CAPÍTULO 7

Policiamento Preditivo e Direitos Humanos na Amazônia: Entre a Inovação Tecnológica e a Vulnerabilização das Periferias

https://doi.org/10.22533/at.ed.433142508077

Edinaldo Inocencio Ferreira Junior

André Marques Araújo

Diogo Bruno Siqueira de Andrade

Ademar Yasuo Minori Júnior

Ana Karoline de Souza Ferreira

Nubya Cristiana Teixeira Bezerra

RESUMO: O avanço do policiamento preditivo no Brasil, impulsionado por tecnologias de inteligência artificial e análise de dados, tem despertado preocupações sobre seus impactos em contextos marcados por desigualdade estrutural. Este capítulo analisa criticamente a aplicação dessas ferramentas na Amazônia urbana, território caracterizado por favelização, invisibilidade institucional e seletividade penal historicamente dirigida às populações periféricas e racializadas. O objetivo é investigar em que medida o uso de algoritmos na segurança pública pode agravar processos de criminalização automatizada e violação de direitos fundamentais. A justificativa da pesquisa baseia-se na ausência de marcos regulatórios nacionais que orientem o uso ético dessas tecnologias, bem como na urgência de incorporar salvaguardas jurídicas que considerem as especificidades socioespaciais amazônicas. Adota-se como metodologia a revisão crítica de literatura nacional e internacional, com destaque para O'Neil (2017), Eubanks (2018), Richardson et al. (2019) e documentos do Fórum Brasileiro de Segurança Pública, além da análise de experiências regulatórias como o caso SyRI, na Holanda, e o GDPR europeu. Os resultados apontam riscos concretos de injustiça algorítmica, reforço da seletividade estatal e violação da privacidade.

Conclui-se que, sem controle social e normativo, o policiamento preditivo tende a intensificar desigualdades já existentes. Propõem-se, ao final, diretrizes para uma governança algorítmica compatível com os princípios democráticos e os direitos humanos.

PALAVRAS-CHAVE: Amazônia urbana; Direitos humanos; Governança de dados; Injustiça algorítmica; Policiamento preditivo.

Predictive Policing and Human Rights in the Amazon: Between Technological Innovation and the Vulnerabilization of the Peripheries

ABSTRACT: The advancement of predictive policing in Brazil, driven by artificial intelligence and data analysis technologies, has raised concerns about its impact in contexts marked by structural inequality. This chapter critically analyzes the application of such tools in the urban Amazon, a territory characterized by informal settlements, institutional invisibility, and historically selective penal practices directed at peripheral and racialized populations. The objective is to investigate the extent to which the use of algorithms in public security may aggravate processes of automated criminalization and violations of fundamental rights. The rationale for this research lies in the absence of national regulatory frameworks to guide the ethical use of these technologies, as well as the urgency of incorporating legal safeguards that consider the socio-spatial specificities of the Amazon. The methodology adopted involves a critical review of national and international literature, highlighting works by O'Neil (2017), Eubanks (2018), Richardsone et al. (2019), and documents from the Brazilian Public Security Forum, in addition to the analysis of regulatory experiences such as the SyRI case in the Netherlands and the European GDPR. The results indicate concrete risks of algorithmic injustice, reinforcement of state selectivity, and privacy violations. The chapter concludes that, in the absence of social and legal oversight, predictive policing tends to intensify pre-existing inequalities. It ultimately proposes guidelines for algorithmic governance compatible with democratic principles and human rights.

KEYWORDS: Algorithmic injustice; Data governance; Human rights; Predictive policing; Urban Amazon;

INTRODUÇÃO

A adoção de tecnologias baseadas em inteligência artificial (IA), análise de big data e algoritmos de previsão criminal tem modificado profundamente as estratégias de atuação das instituições de segurança pública em diversas partes do mundo. No Brasil, ainda que de forma incipiente, o policiamento preditivo tem ganhado espaço como promessa de racionalização da gestão do policiamento ostensivo e de maximização da eficiência operacional das forças de segurança. Essa modalidade de policiamento busca antecipar delitos por meio da análise de dados históricos, padrões de ocorrência e variáveis geoespaciais, apresentando-se como solução técnica para o enfrentamento da criminalidade e a melhoria da alocação de recursos (Ferguson, 2017).

Nos últimos anos, a segurança pública brasileira tem enfrentado um cenário de complexidade crescente, caracterizado por altos índices de violência, sobrecarga dos sistemas policiais e escassez de recursos humanos e materiais. Nesse contexto, a adoção de tecnologias de análise preditiva é vista por gestores públicos como uma resposta estratégica à necessidade de racionalizar recursos e promover maior eficácia nas ações preventivas. A expectativa é que, por meio do cruzamento de grandes volumes de dados e da identificação de padrões criminais recorrentes, seja possível antecipar delitos, identificar locais e horários de maior risco, e planejar ações policiais com base em critérios técnico-científicos (Lucena, 2019). O uso dessas tecnologias, entretanto, não é isento de controvérsias. Autores como Ferguson (2017) e Brayne (2021) alertam para o risco de que esses sistemas, ao se basearem em dados históricos enviesados, reforcem padrões de criminalização seletiva, legitimando práticas discriminatórias sob o verniz de objetividade algorítmica. No Brasil, onde as estatísticas criminais refletem um histórico de ações policiais marcadas por seletividade penal e racismo estrutural, a aplicação acrítica dessas ferramentas pode intensificar a vigilância sobre determinados territórios — sobretudo os periféricos —, aprofundando desigualdades e violações de direitos fundamentais (Minayo, 2006).

Na Amazônia urbana, esse cenário é ainda mais sensível. Cidades como Manaus, Belém, Porto Velho e Macapá apresentam altos índices de violência letal, marcada por uma distribuição espacial concentrada nas periferias e por um histórico de ausência do Estado em áreas de vulnerabilidade (IPEA, 2023). A adoção do policiamento preditivo nesses contextos requer uma análise aprofundada de seus efeitos sociais e institucionais, pois, ao operar com base em dados produzidos por instituições marcadas por desigualdades estruturais, os sistemas preditivos podem não apenas reproduzir, mas também amplificar práticas de repressão seletiva e exclusão social (Richardson et al., 2019).

Diante disso, é imprescindível que o debate sobre o uso de tecnologias preditivas na segurança pública vá além do entusiasmo técnico e se volte para uma reflexão crítica e ética sobre os limites, as potencialidades e os riscos dessas ferramentas. A governança algorítmica deve estar pautada pela transparência, pela responsabilidade institucional e pelo compromisso com os direitos humanos — especialmente em territórios historicamente vulnerabilizados como os da Amazônia urbana (Eubanks, 2018).

Contextualização

O avanço do policiamento preditivo no Brasil está inserido em um processo mais amplo de transformação digital da administração pública, impulsionado por políticas de modernização estatal, incentivo à inovação tecnológica e aumento da demanda social por respostas mais eficazes à criminalidade urbana. Essa transição tem estimulado o uso de tecnologias emergentes em diversas áreas da gestão pública, incluindo a segurança, onde se intensifica o uso de sistemas informatizados, bancos de dados interconectados e softwares de análise preditiva (Vieira; Santos, 2025). Especificamente na área de segurança pública, a incorporação de soluções baseadas em IA, georreferenciamento e mineração de dados tem sido incentivada como estratégia para enfrentar os desafios da criminalidade complexa, da escassez de efetivo e da pressão por resultados. Ferramentas como o PredPol, nos Estados Unidos, e sistemas similares testados no Brasil, propõem antecipar delitos com base em análises estatísticas de ocorrências anteriores, perfil de reincidência e distribuição espacial da violência (Ferguson, 2017).

Contudo, o contexto brasileiro — e mais especificamente o amazônico — impõe peculiaridades que relativizam essa expectativa de neutralidade técnica. As bases de dados utilizadas pelas instituições policiais brasileiras são, em grande medida, derivadas de boletins de ocorrência, relatórios de patrulhamento e registros administrativos frequentemente marcados por subnotificação, inconsistência e forte seletividade. Como aponta Eubanks (2018), quando os dados que alimentam os sistemas algorítmicos refletem desigualdades históricas, esses mesmos sistemas tendem a reproduzir — e até intensificar — essas distorções.

Na Amazônia urbana, essa crítica se torna ainda mais relevante. Cidades como Manaus, com territórios marcados por ocupações irregulares, ausência de serviços públicos básicos e relações tensas entre comunidades periféricas e forças de segurança, tornam-se espaços propensos à reprodução do viés algorítmico. O policiamento preditivo, nesse cenário, tende a reforçar a presença estatal em áreas já historicamente sobrepoliciadas, enquanto perpetua a invisibilidade institucional em outros territórios igualmente vulneráveis, porém com menor visibilidade estatística (Miranda; Schnedier,

2020). Ademais, a infraestrutura tecnológica necessária para a plena execução dessas ferramentas ainda é precária em muitas regiões da Amazônia, o que agrava a dependência de sistemas centralizados e compromete a transparência na gestão dos dados. Isso evidencia a urgência de incorporar ao debate sobre segurança pública algoritmos que sejam regulados por marcos legais específicos, auditáveis e compatíveis com os princípios constitucionais de legalidade, isonomia e dignidade humana (BRASIL, 1988; Maciel, 2025).

Portanto, a contextualização do policiamento preditivo no Brasil não pode prescindir de uma análise crítica sobre o ambiente socioterritorial em que essas tecnologias são implementadas, tampouco ignorar os riscos de agravamento das desigualdades quando a inovação tecnológica é dissociada de uma governança ética e comprometida com os direitos humanos.

