effective institutional control mechanisms, in order to ensure that technological innovation does not occur to the detriment of fundamental rights and democratic legality.

Keywords/Palabras-claves/Mots-clés: Predictive policing, Artificial intelligence, Algorithmic bias, Fundamental rights, Algorithmic governance

1. INTRODUÇÃO

O avanço das tecnologias digitais transformou radicalmente as formas de controle social, especialmente no campo da segurança pública. A crescente adoção de sistemas de inteligência artificial¹ (IA) por instituições policiais têm promovido a consolidação de modelos de policiamento preditivo, nos quais algoritmos são utilizados para identificar padrões de comportamento e prever a ocorrência de delitos com base na análise massiva de dados. Ainda que essas ferramentas sejam promovidas como soluções promissoras para aprimorar a atividade policial, reduzir custos operacionais e aumentar a eficiência na prevenção ao crime, sua implementação tem gerado preocupações de ordem ética, jurídica e social, sobretudo no que tange à reprodução de preconceitos históricos e à violação de direitos fundamentais.

O policiamento preditivo baseia-se em modelos matemáticos e estatísticos que, por meio do cruzamento de dados geográficos, históricos criminais e informações sociais, produzem “zonas de risco” ou “indivíduos suspeitos” com base em probabilidade estatística (Moraes, 2022). Todavia, a literatura especializada já demonstrou que, longe de representar uma racionalidade neutra e objetiva, tais sistemas carregam consigo os vícios dos dados nos quais se baseiam (Moraes, 2022). A depender da base alimentadora dos algoritmos – frequentemente composta por registros enviesados da própria atuação policial –, o sistema pode perpetuar e/ou até intensificar padrões discriminatórios, como o racismo, a criminalização da pobreza e o reforço da seletividade penal (Barocas; Selbst, 2016; Baer, 2019).

Casos emblemáticos, como o do software COMPAS (Perfil de Gerenciamento Corretivo de Infratores para Sanções Alternativas) nos Estados Unidos, demonstraram como a suposta imparcialidade algorítmica pode ser questionada quando submetida ao crivo jurídico e científico (Angwin et al., 2016; Vega, 2025). Estudos empíricos comprovaram que o sistema, amplamente utilizado na concessão de fianças e na fixação de penas, apresentava taxa significativamente mais alta de falsos positivos para pessoas negras (Vieira, 2025). Essa constatação revela que os algoritmos de IA não apenas refletem os preconceitos embutidos em seus dados de treinamento, mas também os institucionalizam em decisões que afetam

¹O termo “inteligência artificial” foi introduzido por John McCarthy em 1956, dando origem a diferentes formas de classificação da IA. Entre as principais, destacam-se aquelas que visam pensar ou agir como humanos e as que operam com base em princípios de racionalidade (Haugeland, 1985; Winston, 1970; Schakoff, 1990). A recorrência à ideia de “humano” reflete a compreensão de que o comportamento humano pode ser analisado como objeto de ciência empírica (Borges, 2023).

diretamente a liberdade e a dignidade das pessoas. O mesmo alerta se observa nos debates internacionais sobre a admissibilidade da prova algorítmica e a confiabilidade jurídica de sistemas opacos (Sackman, 2023).

Nesse contexto, o presente artigo propõe uma análise crítica sobre os impactos do policiamento preditivo na proteção dos direitos fundamentais, com ênfase na reprodução de vieses algorítmicos e suas implicações no processo penal. Trata-se de uma investigação que articula fundamentos técnicos e jurídicos para compreender o funcionamento dessas tecnologias, identificar seus limites epistêmicos e normativos. O estudo se apoia em uma perspectiva teórica interdisciplinar, combinando as contribuições da ciência de dados, do direito processual penal e do direito internacional dos direitos humanos.

Ainda, a temática trabalhada se apoia no crescente protagonismo da inteligência artificial na formulação de políticas públicas e na condução de decisões que outrora cabiam exclusivamente a agentes humanos. Remora-se também que a delegação de poder decisório a sistemas automatizados, sem adequada governança e controle social, pode comprometer a legitimidade democrática das instituições e reduzir a *accountability*² das forças de segurança. Além disso, a ausência de normativas claras sobre a utilização de algoritmos no processo penal ameaça o núcleo duro das garantias individuais, como a presunção de inocência, o contraditório e o devido processo legal.

A metodologia adotada é qualitativa e exploratória, com enfoque analítico-crítico. A pesquisa se desenvolve a partir de revisão bibliográfica, análise de documentos internacionais (como o *Artificial Intelligence Act* da União Europeia, aprovado em 2024, e o Relatório da Europol sobre IA e policiamento, vigente no ano já mencionado). Busca-se, assim, não apenas descrever os riscos do policiamento algorítmico, mas evidenciar possíveis caminhos normativos e institucionais diversos para mitigar seus impactos adversos.

No primeiro capítulo, será examinado o funcionamento técnico do policiamento preditivo, destacando seus fundamentos em inteligência artificial e big data. Com base em exemplos como COMPAS e PredPol, ainda, mostra-se como esses sistemas podem reproduzir desigualdades sociais, intensificar a seletividade penal e comprometer garantias processuais.

O segundo capítulo abordará especificamente os impactos do policiamento preditivo na reprodução de desigualdades estruturais e na violação de direitos fundamentais. A partir de uma análise crítica, será discutido como algoritmos utilizados na segurança pública, longe de

²O termo *accountability* é definido por Rodrigues (2024), como o dever das autoridades prestarem contas à sociedade dos recursos financeiros arrecadados, assim como implementarem uma transparência para facilitar a visualização destes valores. Por outro lado, para Valdés (1988), além de do dever de se prestar contas e da transparência, há uma responsabilização intrínseca por esses gastos públicos

operarem com neutralidade, tendem a reforçar padrões de seletividade penal, em especial em sistemas já marcados por seletividade racial, criminalização da pobreza e fragilidade nos mecanismos de controle democrático.