Problematização

A implementação do policiamento preditivo em contextos profundamente marcados por desigualdades sociais, como as periferias urbanas da Amazônia, levanta preocupações éticas, jurídicas e políticas de alta relevância. Em regiões como Manaus, Belém e Porto Velho, observa-se uma histórica ausência do Estado, associada à seletividade penal que afeta de maneira desproporcional populações negras, indígenas e empobrecidas (IPEA, 2023; Minayo, 2006). Nessas áreas, a suposta neutralidade dos algoritmos pode ser comprometida pela base de dados enviesada que sustenta os modelos preditivos, muitas vezes alimentada por estatísticas produzidas por práticas policiais discriminatórias.

Essa realidade faz emergir o risco de que as ferramentas tecnológicas, ao invés de corrigirem injustiças, venham a legitimá-las sob a aparência de objetividade matemática. Como advertem Eubanks (2018) e Richardson et al. (2019), os algoritmos refletem os valores e vieses de quem os projeta e de quem fornece os dados. Assim, sua aplicação em ambientes já estigmatizados pode aprofundar o ciclo repressivo e invisibilizar ainda mais as violações de direitos fundamentais. A Amazônia urbana, portanto, constitui não apenas um espaço de aplicação dessas ferramentas, mas um campo de disputa por justiça algorítmica e governança democrática da segurança pública.

Objetivos

Este capítulo tem como objetivo geral analisar criticamente em que medida o uso de algoritmos e tecnologias de IA no campo da segurança pública, com foco na Amazônia urbana, pode intensificar processos de criminalização automatizada, aprofundar a seletividade penal e gerar violações de direitos fundamentais, como os direitos à igualdade, à privacidade e à não discriminação.

Como objetivos específicos, propõe-se:

- Investigar o contexto socioespacial da Amazônia urbana e sua relação com padrões históricos de seletividade penal e invisibilidade institucional;
- Identificar os principais riscos éticos e jurídicos associados à aplicação do policiamento preditivo em territórios socialmente vulneráveis;
- Analisar criticamente os fundamentos teóricos e técnicos do policiamento algorítmico e sua aplicabilidade no Brasil;
- Avaliar experiências internacionais de regulação e controle do uso de algoritmos na segurança pública, com destaque para os casos do Sistema de Registro de Riscos (SyRI) (Holanda) e Regulamento Geral sobre a Proteção de Dados (GDPR) (União Europeia);
- Propor diretrizes para uma governança algorítmica orientada pelos princípios dos direitos humanos, com ênfase na realidade amazônica.

Justificativa

A relevância deste estudo reside na ausência de um marco legal nacional que regulamente o uso de tecnologias preditivas pela administração pública, sobretudo no campo da segurança pública. A inexistência de diretrizes claras sobre transparência algorítmica, responsabilidade institucional e respeito aos direitos fundamentais abre margem para aplicações indiscriminadas e potencialmente abusivas, especialmente em contextos marcados por vulnerabilidades históricas. A Amazônia urbana, nesse sentido, constitui um lócus emblemático: trata-se de uma região caracterizada por alta densidade populacional periférica, presença insuficiente do Estado, precariedade nos serviços públicos e índices persistentes de violência estrutural. Ao mesmo tempo, o avanço das tecnologias de vigilância baseadas em IA e big data ocorre em ritmo acelerado, sem que as especificidades socioespaciais do território amazônico sejam consideradas nos desenhos institucionais dessas políticas. A ausência de uma abordagem interseccional que leve em conta variáveis como raça, classe, território e histórico de exclusão institucional torna urgente a produção de conhecimento crítico e situado sobre o tema. Populações negras, indígenas e periféricas correm o risco de se tornarem alvos privilegiados de uma vigilância automatizada e enviesada, mascarada por uma pretensa neutralidade tecnológica.

Dessa forma, o presente capítulo contribui para o debate acadêmico e político ao investigar os limites, riscos e potenciais impactos do policiamento preditivo na Amazônia urbana, buscando subsidiar uma governança algorítmica compatível com os princípios democráticos e com a proteção dos direitos humanos.

Metodologia

A presente pesquisa adota uma abordagem qualitativa, com base em revisão crítica da literatura especializada, nacional e internacional, buscando compreender os impactos sociais, éticos e jurídicos do policiamento preditivo em contextos marcados por desigualdades estruturais. A metodologia fundamenta-se na análise documental e bibliográfica, priorizando autores que tratam das intersecções entre tecnologia, justiça social e direitos humanos, como Cathy O'Neil (2017), Virginia Eubanks (2018) e Rashida Richardson et al. (2019).

Essas autoras discutem como os sistemas algorítmicos, ao serem aplicados em ambientes de vulnerabilidade social, tendem a reproduzir e amplificar preconceitos e desigualdades históricas. A leitura de obras como "Weapons of Math Destruction" (O'Neil, 2017) e "Automating Inequality" (Eubanks, 2018) fornece um marco teórico robusto para compreender os riscos da discriminação automatizada e da opacidade algorítmica, enquanto Richardson et al. (2019) contribuem com dados empíricos e argumentos sobre os efeitos do viés institucional nos sistemas de IA.

Paralelamente, a pesquisa se apoia na análise de experiências internacionais de regulação do uso de algoritmos na administração pública, como o caso SyRI, na Holanda, considerado inconstitucional por violar o princípio da não discriminação e o direito à privacidade. Além disso, examina-se o GDPR, vigente na União Europeia desde 2018, que estabelece parâmetros importantes sobre transparência, finalidade e responsabilidade no uso de dados pessoais por agentes públicos e privados. No contexto brasileiro, são utilizados relatórios, estudos e dados empíricos fornecidos por instituições como o Fórum Brasileiro de Segurança Pública (FBSP), que têm documentado o uso crescente de tecnologias de vigilância e suas repercussões nas dinâmicas de policiamento e controle social. Essa triangulação metodológica permite articular o debate teórico com dados práticos e contextuais, possibilitando uma compreensão crítica e territorializada dos desafios impostos pela adoção do policiamento preditivo na Amazônia urbana.

A escolha dessa metodologia visa não apenas descrever, mas interpretar os significados e implicações sociais da implementação de tecnologias algorítmicas no campo da segurança pública, especialmente em regiões negligenciadas pelas políticas estatais. O estudo, assim, busca subsidiar propostas de governança algorítmica que respeitem os princípios constitucionais e promovam justiça social em territórios historicamente vulnerabilizados.

FUNDAMENTOS TEÓRICOS E CONCEITUAIS

Policiamento Preditivo: Conceitos e Aplicações

O policiamento preditivo pode ser definido como o uso de tecnologias estatísticas e algoritmos baseados em dados históricos de criminalidade para prever onde e quando delitos podem ocorrer. A lógica central por trás dessa prática está na antecipação de comportamentos criminais, possibilitando que as forças de segurança pública direcionem recursos, agentes e ações de forma mais eficiente e estratégica (Perry, 2013). Essa abordagem insere-se em um movimento mais amplo de modernização da gestão da segurança pública, que se orienta pela lógica da governança por dados e da suposta objetividade algorítmica (Brantingham; Brantingham, 2013).

Entre os modelos mais utilizados, destacam-se os sistemas baseados em regressão estatística, redes neurais artificiais, Random Forest, e os modelos ARIMA (Auto Regressive Integrated Moving Average). Essas ferramentas processam grandes volumes de dados sobre localização, horários, tipos de ocorrência, perfis de indivíduos envolvidos e outras variáveis contextuais, oferecendo mapas de calor ou zonas de atenção que orientam o policiamento ostensivo (Ferguson, 2017). A literatura internacional sugere que a promessa de eficiência operacional e prevenção de crimes tem levado diversas cidades a adotarem o policiamento preditivo como política pública. Nos Estados Unidos, por exemplo, o sistema PredPol foi implementado em cidades como Los Angeles, Santa Cruz e Chicago, com a alegação de que poderia reduzir os índices criminais por meio da alocação estratégica de patrulhas (Nakashima, 2024). Já na Europa, experiências mais cautelosas têm ocorrido, especialmente em países como Reino Unido e Alemanha, onde as preocupações com a proteção de dados e os direitos civis têm levado a testes mais restritos e acompanhados por comitês de ética (ZAVRŠNIK, 2020).

No Brasil, a aplicação do policiamento preditivo ainda se encontra em fase experimental e pouco documentada, sendo associada a iniciativas pontuais em estados como São Paulo, Bahia e Rio de Janeiro, geralmente articuladas com centros de comando e controle e sistemas de videomonitoramento urbano (FBSP, 2022). A ausência de dados transparentes sobre os critérios de funcionamento desses sistemas, bem como a escassa participação social em sua implementação, torna difícil avaliar seus reais impactos sobre a segurança pública e os direitos fundamentais.

As principais promessas atribuídas ao policiamento preditivo envolvem o aumento da eficiência policial, a redução da criminalidade e a melhor gestão de recursos públicos. No entanto, essas promessas são acompanhadas de uma série de críticas. A primeira diz respeito à opacidade dos algoritmos utilizados: muitos

dos modelos são proprietários e não permitem auditoria externa, o que dificulta o controle social e a responsabilização por eventuais abusos (O'Neil, 2017). Em segundo lugar, estudos empíricos demonstram que a utilização de dados históricos pode reproduzir práticas de policiamento discriminatórias, uma vez que os dados refletem decisões passadas de agentes estatais que, muitas vezes, foram marcadas por viés racial, territorial ou de classe (Eubanks, 2018; Richardson et al., 2019). Além disso, a eficácia do policiamento preditivo tem sido colocada em dúvida por diversas pesquisas acadêmicas. Em Santa Cruz (EUA), por exemplo, a própria polícia decidiu encerrar o uso do PredPol após constatar que os efeitos na redução da criminalidade eram estatisticamente insignificantes e que a ferramenta concentrava ações policiais em bairros já sobrepoliciados (Nakashima, 2024). Esses dados reforçam a necessidade de um debate crítico e contextualizado sobre a adoção dessa tecnologia no Brasil, especialmente em regiões como a Amazônia urbana, onde a desigualdade estrutural, a violência institucional e a ausência de políticas públicas tornam os riscos ainda mais evidentes.