O terceiro e último capítulo analisa os desafios jurídicos do uso de algoritmos no processo penal, destacando a necessidade de transparência, auditabilidade e regulação. Com base em experiências internacionais, defende-se uma governança algorítmica democrática que garanta o controle jurídico e a proteção dos direitos fundamentais.

2. TECNOLOGIAS DE CONTROLE E O SURGIMENTO DO POLICIAMENTO PREDITIVO: ENTRE A EFICIÊNCIA E A OPACIDADE ALGORÍTMICA

O policiamento preditivo representa uma das manifestações mais emblemáticas da crescente interseção entre tecnologia e segurança pública. Seu surgimento se dá no contexto de transformação das formas tradicionais de controle social, onde a ênfase deixa de recair sobre ações reativas e passa a priorizar intervenções proativas, orientadas por dados e pela lógica da antecipação de riscos (Moraes, 2022).

Originalmente implementado em experiências piloto nos Estados Unidos, a partir dos anos 2000, o policiamento preditivo baseia-se na premissa de que, ao analisar grandes volumes de dados históricos, é possível identificar padrões de criminalidade e, a partir deles, prever onde, quando e por quem um crime poderá ser cometido (Moraes, 2022). A promessa de neutralidade matemática, atribuída aos modelos estatísticos e algoritmos de inteligência artificial, atraiu gestores públicos, seduzidos pela ideia de eficiência e racionalidade operacional. No entanto, autores como Daniel Innerarity (2021), Ignacio Gonzalez Vega (2025) e Moraes (2022) advertem que essa suposta objetividade tende a ocultar os conflitos políticos subjacentes às decisões algorítmicas, resultando no que se convencionou chamar de “falácia da neutralidade técnica”.

Nesse cenário, a informação deixa de ser um insumo secundário para decisões humanas e passa a ser a própria base da decisão. Trata-se de uma racionalidade que desloca a centralidade do julgamento político e jurídico para uma lógica preditiva baseada em cálculos estatísticos. Essa transição traz consequências profundas para o sistema penal, sobretudo no que se refere à proteção das garantias fundamentais, à transparência das decisões e à responsabilização dos agentes envolvidos (Moraes, 2022).

A base técnica do policiamento preditivo é composta por três elementos estruturantes: o *machinelearning*, os sistemas de big data e os algoritmos de inteligência

artificial (Moraes, 2022). O *machinelearning* permite que os sistemas aprendam padrões e façam previsões com base em dados históricos, ajustando seus próprios parâmetros sem intervenção direta humana³. É justamente essa capacidade de “autoaprendizado” que confere flexibilidade ao sistema, mas que também o torna opaco e difícil de auditar. Em geral, os algoritmos utilizados nesse tipo de tecnologia operam como “caixas-pretas”, cujos critérios de decisão não são acessíveis, até mesmo para aqueles que os desenvolveram, assim, em certa medida, pode-se comprometer princípios penais, como contraditório e ampla defesa (Fornasier, 2021).

Complementarmente, os sistemas de big data possibilitam o armazenamento e cruzamento de milhões de registros, provenientes de fontes como boletins de ocorrência, câmeras de vigilância, redes sociais, sensores urbanos e bancos de dados de segurança privada⁴. A partir da análise massiva dessas informações, os algoritmos conseguem gerar zonas de risco geográfico, identificar horários críticos e até sugerir o perfil demográfico dos indivíduos mais propensos à prática de crimes. No entanto, esses dados estão longe de serem neutros, isto porque eles refletem, em grande medida, as práticas policiais históricas, que por sua vez já são marcadas por vieses raciais, territoriais e socioeconômicos (Barocas; Selbst, 2016).

Por fim, a inteligência artificial atua como o elo entre as ferramentas de análise e a ação estatal. Sistemas de IA são capazes de produzir decisões operacionais — como roteiros de patrulhamento, identificação de suspeitos ou recomendação de medidas cautelares — a partir das análises preditivas realizadas. Embora sua adoção seja frequentemente justificada pelo aumento de eficiência, a ausência de critérios objetivos de verificação e a dificuldade de contestação judicial tornam a IA uma ameaça potencial aos fundamentos garantistas do processo penal (Vega, 2025). Como reconhece a Europol (2024), a ausência de governança e a falta de auditoria sobre esses sistemas criam um risco concreto de violação sistemática de direitos fundamentais.

Essas questões tornam-se ainda mais evidentes quando analisamos os casos emblemáticos de uso de algoritmos no contexto penal, como os sistemas COMPAS (Perfil de Gerenciamento Corretivo de Infratores para Sanções Alternativas) e PredPol (Sistema de

³Para Viera e Santos (2025, p. 220), este conceito pode ser ampliando acrescentando que o processamento de dados, permite que a máquina faça previsões e delimitem tendências futuras, algo que influencia diretamente em práticas como, por exemplo, o policiamento. Isto tudo com o fim de maximizar a alocação de recursos.

⁴Para Ferguson (2015), big data, pode ser contemplado como um banco de dados que possuem grande volume de dados, variedade e velocidade. Dado o número massivo de dados e informações, torna-se necessário utiliza-se Inteligência Artificial para processar todas as informações, a partir disso, criam-se padrões e modelos preditivos de dados.

Policciamento Preditivo). O COMPAS, utilizado em diversos estados norte-americanos, visa fornecer aos juízes uma avaliação estatística sobre a probabilidade de reincidência criminal dos acusados. A pontuação gerada influencia diretamente decisões sobre liberdade provisória, fiança e até sentenças. Entretanto, um estudo conduzido pela ProPublica em 2016⁵ revelou que o sistema apresentava um viés racial significativo: pessoas negras tinham mais chances de receber uma pontuação de “alto risco” em comparação com pessoas brancas com antecedentes semelhantes⁶. Além disso, o sistema foi criticado por sua falta de transparência, já que a empresa desenvolvedora se recusou a disponibilizar o código-fonte do algoritmo, alegando segredo industrial.