Portanto, embora o policiamento preditivo se apresente como inovação técnica voltada à modernização do aparato policial, é fundamental questionar os pressupostos de neutralidade e eficácia que sustentam sua disseminação. O contexto brasileiro, e particularmente o amazônico, exige uma abordagem cautelosa, informada por critérios éticos, técnicos e sociais, que reconheça as limitações das tecnologias algorítmicas e priorize a proteção dos direitos fundamentais.

A Lógica Algorítmica e a "Injustiça Algorítmica"

A lógica algorítmica, base dos sistemas de policiamento preditivo, fundamenta-se na coleta, organização e análise massiva de dados históricos para a formulação de previsões sobre o comportamento futuro, incluindo a ocorrência de crimes. À primeira vista, essa abordagem se apresenta como uma alternativa racional e tecnicamente neutra para a tomada de decisões no campo da segurança pública. Contudo, essa pretensa neutralidade é ilusória. Como argumenta Cathy O'Neil (2017), os algoritmos são, na prática, "opiniões incorporadas em código" – isto é, carregam os valores, preconceitos e escolhas políticas de seus programadores e das instituições que os operam.

O conceito de "injustiça algorítmica" cunhado por O'Neil em sua obra "Weapons of Math Destruction" (2017) refere-se ao uso de modelos matemáticos opacos, impenetráveis e desprovidos de mecanismos eficazes de prestação de contas, que causam danos sistemáticos a grupos historicamente marginalizados. Esses modelos são caracterizados por três atributos principais: opacidade (os critérios e parâmetros usados não são acessíveis ou compreensíveis para os afetados), escala (são aplicados

em larga escala e com grande impacto) e dano (produzem consequências adversas significativas, muitas vezes irreversíveis, na vida dos indivíduos e comunidades atingidas). Na segurança pública, esse risco se manifesta na forma de decisões automatizadas que orientam patrulhamentos, abordagens, investigações e uso da força com base em dados históricos que refletem práticas policiais seletivas e discriminatórias. Como apontam Eubanks (2018) e Richardson et al. (2019), os algoritmos de predição criminal, ao se alimentarem de dados produzidos por sistemas policiais e judiciais estruturalmente enviesados, acabam por perpetuar os mesmos padrões de exclusão e estigmatização. Assim, bairros historicamente criminalizados continuam a ser os mais vigiados; grupos raciais frequentemente abordados seguem como alvos prioritários; e indivíduos com histórico de contato com o sistema penal permanecem sob constante suspeita.

Essa lógica circular cria uma retroalimentação perversa: quanto mais uma comunidade é policiada, mais registros de ocorrências ali se acumulam; quanto mais dados, mais razões algorítmicas para intensificar a presença policial. E essa intensificação, por sua vez, gera novos dados, mantendo o ciclo de repressão e estigmatização. Esse fenômeno é conhecido como "feedback algorítmico", e seu impacto é amplamente documentado por estudos empíricos nos Estados Unidos, como o de Lum e Isaac (2016), que analisaram o sistema de policiamento preditivo PredPol e constataram que ele direcionava de forma desproporcional a atuação policial para bairros afro-americanos e latinos, independentemente da real taxa de criminalidade.

No Brasil, embora os estudos empíricos ainda sejam escassos, há indícios preocupantes de que a adoção dessas ferramentas segue lógica semelhante. A ausência de marcos regulatórios, a falta de auditorias independentes e a baixa transparência institucional criam um ambiente propício à opacidade algorítmica e à reprodução de desigualdades estruturais. Como observa Silva (2022), o uso de big data na segurança pública brasileira tende a reforçar os filtros raciais e territoriais já consolidados na prática policial, sobretudo nas periferias urbanas. Além disso, o caráter preditivo desses sistemas desloca o foco da responsabilização individual para a antecipação de riscos coletivos, o que pode levar à adoção de medidas preventivas com base em probabilidades estatísticas, e não em atos concretos. Isso compromete princípios fundamentais do Estado de Direito, como a presunção de inocência e a individualização da responsabilidade penal. Trata-se, portanto, de uma racionalidade que se aproxima perigosamente da lógica do direito penal do inimigo, conforme advertido por Zaffaroni (2001), e que encontra respaldo tecnológico na arquitetura algorítmica contemporânea.

Assim, a noção de injustiça algorítmica é central para compreender os impactos das novas tecnologias na segurança pública. Ela nos alerta para o risco de que, sob o manto da inovação e da eficiência, estejam sendo aprofundadas práticas históricas de exclusão, vigilância seletiva e criminalização das diferenças. Ao invés de corrigirem desigualdades, os algoritmos podem solidificá-las com ainda mais sofisticação, opacidade e legitimidade institucional.

Essa constatação reforça a urgência de políticas públicas orientadas por princípios de justiça algorítmica, que garantam transparência, participação social, mecanismos de auditoria e controle democrático sobre o uso dessas ferramentas. Apenas com tais salvaguardas será possível mitigar os riscos da injustiça algorítmica e promover uma segurança pública compatível com os direitos humanos e a dignidade das populações amazônicas vulnerabilizadas.

Direitos Humanos e o Direito à Cidade

A discussão sobre o uso de tecnologias no campo da segurança pública não pode se dissociar da agenda mais ampla dos direitos humanos, sobretudo quando tais tecnologias são aplicadas em contextos marcados por desigualdade estrutural, como é o caso das periferias urbanas da Amazônia. Nesses territórios, o avanço de práticas como o policiamento preditivo levanta preocupações relativas ao respeito a garantias fundamentais, como o direito à privacidade, à não discriminação e, sobretudo, o direito à cidade — entendido como o acesso pleno aos bens materiais e simbólicos da vida urbana, conforme formulado por Henri Lefebvre (1968) e retomado por De Oliveira e Harvey (2020).

O direito à privacidade é especialmente vulnerável em um cenário de coleta massiva de dados pessoais, georreferenciados e comportamentais por parte do Estado, muitas vezes sem o consentimento informado das populações afetadas. Conforme alerta Solove (2010), a vigilância estatal pode produzir efeitos deletérios sobre a autonomia individual, a liberdade de expressão e a dignidade humana, especialmente quando os indivíduos monitorados pertencem a grupos historicamente marginalizados. Esse risco se intensifica quando os sistemas de vigilância são automatizados e alimentados por algoritmos opacos e não auditáveis, que dificultam a responsabilização institucional em casos de violação. Além disso, o princípio da não discriminação, pilar dos tratados internacionais de direitos humanos como o Pacto Internacional sobre Direitos Civis e Políticos, é frequentemente tensionado por sistemas algorítmicos que replicam padrões históricos de exclusão social (NU, 1966). Como apontam Eubanks (2018) e O'Neil (2017), mesmo quando os algoritmos não contêm variáveis explícitas de raça ou classe, eles podem inferi-las indiretamente por meio de proxies, como endereço, escolaridade ou padrão de consumo, resultando em práticas discriminatórias disfarçadas de neutralidade técnica.

Nesse sentido, o direito à cidade aparece como uma chave conceitual importante para compreender as limitações e os riscos da segurança pública algorítmica. Segundo Rolnik (2017), o direito à cidade implica não apenas o direito de estar e circular nos espaços urbanos, mas o direito de participar das decisões que moldam a vida nas cidades, incluindo as políticas de segurança. No entanto, as populações das periferias amazônicas, muitas vezes alvos preferenciais das tecnologias de vigilância, têm sua agência política reduzida e sua presença tratada como problema de segurança, e não como sujeito de direitos.

Ao superpor lógica algorítmica a territórios já marcados por estigmas e abandono estatal, corre-se o risco de consolidar um modelo de gestão urbana excludente e repressivo, que intensifica a segregação socioespacial e aprofunda a vulnerabilidade das populações racializadas e empobrecidas. A ausência de mecanismos de controle social e de transparência nos processos de coleta, processamento e uso dos dados compromete a legitimidade democrática das ações estatais. Portanto, incorporar os direitos humanos como marco analítico e normativo no debate sobre policiamento preditivo é condição indispensável para evitar que a tecnologia se torne instrumento de aprofundamento das desigualdades urbanas. O desafio é garantir que a inovação tecnológica na segurança pública esteja subordinada à legalidade democrática, aos princípios da dignidade humana e ao compromisso com a justiça social em territórios historicamente vulnerabilizados como a Amazônia urbana.

A AMAZÔNIA URBANA COMO CENÁRIO CRÍTICO

O Contexto Socioespacial Amazônico

A Amazônia urbana constitui um dos cenários mais emblemáticos da desigualdade socioespacial brasileira. Cidades como Manaus, Belém, Macapá, Rio Branco e Porto Velho convivem com uma profunda segmentação territorial marcada por bolsões de pobreza, ausência de infraestrutura básica, exclusão digital e deficiência histórica na prestação de serviços públicos essenciais. A urbanização na região não ocorreu de maneira planejada ou equitativa, mas resultou de processos de ocupação informal e crescimento acelerado, fortemente impactados por fluxos migratórios, dinâmicas econômicas extrativistas e ausência de políticas públicas estruturantes (Mello, 2015; Becker, 2004).