O caso PredPol, por sua vez, está relacionado à previsão de zonas geográficas com maior incidência criminal. Utilizado por departamentos de polícia em cidades como Los Angeles e Chicago, o sistema analisa dados históricos de crimes para sugerir áreas que devem ser patrulhadas com maior intensidade (Moraes, 2022). À primeira vista, a lógica parece funcional: focar os esforços onde há maior risco. Contudo, como esses dados são oriundos de registros anteriores — que já refletem um padrão de policiamento seletivo — o algoritmo tende a intensificar a vigilância sobre comunidades marginalizadas, alimentando um ciclo de criminalização que reforça o viés já existente⁷.

Esses dois casos demonstram que, mesmo quando operam com bases estatísticas e dados aparentemente neutros, os algoritmos são atravessados por decisões humanas, por contextos históricos e por estruturas de poder. O risco, portanto, não está apenas no mau uso da tecnologia, mas em sua própria lógica de funcionamento, que tende a converter desigualdades sociais em probabilidades matemáticas.

A despeito das justificativas voltadas à eficiência e à modernização institucional, os sistemas de policiamento preditivo evidenciam uma contradição essencial: quanto mais refinada é a tecnologia utilizada, maior pode ser o risco de sua opacidade e de sua blindagem contra o controle democrático (Moraes, 2022). Em nome da sofisticação técnica, muitas dessas ferramentas tornam-se ininteligíveis aos usuários finais, às autoridades judiciárias e à sociedade civil. O resultado é a produção de decisões automatizadas que podem escapar do

⁵<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 3 abr. 2025.

⁶ “(...) Segundo o portal, réus negros detinham 77% mais probabilidade de serem considerados de maior risco de cometer um crime violento e 45% mais probabilidade de serem previstos para cometer um futuro crime de qualquer tipo.” (Angwin et al., 2016) (tradução livre).

⁷ O’neil (2020, p. 82 - 83), acrescenta que este modelo amplia áreas marginalizadas, isto porque o policiamento tende a se intensificar nos locais onde o sistema aponta como ‘alto risco’, a partir de uma análise geográfica, desta forma, cria-se um feedback nocivo de determinadas regiões e outras acabam sendo pouco fiscalizadas

crivo da legalidade e da proporcionalidade, abrindo margem para violações graves e sistemáticas de direitos.

A necessidade de regulação normativa desses sistemas tem mobilizado organismos internacionais, universidades e organizações não governamentais. A União Europeia, por exemplo, aprovou em 2024 o *Artificial Intelligence Act*, criando um regime jurídico específico para sistemas de IA. Entre suas inovações, está a categorização dos usos da IA conforme seu grau de risco, sendo os sistemas de policiamento e justiça criminal incluídos na categoria de “alto risco”. Como consequência, tais tecnologias passam a estar submetidas a exigências rigorosas, como a realização de avaliação prévia humana, auditabilidade e possibilidade de contestação dos indivíduos afetados⁸.

Essa abordagem, embora relevante e de grande evolução, encontra limitações práticas. Vejamos, a classificação de risco, por si só, não impede que algoritmos operem com dados enviesados, nem garante que suas decisões sejam compreensíveis. Como afirma Ruha Benjamin (2019), a IA, quando implementada em contextos marcados por desigualdade estrutural, tende a reproduzir essas disparidades sob a aparência de neutralidade matemática. A discriminação não se apresenta de forma direta ou intencional, mas se infiltra nos critérios de treinamento dos algoritmos, nos dados coletados e nas estruturas institucionais que os utilizam. Trata-se de uma nova forma de seletividade penal — mais silenciosa, mais automatizada e, portanto, mais difícil de contestar (Lucena, 2020).

Esse alerta também é reiterado por documentos recentes do Reino Unido, que têm reavaliado o uso de provas digitais em processos penais. Após o escândalo envolvendo o sistema *Horizon*, que gerou centenas de condenações injustas baseadas em evidências computacionais falhas⁹, o Ministério da Justiça britânico lançou em 2025 um *Call for Evidence* propondo a revisão das normas de admissibilidade de provas geradas por software¹⁰. A proposta inverte a lógica vigente: caberá à parte que apresentar a prova comprovar não apenas sua autenticidade, mas também a confiabilidade do sistema que a produziu. Essa mudança representa um avanço na responsabilização dos operadores da tecnologia e na proteção do direito de defesa, especialmente em sistemas onde o contraditório é frequentemente inviabilizado por barreiras técnicas ou comerciais, como o sigilo industrial sobre algoritmos proprietários.

⁸<https://artificialintelligenceact.eu/the-act/>. Acesso em: 3 abr. 2025.

⁹<https://time.com/6552764/uk-post-office-scandal-police-investigate-potential-fraud/>. Acesso em: 3 abr. 2025

¹⁰<https://www.gov.uk/government/calls-for-evidence/use-of-evidence-generated-by-software-in-criminal-proceedings/use-of-evidence-generated-by-software-in-criminal-proceedings-call-for-evidence>. Acesso em: 3 abr. 2025.

Esse cenário revela que os desafios do policiamento preditivo não se limitam à dimensão técnica ou regulatória. Ainda, apontam que a adoção de modelos algorítmicos em estruturas institucionais já marcadas por desigualdades transforma tais ferramentas em instrumentos de legitimação técnica da exclusão. Destaca-se que a lógica estatística dos algoritmos, ao ser alimentada por dados históricos enviesados, tende a consolidar uma criminalização automatizada de grupos vulnerabilizados, como habitantes de áreas periféricas e indivíduos racializados.