Essas condições fazem da Amazônia urbana um território vulnerável à adoção acrítica de tecnologias de vigilância e policiamento preditivo. A lógica algorítmica aplicada em contextos como esse tende a reproduzir padrões de exclusão, uma vez que os dados alimentadores dos sistemas muitas vezes refletem as práticas seletivas e discriminatórias já presentes nas ações de segurança pública. Como

observa Minayo (2006), a violência institucional e a letalidade policial afetam de forma desproporcional jovens negros e moradores de periferias, realidade que pode ser automatizada e intensificada por modelos preditivos mal calibrados. A carência de dados qualificados sobre o território, a baixa presença estatal em áreas periféricas e o descompasso entre as estratégias tecnológicas e a realidade social contribuem para uma aplicação descontextualizada dessas ferramentas. Além disso, a invisibilidade institucional que permeia essas localidades dificulta o monitoramento e a responsabilização das ações policiais mediadas por tecnologia. Eubanks (2018) destaca que os sistemas automatizados tendem a operar com opacidade e baixa prestação de contas, o que se agrava quando implementados em regiões historicamente negligenciadas pelo Estado.

Na Amazônia urbana, a população frequentemente não tem acesso aos meios para questionar ou revisar decisões automatizadas que afetam suas vidas. Isso inclui desde abordagens policiais até a definição de zonas prioritárias para policiamento ostensivo, que muitas vezes coincidem com territórios racializados e estigmatizados. Conforme aponta De Farias (2025), o policiamento orientado por dados tende a reforçar estereótipos territoriais, institucionalizando o estigma social de determinados bairros como "zonas perigosas".

Nesse sentido, a combinação entre exclusão territorial, ausência de políticas públicas e automação decisória baseada em dados enviesados pode instaurar um ciclo perverso de criminalização automatizada. A população da periferia amazônica, já submetida a processos históricos de marginalização, passa a ser monitorada e controlada por tecnologias que pouco compreendem suas dinâmicas socioculturais e históricas. O risco é de que essas ferramentas deixem de ser instrumentos de planejamento estratégico e se convertam em mecanismos de aprofundamento da repressão seletiva. A governança da segurança pública na Amazônia, portanto, deve considerar essas especificidades territoriais e sociais. A aplicação de tecnologias de policiamento preditivo não pode se desvincular da realidade concreta dos territórios nos quais opera. Como argumenta Rolnik (2017), o direito à cidade implica o reconhecimento da pluralidade de formas de vida urbana e a rejeição de soluções tecnocráticas que invisibilizam as complexidades locais. Esse princípio deve orientar qualquer política pública que pretenda ser compatível com os direitos humanos.

Dessa forma, a análise crítica do contexto socioespacial amazônico é fundamental para compreender os riscos de injustiça algorítmica e vigilância seletiva. A produção de políticas públicas em segurança não pode prescindir de escuta social, controle democrático e transparência algorítmica, sob pena de ampliar o abismo entre inovação tecnológica e justiça social na região.

A Seletividade Penal e a Criminalização das Periferias na Região

A Amazônia urbana constitui um território de contradições: é simultaneamente espaço de invisibilidade institucional e foco prioritário de ações repressivas do Estado. Esse paradoxo se manifesta na forma como as políticas de segurança pública historicamente operam na região, onde a seletividade penal é amplamente documentada por estudos empíricos e relatórios institucionais (IPEA, 2023; FBSP, 2022). O sistema de justiça criminal e as forças de segurança atuam de maneira desproporcional em áreas periféricas, majoritariamente habitadas por populações negras, indígenas, ribeirinhas e empobrecidas. Trata-se de uma seletividade estrutural que antecede qualquer processo de automação, mas que se potencializa quando incorporada aos bancos de dados alimentadores de algoritmos preditivos.

A seletividade penal é o mecanismo pelo qual o Estado, em suas práticas concretas, direciona a repressão penal a determinados grupos sociais, geralmente marcados por sua condição de vulnerabilidade socioeconômica, cor da pele e localização territorial. Essa lógica é visível na concentração de operações policiais em bairros periféricos, na abordagem sistemática de jovens negros e pobres, e na incidência de prisões em flagrante por delitos de menor potencial ofensivo, como porte de drogas para consumo pessoal (Batista, 1990; De Oliveira; De Paulo, 2019).

Na Amazônia, essa seletividade é ainda mais acentuada devido à ausência de políticas públicas universais, à baixa cobertura de direitos sociais e à criminalização histórica das formas de organização popular. Conforme argumenta Minayo (2006), o aparato de segurança atua nesses territórios com uma lógica de contenção e controle, e não de proteção ou mediação de conflitos. Isso significa que o Estado se faz presente sobretudo por meio da coerção, contribuindo para a construção simbólica desses espaços como áreas de risco, perigo e anomia. Esse cenário é fundamental para compreender os riscos do policiamento preditivo. Os sistemas algorítmicos que orientam ações de segurança pública se baseiam em dados históricos, que, por sua vez, refletem as práticas discriminatórias passadas e presentes. Como destacam Lum e Isaac (2016), os algoritmos não criam vieses, mas amplificam aqueles que já estão embutidos nas bases de dados. Assim, ao utilizar registros de ocorrências, boletins de prisão e mapas de calor da criminalidade, os sistemas acabam por retroalimentar a lógica de seletividade territorial e social.

No caso da Amazônia, isso significa que bairros já hipervigiados continuarão a ser priorizados pelas tecnologias preditivas, enquanto regiões com baixa notificação de crimes — muitas vezes por ausência de presença estatal — permanecerão invisibilizadas. A criminalidade, portanto, não é mapeada de forma objetiva, mas a partir da ação institucional previamente direcionada. Isso compromete o princípio da igualdade perante a lei e cria uma distorção no próprio conceito de risco criminal.

Além disso, a criminalização das periferias amazônicas está associada à construção de estigmas territoriais que são absorvidos sem crítica pelos modelos computacionais. Como argumenta Wacquant (2001), a estigmatização de territórios pobres opera como um mecanismo de dominação simbólica, que legitima intervenções repressivas e naturaliza a presença permanente das forças de segurança. Quando esse estigma é codificado em linguagem algorítmica, sua reprodução ganha contornos ainda mais problemáticos, pois se torna opaca, automatizada e difícil de contestar judicialmente. Outro aspecto relevante é o tipo de criminalidade que costuma ser mapeado pelas tecnologias de policiamento preditivo. Em geral, essas ferramentas se concentram em delitos de rua, furtos, roubos, vandalismo e tráfico de pequenas quantidades de drogas — infrações comumente registradas em bairros pobres. Já crimes como corrupção, desmatamento ilegal em larga escala, crimes ambientais cometidos por grandes empresas, e tráfico internacional de armas ou drogas, não costumam estar presentes nas bases de dados que alimentam os algoritmos (Vieira; Santos, 2025).

Essa seleção já define uma agenda punitiva enviesada, voltada à repressão de comportamentos marginalizados e não ao enfrentamento de estruturas organizadas de violência. A aplicação do policiamento preditivo, nesses moldes, contribui para a consolidação de um modelo de justiça penal seletiva, voltado para o controle de populações consideradas "suspeitas" por sua posição social e geográfica.

Por fim, deve-se considerar que as comunidades periféricas da Amazônia urbana possuem baixa capacidade institucional de questionamento das decisões automatizadas. Em um cenário de déficit educacional, ausência de transparência institucional e precariedade dos mecanismos de controle externo da atividade policial, as populações afetadas têm dificuldade de acessar informações sobre os critérios utilizados para definição das áreas de risco ou para a realização de abordagens policiais (Eubanks, 2018). A falta de mecanismos de prestação de contas e de governança democrática sobre o uso de tecnologias preditivas compromete gravemente os direitos fundamentais dessas populações. Como propõe Silva (2022), a legitimação de intervenções repressivas com base em dados opacos configura uma forma contemporânea de dominação tecnológica, que se soma às formas tradicionais de controle territorial.

Diante disso, é necessário compreender que a Amazônia urbana não é apenas um espaço de aplicação de tecnologias de segurança, mas um território político onde se disputam narrativas sobre o que é o crime, quem é o criminoso e quem merece proteção. A crítica à seletividade penal, nesse contexto, deve vir acompanhada da exigência de transparência algorítmica, regulação normativa e participação social na construção das ferramentas tecnológicas aplicadas à segurança pública. Sem isso, o risco é que os algoritmos deixem de ser instrumentos de eficiência e se tornem vetores de injustiça automatizada, perpetuando desigualdades históricas sob uma nova roupagem digital.

Policiamento Preditivo em Operação

A implementação de tecnologias de policiamento preditivo na Amazônia urbana vem ocorrendo de maneira fragmentada, porém crescente, inserindo-se em um contexto de experimentação tecnológica guiada por promessas de eficiência e modernização da gestão da segurança pública. Exemplos dessas tecnologias incluem o uso de câmeras inteligentes com reconhecimento facial, softwares de análise preditiva de padrões criminais, e plataformas de georreferenciamento de ocorrências. Embora essas ferramentas ainda não estejam consolidadas como política pública nacional integrada, sua aplicação pontual em estados como Amazonas e Pará revela importantes implicações para os direitos fundamentais das populações afetadas.