3. POLICIAMENTO PREDITIVO E REPRODUÇÃO DE DESIGUALDADES: O ALGORITMO COMO AGENTE DA SELETIVIDADE PENAL

Conforme abordado acima, a utilização de inteligência artificial na segurança pública, particularmente por meio de sistemas de policiamento preditivo, tem gerado preocupações crescentes no que tange à proteção dos direitos fundamentais e à perpetuação de desigualdades estruturais. Embora essas tecnologias sejam frequentemente apresentadas sob a promessa de eficiência e racionalidade, sua operação concreta revela a incidência de vieses que comprometem não apenas a neutralidade do processo, mas também a legitimidade da atuação estatal.

De início, cabe ressaltar que, por serem produto do intelecto humano, os algoritmos não são neutros, uma vez que refletem as escolhas e valores de seus criadores, os quais possuem suas próprias atribuições de valor à realidade e “por isso, os algoritmos estão sujeitos a terem os mesmos vieses sociais e culturais dos seus criadores” (De Freitas, 2023, p. 118)

No entanto, não é apenas na gênese algorítmica que está marcado tal enviesamento, mas também na execução do fim para o qual foi criado. Quando os algoritmos são treinados com registros oriundos de uma atuação policial historicamente seletiva – como ocorre em contextos marcados por desigualdades raciais, territoriais e socioeconômicas – há uma tendência à reprodução automática desses padrões discriminatórios. O viés, portanto, não resulta de um erro técnico isolado, mas da transposição acrítica de um passado excludente para a lógica da decisão automatizada.

Esse fenômeno, conhecido como *feedback loop*, passa a reforçar e reproduzir padrões enviesados pelo policiamento com base em dados historicamente contaminados. Isso ocorre porque os algoritmos são treinados com dados de ocorrências criminais registradas, os quais, por sua vez, refletem práticas seletivas, influenciadas por fatores como raça, classe social e localização geográfica. Desse modo, áreas que foram mais policiadas no passado - muitas

vezes bairros periféricos e racializados - tendem a ser classificadas como de maior risco e, portanto, recebem um maior patrulhamento no presente (Lum; Isaac, 2016). Deste feita, conforme Felipe de Oliveira Moraes:

Pessoas moradoras de determinados lugares com grande incidência criminal podem receber tratamentos diferenciados pelo simples fato de viverem em zonas quentes de criminalidade, pois o sistema quando baseado em índices sempre aponta aquela área como um local perigoso e propício de crimes futuros. Esses indivíduos podem ser alvo de um tratamento diferenciado, que de certo modo, justificado ou não, prejudica sua relação e inclusão social. Ter a força policial do estado sempre operando nas mesmas áreas e em outras não, além de possível constrangimento, poderá resultar em discriminação social (Moraes, 2022, p. 107).

Esse patrulhamento intensificado gera mais registros de incidentes independentemente de a criminalidade real ser maior, o que realimenta o sistema com dados que confirmam o suposto risco da região. Assim, o algoritmo passa a indicar essas áreas com ainda mais frequência, em um ciclo auto forçado e potencialmente injusto, configurando-se numa verdadeira distorção sistemática da realidade, que acaba reproduzindo e amplificando desigualdades sociais preexistentes.

Além disso, a confiança excessiva nas inferências geradas por algoritmos tende a deslocar a responsabilidade pelas decisões. Quando um agente público se ampara em um “alerta de risco” emitido por um sistema automatizado, ocorre uma espécie de deslocamento da responsabilidade (*accountability*), com a imputação da decisão a um ente tecnicamente neutro e, possivelmente, inalcançável do juridicamente falando. Assim, esse cenário pode dificultar a responsabilização por práticas discriminatórias e enfraquece o controle democrático sobre as instituições de segurança pública (De Araújo; Júnior; De Albuquerque, 2023).

Ao reforçarem padrões históricos de criminalização, os algoritmos contribuem para o agravamento da seletividade do sistema penal. Tal lógica preditiva opera, muitas vezes, com base em atributos agregados, como local de residência, rede de contatos ou padrões de mobilidade, convertendo indivíduos em alvos preferenciais de vigilância não em razão de condutas concretas, mas em função de perfis estatísticos, incompatível com os objetivos fundamentais dispostos no art. 3º da Constituição Federal¹¹, além princípios como a

¹¹Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil: I - construir uma sociedade livre, justa e solidária; II - garantir o desenvolvimento nacional; III - erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais; **IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.** (grifo nosso)

presunção de inocência, a legalidade estrita e a vedação ao tratamento discriminatório (Vieira, 2019).

Mais grave ainda é a possibilidade de que esses sistemas sejam utilizados para orientar decisões que envolvam, em algum grau, restrições de direitos¹², como abordagens, buscas pessoais, prisões preventivas ou recomendações em audiências de custódia. A antecipação da punição com base em supostas probabilidades de reincidência ou periculosidade transforma o aparato repressivo em um instrumento de punição preditiva, descolado da análise de fatos individualizados (Balduino, 2024).

Nessas condições, então, um circuito fechado de validação é gerado: algoritmos são treinados com dados contaminados por práticas discriminatórias, produzem diagnósticos enviesados e retroalimentam a base de dados com informações que reforçam as mesmas lógicas excludentes, consolidando uma tecnocracia penal sem espaço para revisão crítica dos padrões que reproduz. Tais sistemas, longe de corrigirem injustiças históricas, tendem a cristalizá-las sob uma capa de neutralidade técnica.

É difícil, pois, pensar ainda em um sistema guiado por algoritmos que elimine vieses indesejáveis, afinal “nenhum programa de policiamento preditivo é inteiramente objetivo, pois a sua construção envolve necessariamente decisões humanas, tais como a escolha de um modelo de previsão de risco em detrimento de outro e de determinados tipos de crimes” (De Freitas, 2023, p. 117) e não obstante os algoritmos detenham a capacidade de otimizar o trabalho humano e os recursos públicos, executando atividades que de outro modo seriam mais custosas ou mesmo menos eficientes, não se demonstra razoável considerar suficiente esse cenário para legitimar o uso desregulado¹³ dos sistemas de predição criminal orientado por sistemas computacionais.

A partir das contribuições da criminologia crítica, observa-se que o aparato punitivo estatal opera, muitas vezes, como instrumento de manutenção das desigualdades estruturais e de sustentação dos interesses vinculados à lógica capitalista (Vieira; Santos, 2025). Nesse panorama, o uso de tecnologias de policiamento preditivo surge como ferramenta que pode acentuar a vigilância dirigida a setores historicamente vulnerabilizados (Dias, 2022, p. 170). Tais dispositivos reforçam a seletividade penal ao intensificarem medidas repressivas voltadas a determinadas camadas sociais.

¹² Tal como ocorre nos EUA por via do Compas, conforme tratado no tópico 2.

¹³ Insta pontuar que, em 2022, foi proposta nos EUA a Lei de Responsabilidade Algorítmica (*S.2892 – AccountabilityAlgorithmicAct*). *AAAA* aborda as crescentes preocupações públicas a respeito do uso generalizado de sistemas de decisão automatizados (ADS) e propõe que as organizações que implementam tais sistemas tomem várias medidas concretas para identificar e mitigar os riscos sociais, éticos e legais. Até o momento do envio deste trabalho, a *AAA* ainda se encontra em tramitação no congresso americano.

Essa concepção de segurança, moldada por uma racionalidade que privilegia o controle social em detrimento da efetivação de direitos fundamentais, é sustentada por uma arquitetura de punição e monitoramento. A introdução de inovações tecnológicas no campo penal tende a reiterar lógicas excludentes, na medida em que direciona os mecanismos repressivos contra indivíduos socialmente estigmatizados, onde esses sujeitos são incorporados ao sistema não como destinatários de garantias, mas como fontes de dados que alimentam dinâmicas de vigilância, descoladas da promoção de sua dignidade (Arruda; Resende; Fernandes, 2022).

Não se demonstra demasiado afirmar, portanto, que essa digitalização e automação de práticas estatais de segurança traduzem uma ampliação de estratégias punitivas voltadas ao controle da pobreza, haja vista que os algoritmos aplicados nesses sistemas funcionam como engrenagens de uma vigilância sistêmica que reforça estruturas de repressão, contribuindo não apenas para o fortalecimento do sistema penal (no molde em que se encontra) e a reprodução de estereótipos sociais, mas também para a segregação espacial e social, promovendo uma divisão do espaço público conforme lógicas de exclusão (Firmino, 2018).

Assim sendo, a ausência de uma regulação específica para o uso de sistemas baseados em algoritmos e/ou inteligência artificial no sistema penal brasileiro intensifica os riscos já identificados no cenário internacional. A recente e embrionária adoção de sistemas preditivos em estados como São Paulo e Rio de Janeiro, sem mecanismos de controle social, transparência ou auditoria, evidencia um vácuo normativo preocupante. Em um país historicamente marcado pela seletividade racial e pela criminalização da pobreza, o uso de algoritmos não regulados pode aprofundar práticas discriminatórias já consolidadas, tornando o processo penal ainda mais excludente e assimétrico.

4. IMPLICAÇÕES JURÍDICAS E DESAFIOS REGULATÓRIOS: POR UMA INTELIGÊNCIA ARTIFICIAL TRANSPARENTE NO PROCESSO PENAL

A partir das reflexões expostas nos capítulos anteriores, torna-se evidente que a adoção de sistemas de policiamento preditivo, ainda que envolva na promessa de maior eficiência e racionalidade na segurança pública, traz consigo riscos substanciais à legalidade e à proteção dos direitos fundamentais. No plano jurídico, emerge um desafio central: como integrar essas inovações tecnológicas ao processo penal sem comprometer os pilares do Estado Democrático de Direito? A resposta exige um olhar atento tanto para os mecanismos

de admissibilidade da prova algorítmica quanto para os modelos de *accountability* e governança capazes de mitigar os riscos de decisões automatizadas opacas e discriminatórias.

No contexto brasileiro, a ausência de normativas específicas para disciplinar o uso de inteligência artificial no processo penal revela um vácuo normativo preocupante. Ainda que o art. 158-A e seguintes do Código de Processo Penal trate da cadeia de custódia das provas — inclusive digitais (Brasil, 1941) —, ele não contempla, de forma suficiente, as peculiaridades da produção probatória por algoritmos opacos ou por sistemas proprietários que impedem o contraditório efetivo. Doutrinadores como Prado (2021) e Badaró (2020) destacam que a quebra da cadeia de custódia pode ensejar a inadmissibilidade da prova digital, sobretudo quando não se demonstram a autenticidade e integridade dos elementos apresentados.

Nesse sentido, o ônus da prova algorítmica deve ser revisto. Diante da assimetria técnica entre as partes processuais e os desenvolvedores dos sistemas de IA, parece mais razoável que recaia sobre quem apresenta a prova o dever de demonstrar a confiabilidade do algoritmo utilizado — inclusive quanto aos seus parâmetros técnicos, dados de treinamento e funcionamento decisório. Essa carga do ônus é coerente com o movimento internacional de revisão da admissibilidade das provas digitais, como evidenciado no recente "*Call for Evidence*" do Ministério da Justiça britânico (2025), o qual propõe que a parte que deseja utilizar software como meio de prova deve comprovar não apenas sua autenticidade, mas também a robustez e auditabilidade do sistema tecnológico envolvido.

Ainda no plano internacional, vale rememorar, uma vez mais, o *Artificial Intelligence Act*. Este, conforme já delimitado, visa classificar os diferentes níveis de risco de sistemas de IA. No caso da justiça criminal e o policiamento preditivo, dentre as exigências já mencionadas no capítulo inicial deste trabalho, ainda se inclui: a obrigação de avaliação prévia de impacto sobre direitos fundamentais, ainda, garantir a manutenção da contestação dos indivíduos.