Um exemplo notório é a adoção de sistemas de videomonitoramento com algoritmos de reconhecimento facial em cidades como Manaus. Segundo o FBSP (2022), o governo do Estado do Amazonas tem investido em programas de vigilância inteligente, como o sistema "Paredão Digital" — que integra câmeras com capacidade de identificar indivíduos com mandado de prisão em aberto ou inseridos em bancos de dados criminais. (SSP-AM, 2025) Embora haja apelo à eficiência e à agilidade operacional, experiências semelhantes em outros estados brasileiros, como no Rio de Janeiro e na Bahia, demonstraram taxas alarmantes de falsos positivos, sobretudo contra pessoas negras (Instituto Igarapé, 2021). Além disso, a SSP-AM já manifestou interesse em ampliar o uso de softwares de análise preditiva para antecipar zonas de risco e definir prioridades de patrulhamento, com base em mapas de calor e padrões históricos de ocorrência. Essas ferramentas geralmente se baseiam em modelos estatísticos e aprendizado de máquina para indicar regiões com maior probabilidade de incidência de crimes, o que influencia diretamente a alocação de efetivo policial e recursos logísticos. O problema, entretanto, reside no fato de que os dados que alimentam esses sistemas são gerados por práticas de policiamento seletivo e registros criminais historicamente concentrados em bairros periféricos e racializados, como o Coroado, Compensa e Jorge Teixeira, em Manaus (Vieira, 2024).

Essa retroalimentação de dados enviesados reforça a concentração da vigilância sobre determinados territórios, independentemente de suas dinâmicas sociais e contextos históricos. Como destaca Lum e Isaac (2016), algoritmos treinados em bases de dados desiguais reproduzem a geografia da repressão estatal, institucionalizando padrões discriminatórios sob a aparência de neutralidade técnica. Na Amazônia urbana, esse processo agrava o estigma territorial e o tratamento das populações periféricas como potenciais ameaças, mesmo na ausência de condutas delitivas. Outro ponto crítico refere-se à opacidade dos sistemas utilizados. Não há, no Brasil, legislação específica que obrigue os órgãos de segurança a publicarem os critérios e parâmetros utilizados por softwares de policiamento preditivo. Isso significa que a sociedade civil, o sistema de justiça e os próprios cidadãos monitorados desconhecem como as decisões são tomadas — uma violação direta aos princípios de transparência, accountability e devido processo legal. Como argumenta Eubanks (2018), a automação sem transparência transforma os cidadãos em "dados vivos" submetidos a sistemas de controle que escapam à revisão democrática.

Do ponto de vista das comunidades afetadas, os impactos cotidianos do policiamento preditivo são profundos. Jovens moradores de bairros monitorados passam a ser abordados com maior frequência, não por ação concreta, mas pela mera associação territorial ou estatística. Mulheres negras e indígenas relatam maior incidência de revistas, interrupções em seus deslocamentos e vigilância constante em locais públicos. Essa realidade reproduz o que Eley e Rampton (2019) chama de "vigilância ampliada", na qual a presença policial constante opera não apenas como controle físico, mas também como disciplinamento simbólico dos corpos indesejáveis.

Por outro lado, o discurso oficial tende a invisibilizar essas violações, apresentando os sistemas como instrumentos objetivos e racionais. Entretanto, a literatura crítica adverte que o uso de tecnologia no policiamento não elimina o viés humano; ao contrário, pode amplificá-lo por meio de decisões automatizadas que escapam ao controle e à responsabilização institucional (O'Neil, 2017). Na Amazônia, onde a desigualdade é historicamente naturalizada e os territórios periféricos permanecem sub-representados nos espaços de decisão, o risco de injustiça algorítmica é exponencial. A ausência de protocolos públicos de auditoria, governança e participação social agrava esse cenário. Diferentemente da União Europeia, que impõe obrigações normativas claras para sistemas de IA com impacto em direitos fundamentais, o Brasil carece de marcos legais específicos. A lacuna legislativa deixa a critério dos próprios órgãos de segurança a definição sobre a implementação, o uso e a supervisão das tecnologias, o que perpetua práticas autoritárias e desprovidas de controle social.

Nesse contexto, é fundamental propor mecanismos de proteção e governança algorítmica compatíveis com os princípios democráticos. Isso inclui a exigência de avaliação de impacto em direitos humanos antes da adoção de qualquer tecnologia de policiamento preditivo; a publicação dos critérios algorítmicos e indicadores utilizados; a criação de instâncias independentes de fiscalização e a participação efetiva das comunidades afetadas nos processos decisórios. A construção de uma política de segurança orientada pelos direitos humanos não pode prescindir de uma abordagem crítica e contextualizada do uso da tecnologia, especialmente em territórios vulneráveis como os da Amazônia urbana. Portanto, a operação do policiamento preditivo na região não pode ser compreendida apenas como inovação tecnológica, mas como parte de um arranjo político e social mais amplo, que envolve disputa por controle, legitimação do uso da força e gestão seletiva da insegurança. Analisar criticamente esses processos é um passo necessário para romper com o ciclo de criminalização automatizada e construir caminhos institucionais voltados à justiça social e à proteção dos direitos fundamentais.

RISCOS E VULNERABILIZAÇÕES: UMA ANÁLISE CRÍTICA

O Reforço da Seletividade e o Ciclo Vicioso da Criminalização

O policiamento preditivo, ao se apoiar fortemente em dados históricos de ocorrências criminais, registros de abordagens, prisões e patrulhamentos realizados ao longo do tempo, acaba por reproduzir padrões de atuação policial que, historicamente, se concentraram em territórios e populações específicas. No contexto da Amazônia urbana, esse viés é ainda mais acentuado devido à forte desigualdade socioespacial, à carência de políticas públicas e à presença marcante de seletividade penal na atuação das forças de segurança pública (IPEA, 2023; Minayo, 2006).

Na prática, a tecnologia tende a direcionar a atenção policial para os mesmos bairros pobres, periféricos e racializados que já são alvos recorrentes de operações ostensivas. Como os algoritmos de policiamento preditivo operam com base em padrões identificados nos dados históricos, áreas que apresentaram elevados índices de criminalidade no passado são interpretadas como mais propensas à reincidência de delitos, mesmo que essa criminalidade seja, em parte, resultado de um policiamento intensivo e seletivo (Lum; Isaac, 2016). A consequência direta é a retroalimentação de um ciclo vicioso: quanto mais a polícia atua em uma área, mais registros são produzidos e mais aquela área se torna alvo prioritário nos mapas de calor e nos relatórios preditivos. Esse ciclo é particularmente problemático porque desconsidera as causas estruturais da violência, como a exclusão social, a falta de acesso a serviços públicos e a ausência do Estado em diversas dimensões da vida cotidiana. Em vez de promover políticas integradas de segurança e cidadania, a tecnologia acaba reforçando um modelo repressivo de controle social, automatizando preconceitos e estigmas. A obra de Loïc Wacquant (2001) sobre o "Estado penal" e o "encarceramento das margens" é elucidativa ao demonstrar como a seletividade penal opera para conter e controlar populações marginalizadas, transformando o espaço urbano em zonas de exceção.

Essa lógica de vigilância intensificada e segmentada também é criticada por autores como Eubanks (2018), que aponta o risco da "automação da desigualdade". Em sua análise, os sistemas tecnológicos que operam sob a aparência de neutralidade técnica muitas vezes aprofundam as vulnerabilidades das populações mais pobres, pois incorporam e naturalizam desigualdades históricas nos processos de decisão automatizada. O policiamento preditivo, inserido nesse contexto, representa um novo estágio de controle social baseado na tecnologia, sem, contudo, romper com as práticas de estigmatização e repressão seletiva.

Outro fator preocupante é a opacidade dos sistemas algorítmicos. Em geral, as comunidades afetadas não têm acesso aos critérios utilizados para definir áreas de risco ou perfis suspeitos, tampouco dispõem de mecanismos para questionar ou revisar essas classificações. Isso gera um ambiente de insegurança jurídica e de desproteção frente às ações do Estado. Conforme argumenta Cathy O'Neil (2017), os "algoritmos de destruição em massa" operam sem transparência, sem accountability e com forte impacto sobre populações vulneráveis.

Na Amazônia urbana, onde a presença do Estado se dá, frequentemente, apenas sob a forma de repressão policial, a introdução dessas tecnologias tende a agravar o abismo entre as promessas de eficiência e os direitos fundamentais. A criminalização automatizada se expressa não apenas nas abordagens mais frequentes, mas também na intensificação do monitoramento digital, na expansão de bancos de dados de reconhecimento facial, e na aplicação de medidas preventivas que impactam desproporcionalmente determinados grupos raciais e sociais (De Oliveira; De Paulo, 2019). Esse contexto evidencia a necessidade de políticas públicas que enfrentem a seletividade penal não apenas em sua dimensão tradicional, mas também nas novas formas tecnológicas de discriminação. A governança algorítmica deve ser orientada por princípios de justiça social, transparência, auditabilidade e participação cidadã, especialmente em territórios onde o histórico de violações de direitos é persistente. Como destaca Richardson et al. (2019), não se trata apenas de aprimorar os algoritmos, mas de reformular o modelo de policiamento e a lógica de segurança pública para torná-los compatíveis com os direitos humanos e a democracia.

Portanto, o uso de tecnologias preditivas no campo da segurança pública deve ser cuidadosamente avaliado quanto à sua conformidade com os princípios constitucionais, as normas internacionais de direitos humanos e a realidade socioespacial onde serão aplicadas. Na ausência de uma legislação clara e de mecanismos de controle independentes, há o risco de que a inovação tecnológica se transforme em instrumento de aprofundamento das desigualdades e da violência institucional na Amazônia urbana.