Essas diretrizes se mostram cruciais em um cenário no qual a opacidade algorítmica não dialoga com os princípios do devido processo legal. Como sublinhado por Vieira e Santos (2025), o uso de inteligência artificial no processo penal exige uma adaptação epistemológica e normativa, pois os sistemas de IA não operam com critérios hermenêuticos típicos da decisão jurídica, mas com parâmetros estatísticos que não captam a singularidade do caso.

Ainda sob este cenário, o Reino Unido também avançou no debate regulatório. Após os escândalos envolvendo falhas de software no sistema judicial, o país propôs alterações legislativas que reforçam a exigência de auditoria dos algoritmos utilizados como prova e a responsabilidade das autoridades judiciais na aferição técnica dessas ferramentas (Vieira;

Santos, 2025). Em ambos os casos, a tônica é clara: a legitimidade da prova digital deve ser construída a partir da transparência, da explicabilidade e da possibilidade de contestação jurídica efetiva.

Diante desse panorama, é imperioso refletir sobre alternativas de governança algorítmica que possam ser compatíveis com os valores constitucionais. O conceito de *accountability* algorítmica ganha centralidade nesse debate, significando a exigência de que os sistemas tecnológicos empregados pelo Estado sejam submetidos a mecanismos contínuos de supervisão pública, auditoria independente e responsabilização em caso de violação de direitos. Como adverte o *Boletín de Inteligencia Artificial* (2025), a política democrática não pode ser reduzida a um exercício técnico de otimização de resultados; trata-se de um campo onde os objetivos precisam ser discutidos e legitimados politicamente, e não apenas calculados.

Nesse sentido, as propostas de *accountability* e de uma governança algorítmica democrática não se limitam à mera publicização dos sistemas utilizados, mas exigem a criação de estruturas institucionais específicas para acompanhamento, fiscalização e controle contínuo desses mecanismos. Conforme defende Marcelo Varela (2013), a complexidade das tecnologias digitais exige que os processos de responsabilização não sejam pensados de forma pontual ou exclusivamente judicial, mas estruturados em camadas: controle legislativo, revisão judicial, participação da sociedade civil e, especialmente, auditorias técnicas independentes capazes de atestar a conformidade dos algoritmos com os direitos fundamentais.

Essa perspectiva também tem sido discutida por autores que abordam o fenômeno da governança transversal dos direitos fundamentais frente à inovação tecnológica. Como destaca Campos (2022, p. 432 - 437), o direito não pode mais operar isoladamente da técnica. As decisões judiciais que envolvem tecnologias algorítmicas exigem uma nova arquitetura institucional que articule saberes técnicos e jurídicos, promovendo uma racionalidade deliberativa e democrática. Isso significa reconhecer que os sistemas de IA não devem apenas ser auditáveis, mas também compreensíveis e contestáveis por todos os envolvidos no processo, incluindo os acusados, seus defensores, Ministério Público e juízes.

A adoção de modelos de “IA explicável” (*explainable AI*), já defendida em diversas jurisdições, constitui um passo relevante na construção dessa governança¹⁴. Trata-se de

¹⁴Silva (2024, p. 39 - 40), explica que o termo ‘IA explicável’ refere-se “à capacidade de compreender e explicar os processos de tomada de decisão dos modelos de inteligência artificial (...) à capacidade de compreender e explicar os processos de tomada de decisão dos modelos de inteligência artificial”.

estabelecer critérios técnicos mínimos de transparência algorítmica, incluindo documentação acessível, lógica decisória legível e capacidade de verificação dos resultados. A implementação desses critérios deve ser exigida especialmente nas áreas sensíveis, como o sistema penal, onde as decisões têm potencial para afetar diretamente a liberdade dos indivíduos (Silva, 2024). Sem isso, como afirma Pasquale (2016), perpetua-se a chamada “sociedade da caixa-preta”, na qual decisões são tomadas por sistemas cuja lógica permanece inacessível, impedindo o controle democrático e jurídico sobre o poder público.

No caso brasileiro, é fundamental que o debate sobre a regulação da inteligência artificial avance para além de iniciativas genéricas e se volte com atenção às especificidades do processo penal. Propostas legislativas como o PL n. 2338/2023, que se encontra a caminho da deliberação da Câmara dos Deputados,¹⁵ carece de dispositivos que tratem com profundidade da admissibilidade de provas algorítmicas, da responsabilidade por falhas técnicas e da exigência de transparência dos sistemas. Neste cenário, a experiência comparada demonstra que, sem diretrizes normativas claras, o risco de decisões judiciais amparadas por sistemas opacos aumenta, comprometendo a confiabilidade do processo e a efetividade das garantias processuais.

Ao mesmo tempo, é preciso reconhecer que a regulação da inteligência artificial no processo penal não pode se limitar à criação de normas genéricas ou à simples importação de modelos estrangeiros. O caso brasileiro, com seu histórico de seletividade penal, racismo estrutural e desigualdade de acesso à justiça, exige soluções normativas que considerem as especificidades do sistema jurídico nacional. Como apontam Vieira e Santos (2025), é necessário repensar os próprios fundamentos do uso da tecnologia no processo penal, assegurando que o avanço digital não sirva como instrumento de legitimação técnica da exclusão social, mas sim como ferramenta de promoção da igualdade, da dignidade e da justiça.

Portanto, as alternativas regulatórias devem se concentrar na imposição de deveres concretos de transparência às autoridades públicas e às empresas contratadas, na garantia de mecanismos de fiscalização por órgãos autônomos e na criação de estruturas jurídicas que permitam o controle social efetivo sobre os sistemas algorítmicos. A construção de uma inteligência artificial compatível com a democracia exige que suas decisões possam ser compreendidas, auditadas e, sobretudo, contestadas. Isso implica a rejeição de qualquer presunção de confiabilidade automática, a imposição de obrigações de prestação de contas e o

¹⁵<https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em 02 abr. 2025.

reconhecimento de que, no processo penal, o controle tecnológico não pode jamais se sobrepor ao controle jurídico.

Por fim, se reconhece que os desafios impostos pela inteligência artificial ao processo penal são de natureza complexa, transversal e estrutural. A resposta a esses desafios não está apenas em soluções técnicas, mas na reafirmação de um compromisso político-jurídico com a transparência, a equidade e a proteção incondicional dos direitos fundamentais.

5. CONCLUSÃO

O presente estudo buscou analisar o uso da inteligência artificial no policiamento preditivo, a partir de uma abordagem interdisciplinar que combinou fundamentos técnicos, jurídicos e institucionais. A investigação se concentrou nos possíveis impactos dessa tecnologia sobre o processo penal, particularmente no que se refere à proteção de direitos fundamentais, à admissibilidade de provas digitais e aos desafios regulatórios associados à sua implementação.

No decorrer dos capítulos, foi possível observar que os sistemas de policiamento preditivo operam com base em tecnologias como *machinelearning* e análise de big data, aplicadas ao mapeamento de padrões criminais e à formulação de zonas de risco. Apesar de sua finalidade declarada de contribuir para maior eficiência no combate à criminalidade, verificou-se que o funcionamento desses sistemas depende, em grande medida, da qualidade e da neutralidade dos dados utilizados. Quando alimentados por informações que refletem práticas históricas seletivas, há possibilidade de que os algoritmos reproduzam ou reforcem padrões já existentes no sistema de justiça criminal.

A análise de casos práticos, como os sistemas COMPAS e PredPol, revelou que a utilização de dados históricos pode influenciar decisões operacionais e judiciais com base em probabilidades, o que pode acarretar desafios em relação à transparência, à auditabilidade e à conformidade com os princípios processuais. Esses elementos foram retomados na discussão jurídica sobre a admissibilidade da prova algorítmica, destacando-se a importância de garantir mecanismos que assegurem o contraditório e a ampla defesa nos processos em que tais ferramentas forem utilizadas.

No campo regulatório, foram examinadas experiências internacionais, como o *Artificial Intelligence Act* da União Europeia e os debates promovidos no Reino Unido após o caso *Horizon*, os quais apontam para a necessidade de critérios normativos que estabeleçam padrões mínimos de governança, responsabilidade e controle dos sistemas algorítmicos. A adoção de práticas como a exigência de avaliação de impacto, transparência dos parâmetros

utilizados e mecanismos de revisão técnica independentes aparece como possível alternativa para lidar com a complexidade dessas ferramentas no contexto jurídico.

No caso brasileiro, observou-se a inexistência de um marco legal específico sobre o uso de inteligência artificial no processo penal. A legislação vigente, embora contemple dispositivos sobre a cadeia de custódia de provas digitais, ainda não regulamenta aspectos centrais da produção e utilização de provas automatizadas. Nesse cenário, experiências comparadas podem contribuir para a formulação de diretrizes normativas que contemplem as especificidades do sistema jurídico nacional e que promovam um equilíbrio entre inovação tecnológica e observância das garantias constitucionais.

Sendo assim, observa-se que a incorporação de tecnologias de inteligência artificial no sistema penal requer não apenas uma atualização normativa, mas também o desenvolvimento de estruturas institucionais capazes de garantir controle, fiscalização e compreensão sobre o funcionamento dessas ferramentas. A construção de um modelo de governança algorítmica voltado à transparência e à responsabilidade pode representar um passo importante para assegurar que a aplicação de novas tecnologias se mantenha alinhada aos princípios fundamentais do processo penal e à legalidade democrática.

REFERÊNCIAS:

ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. *Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks*. ProPublica, 23 maio 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 3 de abril. 2025.

BADARÓ, Gustavo Henrique Righi Ivahy. **Processo penal: provas**. 2. ed. São Paulo: Revista dos Tribunais, 2020.

BAER, T. **Understand, manage, and prevent algorithmic bias: a guide for business users and data scientists**. Nova Iorque: Apress, 2019. Disponível em: <https://doi.org/10.1007/978-1-4842-4885-0>. Acesso em: 3 de abril de 2025.

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. **California Law Review**, v. 104, p. 671-732, 2016. Disponível em: <https://ssrn.com/abstract=2477899>. Acesso em: 3 de abril de 2025.

BENJAMIN, Ruha. *Race after technology: Abolitionist tools for the new Jim Code*. Cambridge: Polity Press, 2019.

BORGES, Aline de Fátima Soares. **Uso estratégico da Inteligência Artificial nas organizações**. 2023. Tese (Doutorado em Ciências) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2023. Disponível em:

<https://www.teses.usp.br/teses/disponiveis/3/3136/tde-12092023-074354/publico/AlinedeFatimaSoaresBorgesCorr23.pdf>. Acesso em: 09 de fevereiro de 2025.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016].

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Diário Oficial da União: seção 1, p. 23913, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 2 abr. 2025.

BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Call for evidence: The use of evidence generated by software in criminal proceedings**. London: The Stationery Office, 2025. Disponível em: <https://assets.publishing.service.gov.uk>. Acesso em: 30 mar. 2025.

CAMPOS, Ricardo. **Metamorfoses do Direito Global**: sobre a interação entre Direito, tempo e tecnologia. São Paulo: Contracorrente, 2022.

DE ARAUJO, Valter Shuenquener; JUNIOR, Júlio José Araujo; DE ALBUQUERQUE, Lucca Fernandes. Policiamento preditivo na era da vigilância: a busca de um modelo constitucional e democrático. **Quaestio Iuris**, v. 16, n. 1, p. 313-337, 2023. Disponível em: https://www.academia.edu/download/102028765/V_16_N_01_2023.pdf. Acesso em 07 de abril de 2025.