A análise crítica do policiamento preditivo deve, portanto, considerar não apenas os aspectos técnicos, mas, sobretudo, os seus impactos sociais, jurídicos e políticos. O combate à criminalidade não pode ser feito à custa da liberdade, da dignidade e da cidadania das populações historicamente vulnerabilizadas. Sem um marco normativo robusto e uma escuta ativa das comunidades afetadas, a tecnologia será apenas mais uma camada de opressão em contextos já marcados pela exclusão e pela seletividade estatal.

Violação da Privacidade e do Devido Processo Legal

A emergência das tecnologias preditivas no campo da segurança pública, notadamente aquelas baseadas em IA, algoritmos de aprendizado de máquina e mineração massiva de dados, tem gerado preocupações crescentes acerca das violações do direito à privacidade e do devido processo legal. Tais dispositivos operam sob uma lógica de vigilância contínua, muitas vezes opaca, que transcende os limites do espaço público e adentra esferas cada vez mais íntimas da vida social dos cidadãos. Essa expansão da vigilância automatizada é especialmente problemática em contextos de vulnerabilidade estrutural, como as periferias urbanas da Amazônia, onde a ausência de garantias institucionais fortalece a assimetria entre o aparato estatal e a cidadania.

No que se refere à privacidade, as práticas de policiamento preditivo frequentemente envolvem a coleta e o processamento de dados pessoais sem o consentimento dos indivíduos afetados. Informações como localização, histórico criminal de terceiros, padrões de deslocamento e até mesmo interações em redes sociais podem ser analisadas por sistemas de IA sem que haja transparência sobre o uso desses dados. Segundo Solove (2010), essa lógica de "agregação de dados" mina a autonomia informacional dos cidadãos e ameaça um dos pilares do Estado Democrático de Direito. No Brasil, a ausência de uma regulação robusta específica para o uso de tecnologias de segurança pública agrava esse cenário, ainda que a Lei Geral de Proteção de Dados (LGPD) estabeleça princípios como a finalidade, necessidade, transparência e segurança (BRASIL, 2018). Contudo, como observam Mendes e Doneda (2018), a LGPD possui lacunas significativas no tocante à atuação do Estado em contextos de segurança e investigação criminal, o que possibilita interpretações permissivas por parte dos órgãos públicos. Em países da União Europeia, por exemplo, o GDPR impõe limites mais claros às ações estatais e exige avaliações de impacto algorítmico que considerem a proporcionalidade e a legalidade da coleta e uso de dados, conforme disposto no artigo 35 do referido regulamento. No Brasil, tais exigências ainda não se consolidaram como prática institucional.

No que tange ao devido processo legal, o uso de algoritmos em processos decisórios de segurança pública apresenta riscos sérios à legalidade, à ampla defesa e ao contraditório. A lógica algorítmica, por definição, opera com base em modelos estatísticos complexos, muitas vezes incompreensíveis mesmo para os técnicos que os desenvolvem — fenômeno conhecido como "caixa-preta algorítmica" (Pasquale, 2015). Isso significa que as decisões tomadas com base em sistemas preditivos — como intensificação de patrulhamento em determinados bairros, classificação de indivíduos como "potencialmente perigosos" ou definição de rotas estratégicas — ocorrem sem que os cidadãos tenham ciência, acesso ou mecanismos de contestação. A ausência de mecanismos claros de accountability algorítmica compromete, portanto,

a transparência e a legitimidade do aparato estatal, sobretudo quando tais decisões impactam diretamente o exercício de direitos fundamentais. Conforme sustentam Zuboff (2023) e Eubanks (2018), a substituição de juízos humanos por inferências computacionais tende a obscurecer os critérios de imputação de responsabilidade e a consolidar um modelo tecnocrático de poder, com efeitos potencialmente autoritários.

Além disso, o uso de dados enviesados ou incompletos pode gerar classificações incorretas e injustas, reforçando estigmas sociais e raciais já presentes nas estruturas de poder. Como demonstram estudos empíricos conduzidos por Lum e Isaac (2016), a utilização de registros policiais históricos como base de treinamento de algoritmos tende a reproduzir padrões seletivos de criminalização, especialmente contra populações negras e periféricas. Tais práticas não apenas violam a igualdade perante a lei, como corroem os fundamentos do processo penal democrático, ao antecipar a culpa e orientar decisões com base em perfis estatísticos, e não em evidências concretas.

Na Amazônia urbana, essas dinâmicas assumem contornos ainda mais críticos. A precariedade institucional, a sobreposição de vulnerabilidades socioambientais e a baixa densidade de representação política tornam as populações locais particularmente expostas aos abusos das tecnologias de vigilância. A falta de informação, de acesso a mecanismos de justiça e de espaços institucionais de deliberação agrava a assimetria entre Estado e cidadão, possibilitando a consolidação de um sistema de policiamento baseado em suspeição algorítmica e vigilância permanente.

Diante desse cenário, é imprescindível a construção de marcos regulatórios que assegurem não apenas a proteção de dados pessoais, mas também a transparência das decisões algorítmicas e o controle democrático sobre seu uso. Medidas como a obrigatoriedade de auditorias externas, a disponibilização de relatórios de impacto de direitos humanos, e a criação de conselhos de fiscalização civil são instrumentos essenciais para garantir que o uso de tecnologias na segurança pública esteja alinhado aos princípios constitucionais e aos tratados internacionais de direitos humanos ratificados pelo Brasil. Portanto, a vigilância algorítmica e o policiamento preditivo, quando operados sem garantias mínimas de legalidade, transparência e participação social, representam ameaças significativas ao direito à privacidade e ao devido processo legal. Esses riscos se intensificam em contextos como a Amazônia urbana, onde a lógica da seletividade penal e da invisibilidade institucional já opera com grande intensidade. Cabe, assim, à academia, aos operadores do direito e à sociedade civil organizada desenvolverem mecanismos efetivos de resistência, controle e transformação dessa realidade.

Experiências Internacionais e Lições Aprendidas

A análise de experiências internacionais que envolveram o uso de tecnologias preditivas e sistemas automatizados de vigilância pode oferecer subsídios fundamentais para compreender os riscos e as vulnerabilidades que essas ferramentas impõem aos direitos fundamentais. Dentre os casos mais emblemáticos, destaca-se o SyRI, implementado nos Países Baixos, e os marcos regulatórios estabelecidos pelo GDPR da União Europeia. Ambos os exemplos ilustram, por caminhos distintos, a importância da regulação estatal e da proteção de dados na construção de uma governança algorítmica compatível com os valores democráticos.

O caso SyRI consistia em um sistema desenvolvido pelo governo holandês que combinava dados de diferentes fontes — como registros fiscais, dados de habitação e assistência social — para identificar indivíduos com alto risco de cometer fraudes em programas públicos (Van Oirsouw, 2024). Embora a proposta oficial fosse aumentar a eficiência do Estado no combate a fraudes, o sistema operava de forma sigilosa, com lógica algorítmica opaca e sem a possibilidade de contestação pelas pessoas afetadas. Em 2020, a Corte Distrital de Haia declarou a inconstitucionalidade do SyRI, afirmando que sua operação violava o direito à privacidade previsto no artigo 8 da Convenção Europeia de Direitos Humanos (CEDH). Segundo a sentença, o uso indiscriminado e desproporcional de dados, especialmente em bairros de baixa renda, perpetuava a estigmatização e a vigilância seletiva de grupos vulneráveis (Van Oirsouw, 2024).

A decisão da Justiça holandesa se tornou um marco para o debate global sobre os limites éticos e jurídicos da IA aplicada à administração pública. O caso SyRI evidenciou que, mesmo em democracias consolidadas, a ausência de transparência, accountability e participação cidadã no desenvolvimento de sistemas automatizados pode resultar em violações estruturais de direitos humanos. Mais do que um problema técnico, a aplicação de algoritmos na esfera pública exige uma abordagem política, centrada na proteção das liberdades fundamentais. Nesse sentido, o GDPR, em vigor desde 2018 na União Europeia, representa uma tentativa robusta de estabelecer padrões jurídicos para o tratamento ético de dados pessoais. O GDPR reconhece, em seu artigo 22, o direito dos indivíduos de não serem submetidos a decisões baseadas exclusivamente em processamento automatizado, incluindo a definição de perfis, que produzam efeitos legais ou significativamente similares. Além disso, prevê o direito à explicação sobre os critérios adotados pelos algoritmos, consagrando o princípio da transparência algorítmica (UE, 2016).

A experiência europeia com o GDPR tem sido apontada como modelo internacional de proteção de dados, ainda que enfrente desafios na sua implementação prática. Como ressalta Zuboff (2023), o avanço das tecnologias digitais demanda não apenas

a criação de marcos normativos, mas também mecanismos eficazes de fiscalização e controle social. O simples reconhecimento formal de direitos não garante sua efetividade em contextos de assimetria informacional entre o Estado, as corporações e os cidadãos.

Em contraste com esses avanços internacionais, o Brasil carece de um arcabouço jurídico que regule especificamente o uso de tecnologias preditivas na segurança pública. A LGPD, embora represente um avanço, ainda possui lacunas significativas no que tange à responsabilização do Estado e à transparência na aplicação de algoritmos por órgãos públicos. Como observa Mendes e Doneda (2018), a LGPD não proíbe decisões automatizadas, tampouco impõe obrigações claras de explicabilidade nos casos em que tais decisões afetam diretamente a vida dos cidadãos. A ausência de normas específicas tem permitido a expansão de projetos de vigilância tecnológica no Brasil, especialmente em regiões marcadas por vulnerabilidade social, como a Amazônia urbana. Iniciativas que envolvem câmeras inteligentes, softwares de reconhecimento facial e plataformas de análise preditiva são frequentemente implementadas sem debate público, avaliação de impacto ou consentimento das comunidades afetadas (Souza, 2022). Tal cenário aprofunda o risco de que o país repita os mesmos erros do caso SyRI, aplicando tecnologias de alta complexidade sobre populações já estigmatizadas e historicamente invisibilizadas.