DE FREITAS, IandaraBergamaschi. Policiamento Preditivo: aspectos discriminatórios no uso das novas tecnologias. **Revista de Direito, Governança e Novas Tecnologias**, v. 9, n. 1, p. 113–129, 2023. Disponível em: <https://core.ac.uk/download/pdf/581035190.pdf>. Acesso em: 07 de abril de 2025.

DIAS, F. V. **Criminologia midiática e tecnopolítica**. São Paulo: Tirantloblanch, 2022.

EUROPOL. **Europol Innovation Lab – Strategic report: Innovation and AI in law enforcement**. The Hague: Europol, 2023. Disponível em: <https://www.europol.europa.eu>. Acesso em: 30 de março de 2025.

FIRMINO, R. J. Securitização, vigilância e territorialização em espaços públicos. In: BRUNO, F. et al (orgs.). **Tecnopolíticas da vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018. Disponível em: https://medialabufrj.net/wp-content/uploads/2020/10/Tecnopoliticas-da-vigilancia_mioilo_download.pdf. Acesso em: 07 de abril de 2025.

FORNASIER, Mateus de Oliveira. **Cinco questões ético-jurídicas fundamentais sobre a inteligência artificial**. Rio de Janeiro: Lumen Juris, 2021.

INNERARITY, Daniel. A política em tempos de indignação. Tradução de Antonio Paim. São Paulo: Estação Liberdade, 2021.

LUCENA, Pedro Arthur Capelari de. **Viés e racismo no policiamento preditivo**: casos estadunidenses e os reflexos de conexão com o Brasil. **Revista de Direito e as Novas Tecnologias**. vol. 7, abr./jun 2020. Disponível em: <https://www.thomsonreuters.com.br/content/dam/ewp-m/documents/brazil/pt/pdf/other/rdtec-7-vies-e-racismo-no-policiamento-preditivo.pdf>. Acesso em 7 abr. 2025.

HAUGELAND, J. **Artificial Intelligence: the very idea**. Cambridge, Massachusetts: MIT Press, 1985.

LUM, Kristian; ISAAC, William. To predict and serve? **Significance**, v. 13, n. 5, p. 14-19, 2016. Disponível em: <https://academic.oup.com/jrssig/article-abstract/13/5/14/7029190>. Acesso em: 07 de abril de 2025.

MORAES, Felipe Oliveira de. **Policiamento Preditivo e aspectos constitucionais**. São Paulo: Dialética. 2022.

NOBLE, Safiya Umoja. **Algorithms of oppression**: How search engines reinforce racism. New York: NYU Press, 2018.

O'NEIL, Cathy. **Algoritmos de destruição em massa**: como o big data aumenta a desigualdade e ameaça a democracia. Tradução Rafael Abraham. 1. ed. Santo André, SP: Editora Rua do Sabão, 2020.

PASQUALE, Frank. **The black box society**: The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PRADO, Geraldo. **Sistemas de provas no processo penal brasileiro**. 2. ed. São Paulo: Marcial Pons, 2021.

PROPUBLICA. Machine Bias – **There's software used across the country to predict future criminals. And it's biased against blacks**. 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 30 mar. 2025.

RODRIGUES JUNIOR, Manuel Salgueiro. **Accountability, transparência e controle social**. Fortaleza: Editora da UECE, 2024. ISBN 978-85-7826-941-8.

SACKMAN, Sarah. **The use of evidence generated by software in criminal proceedings**. London: Government Digital Service, 2023. Disponível em: <https://assets.publishing.service.gov.uk/media/67892f5a93d4eae3088bd324/use-evidence-generated-software-criminal-proceedings.pdf>. Acesso em: 2 abr. 2025.

SCHALKOFF, RJ. **Motor de inteligência artificial**. Nova York: McGraw-Hill, 1990.

SILVA, Bruno Cassol da. **Inteligência artificial explicável e decisões judiciais**: experimentações com o método SHAP. 2024. Dissertação (Mestrado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2024. Disponível em: <https://repositorio.ufsc.br/handle/123456789/254969>. Acesso em: 2 de abril de 2025.

VALDÉS, Dayse de A. Y. **Dever de Prestar Contas e Responsabilidade Administrativa: evolução de conceitos e aplicação na administração pública brasileira**. Revista de Informação Legislativa. Brasília. p. 25, n. 99, p. 29-56, jul./set. 1988.

VARELLA, Marcelo Dias. **Internacionalização do Direito: direito internacional, globalização e complexidade**. Brasília: UniCEUB, 2013.

VEGA, Ignacio Gonzalez. Desafios y riesgos en la aplicación de la IA en el Poder Judicial. In: JUEZAS Y JUECES PARA LA DEMOCRACIA. **Boletín de Inteligencia Artificial**. Vol. IV. Madrid: Juezas y Jueces para la Democracia, 15 jan. 2025. Disponível em: <https://www.juecesdemocracia.es/wp-content/uploads/2025/01/Boletin-Inteligencia-Artificial-Volumen-IV.pdf>. Acesso em: 3 abr. 2025.

VIEIRA, Andrey Bruno Cavalcante; SANTOS, Hugo Leonardo Rodrigues. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 11, n. 1, p. 403–432, jan./abr. 2025. Disponível em: <https://doi.org/10.22197/rbdpp.v11i1>. Acesso em: 30 mar. 2025.

VIEIRA, Leonardo Marques. A problemática da inteligência artificial e dos vieses algorítmicos: caso COMPAS. In: **Brazilian Technology Symposium**. 2019.

WINSTON, P.H. **Aprendendo descrições estruturais a partir de exemplos**. Massachusetts: Instituto de Tecnologia de Massachusetts, 1970.