Portanto, as lições aprendidas a partir de experiências como a dos Países Baixos e da União Europeia apontam para a necessidade urgente de um marco regulatório brasileiro robusto, que considere os princípios da legalidade, transparência, proporcionalidade e não discriminação. A implementação de um sistema nacional de avaliação de impacto algorítmico, inspirado nas diretrizes do GDPR, pode representar um avanço significativo na prevenção de abusos e na garantia de direitos fundamentais. Além disso, é imprescindível incorporar à legislação brasileira dispositivos que assegurem o direito à explicação, à revisão humana das decisões automatizadas e à reparação em casos de danos decorrentes da ação de sistemas preditivos. Como enfatiza Souza (2022), a responsabilização algorítmica não deve se limitar à regulação técnica, mas abranger as dimensões éticas, sociais e políticas da governança de dados.

Em suma, o panorama internacional evidencia que a adoção de tecnologias de vigilância e predição deve ser acompanhada de rigorosos mecanismos de controle democrático, sob pena de legitimação de práticas de injustiça algorítmica e violação de direitos fundamentais. A Amazônia urbana, com suas especificidades territoriais e sociais, demanda atenção redobrada nesse processo, de modo a evitar que a inovação tecnológica se converta em mais um vetor de exclusão e opressão institucionalizada.

DIRETRIZES PARA UMA GOVERNANÇA ALGORÍTMICA DEMOCRÁTICA

A Urgência de um Marco Regulatório Nacional

A crescente incorporação de tecnologias algorítmicas na segurança pública brasileira, especialmente aquelas voltadas ao policiamento preditivo, impõe a necessidade urgente de um marco regulatório nacional que estabeleça diretrizes claras sobre os limites éticos, legais e operacionais para o uso dessas ferramentas. No atual cenário normativo, o Brasil ainda carece de uma legislação específica que discipline o uso de algoritmos por agentes estatais, o que abre espaço para abusos, violações de direitos e práticas discriminatórias institucionalizadas por meio da tecnologia (Mendes; Doneda, 2018).

O debate sobre a regulação da IA tem avançado no Congresso Nacional, mas ainda de forma genérica, sem abordar com profundidade os riscos específicos da aplicação em políticas de segurança pública. O Projeto de Lei n.º 2.338/2023, que trata da IA, embora represente um avanço, ainda não estabelece salvaguardas robustas no que tange ao uso estatal de sistemas preditivos voltados à vigilância e policiamento (BRASIL, 2023). Isso é especialmente preocupante em um contexto como o da Amazônia urbana, onde a desigualdade estrutural e a seletividade penal podem ser amplificadas por algoritmos não regulados.

Para além da ausência normativa, é igualmente grave a inexistência de instâncias institucionais de controle social e transparência algorítmica. No modelo brasileiro, os dados utilizados pelas forças policiais frequentemente não são disponibilizados ao público, o que impede a auditoria independente e o debate público qualificado sobre suas implicações. Diferentemente do modelo europeu, onde o GDPR prevê o direito à explicação, à revisão humana de decisões automatizadas e ao consentimento no uso de dados sensíveis (UE, 2016), o Brasil não dispõe de mecanismos equivalentes na LGPD que sejam suficientemente aplicados ou fiscalizados no setor público (Mendes; Doneda, 2018).

Nesse sentido, a construção de um marco regulatório nacional deve observar ao menos três pilares fundamentais: transparência, accountability e participação social. A transparência exige que os modelos algorítmicos utilizados pelas forças de segurança sejam auditáveis, com divulgação dos critérios de funcionamento, das fontes de dados utilizadas e das lógicas decisórias incorporadas aos sistemas. A accountability demanda a criação de mecanismos institucionais que responsabilizem gestores públicos e empresas contratadas por eventuais violações de direitos decorrentes do uso de tecnologias. Já a participação social pressupõe a inclusão de organizações da sociedade civil, especialistas e comunidades vulnerabilizadas

nos processos de formulação, monitoramento e avaliação de políticas públicas baseadas em IA (Richardson et al., 2019). Ademais, é necessário que a legislação preveja a realização de avaliações de impacto algorítmico (Algorithmic Impact Assessment – AIA) antes da implementação de qualquer sistema automatizado que afete direitos fundamentais. Esse tipo de análise preventiva já é exigido em algumas jurisdições, como no Canadá e nos Estados Unidos, e permite identificar, desde o início, potenciais riscos de discriminação, violação de privacidade e reforço de desigualdades (Richardson et al., 2019).

Outro ponto essencial a ser incorporado no marco legal diz respeito ao direito à explicação, ou seja, a obrigatoriedade de que decisões tomadas por algoritmos — especialmente aquelas com efeitos sobre liberdades individuais — sejam compreensíveis, revisáveis e passíveis de contestação. Isso evita o chamado "efeito caixa-preta" das decisões automatizadas, em que a pessoa afetada sequer tem conhecimento dos critérios utilizados para sua inclusão em um determinado banco de dados de risco ou zona prioritária de policiamento (O'Neil, 2017; Eubanks, 2018).

Por fim, o processo de elaboração de uma legislação nacional deve incorporar a perspectiva territorial, reconhecendo que os impactos dos algoritmos não são homogêneos em todo o território nacional. Como discutido ao longo deste capítulo, a Amazônia urbana apresenta especificidades socioespaciais que potencializam os riscos da tecnologia: ausência do Estado, estigmatização racial e precariedade de políticas públicas. Por isso, é imprescindível que qualquer marco regulatório considere os contextos locais e seja sensível às vulnerabilidades históricas que afetam determinadas regiões e populações. Em síntese, a urgência de um marco regulatório nacional para o uso de tecnologias algorítmicas na segurança pública decorre não apenas da inovação tecnológica em si, mas dos riscos reais de que essa inovação agrave desigualdades, legitime abusos e produza novas formas de controle social seletivo. Regular, portanto, não significa impedir a inovação, mas orientá-la por princípios democráticos, garantindo que os avanços tecnológicos não se convertam em instrumentos de opressão institucionalizada.

Transparência, Auditoria e Controle Social

A governança algorítmica em uma sociedade democrática não pode prescindir da transparência, da possibilidade de auditoria e do controle social sobre os sistemas utilizados, especialmente quando aplicados em políticas públicas sensíveis, como a segurança pública. O caráter opaco dos algoritmos — muitas vezes operando como "caixas-pretas" (Pasquale, 2015) — compromete princípios básicos do Estado de Direito, como a legalidade, a publicidade e a responsabilização por atos da administração pública. A ausência de mecanismos de explicabilidade e de

participação pública transforma decisões automatizadas em instrumentos de poder não controlado, o que representa uma ameaça direta aos direitos fundamentais, à justiça e à equidade.

Cathy O'Neil (2017) adverte que os algoritmos utilizados em sistemas públicos frequentemente operam de forma obscura, sem possibilidade de auditoria por parte dos afetados ou de seus representantes. Essa situação agrava-se em contextos de vulnerabilidade institucional, como ocorre na Amazônia urbana, onde a assimetria informacional entre o Estado e a população é ainda mais acentuada. A lógica algorítmica, se não for passível de escrutínio público, reforça uma cultura de opacidade decisória, na qual os cidadãos são alvos de decisões baseadas em critérios que não compreendem e sobre os quais não têm qualquer influência. A transparência algorítmica exige a adoção de políticas que garantam o acesso às informações sobre como os algoritmos são construídos, quais dados são utilizados, quais as regras de decisão aplicadas e quais os critérios de risco envolvidos. Esse princípio deve ser incorporado tanto nas fases de desenvolvimento quanto nas etapas de implementação e monitoramento das tecnologias. A abertura dos códigos-fonte, ou ao menos sua disponibilização para auditorias independentes, é um passo fundamental nessa direção. Além disso, os relatórios de impacto algorítmico, inspirados no modelo europeu de avaliação de impacto em proteção de dados (UE, 2016), devem se tornar obrigatórios em qualquer programa de policiamento preditivo.

A auditoria algorítmica, por sua vez, deve ser entendida como uma prática permanente e multidimensional. Ela precisa englobar não apenas aspectos técnicos, como a verificação de acurácia e consistência estatística dos modelos, mas também uma análise crítica de seus impactos sociais, éticos e jurídicos. Conforme propõem Selbst e Barocas (2018), a auditoria não pode ser reduzida à revisão técnica interna feita pelas próprias instituições que implementam os sistemas, sob risco de neutralizar sua função fiscalizadora. A participação de entidades independentes, universidades, organizações da sociedade civil e defensorias públicas é essencial para conferir legitimidade e efetividade a esse processo. O controle social, nesse contexto, deve ser concebido como um direito coletivo e um instrumento democrático de fiscalização das políticas públicas. Inspirado nos mecanismos já previstos em conselhos de segurança, ouvidorias e conferências públicas, o controle dos algoritmos precisa ser institucionalizado e ter poder deliberativo. As populações impactadas devem ter direito à informação prévia, ao consentimento informado (quando cabível) e à contestação de decisões automatizadas. A inexistência desses mecanismos compromete o devido processo legal e contribui para a desumanização da segurança pública.

No caso brasileiro, a Constituição Federal de 1988 prevê, em seu artigo 5º, inciso XXXIII, o direito de acesso às informações públicas, além de estabelecer, no artigo 37, os princípios da administração pública, como legalidade, impessoalidade, moralidade, publicidade e eficiência (BRASIL, 1988). Esses dispositivos devem orientar a formulação de políticas de transparência algorítmica. A Lei de Acesso à Informação, Lei nº 12.527/2011, também oferece fundamentos normativos importantes para obrigar o poder público a divulgar informações sobre os sistemas automatizados utilizados na segurança (BRASIL, 2011).

Por outro lado, a experiência internacional demonstra que iniciativas robustas de transparência e controle são viáveis e necessárias. O caso do SyRI na Holanda mostrou os perigos do uso opaco de algoritmos para classificar famílias em risco de fraude. A falta de transparência e de base científica nos critérios utilizados levou à declaração de inconstitucionalidade do programa pelo Tribunal Distrital de Haia em 2020, com base no princípio da não discriminação (Mantelero, 2016). Já o GDPR da União Europeia obriga os controladores de dados a explicarem as decisões automatizadas e prevê o direito à revisão humana dessas decisões (UE, 2016).

No Brasil, ainda que de maneira incipiente, iniciativas como os relatórios do FBSP e projetos acadêmicos sobre accountability algorítmica têm contribuído para o amadurecimento do debate. No entanto, permanece a lacuna de políticas públicas que institucionalizem práticas permanentes de transparência e participação social na gestão das tecnologias policiais. Na ausência desses mecanismos, o risco é que a inovação tecnológica avance sem o devido lastro democrático, convertendo algoritmos em instrumentos de reprodução das desigualdades que deveriam combater.

Portanto, é urgente incorporar à governança algorítmica no campo da segurança pública um conjunto de princípios baseados na transparência, na auditabilidade e no controle social. Esses pilares devem orientar tanto a formulação quanto a execução das políticas que envolvem IA e big data, especialmente em contextos de alta vulnerabilidade, como as periferias da Amazônia urbana. Somente assim será possível construir uma segurança pública tecnicamente eficiente, juridicamente legítima e eticamente compatível com os princípios democráticos e os direitos humanos.

Alternativas e Salvaguardas

Diante dos riscos substanciais impostos pelo policiamento preditivo à luz da ausência de regulação, transparência e controle democrático, torna-se imperativo propor alternativas viáveis e salvaguardas robustas que assegurem o respeito aos direitos humanos no uso de tecnologias de segurança pública. A construção de um modelo de segurança que seja verdadeiramente democrático e inclusivo exige

mais do que o aperfeiçoamento de sistemas algorítmicos: requer a priorização de abordagens que considerem o contexto socioespacial, promovam justiça social e fortaleçam o pacto civilizatório baseado nos direitos fundamentais. Uma das principais alternativas ao modelo puramente preditivo de segurança é o investimento em políticas de segurança pública comunitária. Essa abordagem parte do princípio de que a segurança não pode ser pensada apenas como repressão ou controle territorial, mas sim como resultado de relações de confiança, participação cidadã e fortalecimento dos laços sociais. Iniciativas como policiamento comunitário, mediação de conflitos e fóruns permanentes de diálogo entre forças de segurança e moradores das periferias têm mostrado eficácia na redução de crimes e na construção de um ambiente mais seguro e justo (Minayo, 2006)

Além disso, políticas sociais voltadas à redução das desigualdades estruturais devem ser entendidas como centrais no debate sobre segurança pública. A literatura crítica em criminologia, como os estudos de Wacquant (2001), mostra que o encarceramento em massa e a intensificação da vigilância são respostas ineficazes às causas profundas da violência, que estão enraizadas em exclusões históricas. Assim, o fortalecimento de políticas públicas em áreas como saúde, educação, cultura e habitação deve ser incorporado como estratégia complementar – e muitas vezes mais eficaz – que a repressão baseada em tecnologia.

Do ponto de vista tecnológico, é essencial que qualquer sistema algorítmico empregado em segurança pública seja projetado com salvaguardas jurídicas e éticas. Isso inclui a obrigação de realizar avaliações de impacto em direitos humanos antes da implementação de qualquer sistema de IA, conforme já recomendado por organismos internacionais como a ONU e a OCDE (UNESCO, 2021; OECD, 2019). Tais avaliações devem considerar, sobretudo, o potencial de discriminação, invasão de privacidade, opacidade decisória e efeitos desproporcionais sobre grupos vulneráveis. Outra salvaguarda crucial é a exigência de mecanismos de explicabilidade e interpretabilidade dos algoritmos, conhecidos como "algoritmos explicáveis" (Fernandes et al., 2022). A possibilidade de compreender como uma decisão algorítmica foi tomada é fundamental não apenas para garantir o devido processo legal, mas também para permitir auditorias técnicas e controle social. Isso exige que as tecnologias adotadas não sejam caixas-pretas inacessíveis, mas que possam ser inspecionadas, questionadas e corrigidas quando necessário (Pasquale, 2015).

A transparência deve ser acompanhada de mecanismos efetivos de responsabilização. Para isso, propõe-se a criação de conselhos de governança algorítmica com participação paritária entre Estado, academia e sociedade civil, incluindo representantes das comunidades impactadas. Esses conselhos teriam como função monitorar o desenvolvimento, a aquisição e o uso de tecnologias na segurança

pública, emitindo pareceres vinculantes sobre sua legalidade, proporcionalidade e adequação. Essa proposta já foi testada em experiências internacionais como o "Office of Algorithmic Accountability" em Nova York e poderia ser adaptada à realidade brasileira com enfoque interseccional e territorial.

No campo jurídico, é imprescindível que o ordenamento brasileiro avance na formulação de um marco legal específico para o uso de tecnologias de vigilância e policiamento preditivo. Essa legislação deve conter princípios como legalidade, finalidade, proporcionalidade, não discriminação, minimização de dados e proteção ao devido processo legal, em consonância com as diretrizes do GDPR europeu e os princípios de justiça algorítmica já consolidados em tratados internacionais de direitos humanos.

Por fim, deve-se considerar a importância da educação digital e da literacia algorítmica. A capacitação de operadores do direito, gestores públicos, policiais, defensores de direitos humanos e cidadãos para compreender os impactos das tecnologias de IA é fundamental para criar uma cultura de governança democrática. A opacidade técnica não pode ser usada como justificativa para afastar o controle social e institucional sobre decisões que afetam vidas humanas. Em síntese, o enfrentamento das vulnerabilizações decorrentes do policiamento preditivo na Amazônia urbana passa por um conjunto integrado de ações: investimento em políticas comunitárias e sociais, formulação de marcos regulatórios robustos, adoção de salvaguardas tecnológicas e jurídicas, fortalecimento do controle social e promoção de uma cultura de direitos no uso de tecnologias. O desafio é construir um modelo de segurança que reconheça a centralidade da dignidade humana e que, mesmo diante da inovação tecnológica, não perca de vista a justiça social e o respeito às diversidades territoriais, raciais e econômicas que marcam o Brasil e, em especial, a Amazônia.

RESULTADOS E DISCUSSÕES

A análise crítica desenvolvida ao longo deste capítulo permitiu a identificação de um conjunto de riscos, dilemas e contradições associados à implementação do policiamento preditivo na Amazônia urbana, especialmente no que se refere à violação de direitos fundamentais e à reprodução de desigualdades históricas. Os principais resultados se estruturam em torno de três eixos: (i) a intensificação da seletividade penal a partir de dados enviesados, (ii) a fragilidade jurídica diante da ausência de regulação nacional, e (iii) a urgência de salvaguardas institucionais e sociais voltadas à governança algorítmica democrática.

O primeiro eixo de discussão revela que os sistemas de policiamento preditivo, ao se basearem em dados históricos de ocorrências criminais — muitas vezes coletados sob práticas discriminatórias —, tendem a retroalimentar a criminalização de determinados territórios e grupos sociais. Conforme demonstrado por Lum e Isaac (2016), os algoritmos, embora revestidos de uma aparência de neutralidade técnica, reproduzem os vieses presentes nos registros policiais, concentrando a vigilância em bairros periféricos e de maioria negra, indígena e empobrecida. No contexto da Amazônia urbana, tal fenômeno se manifesta de forma ainda mais preocupante, dada a histórica invisibilidade institucional dessas populações (Minayo, 2006; IPEA, 2023).

O segundo eixo destaca a insuficiência de marcos normativos que regulem o uso de IA e análise preditiva no campo da segurança pública. A ausência de uma legislação nacional específica, somada à opacidade dos sistemas utilizados, compromete o direito ao devido processo legal, à privacidade e à transparência na ação estatal. Como evidenciado no caso SyRI, na Holanda, a falta de critérios claros e auditáveis para o funcionamento de sistemas preditivos pode levar a decisões estigmatizantes e inconstitucionais (Fernandes et al., 2022). No Brasil, documentos como o Relatório Anual do FBSP (2023) já alertam para a crescente utilização de tecnologias de vigilância sem o devido controle social, especialmente em estados como São Paulo, Bahia e Amazonas.

O terceiro eixo aponta para a necessidade de construção de salvaguardas que garantam a compatibilidade entre inovação tecnológica e o respeito aos direitos humanos. Tais salvaguardas incluem: a exigência de avaliações de impacto em direitos fundamentais antes da implementação de novos sistemas; a criação de órgãos de auditoria independentes para fiscalizar algoritmos usados pelo Estado; a transparência sobre os critérios técnicos e estatísticos adotados; e a inclusão de mecanismos de participação popular nas decisões sobre o uso dessas tecnologias. Esses elementos são consistentes com os princípios do GDPR e com os debates emergentes sobre "justiça algorítmica" (O'Neil, 2017; Eubanks, 2018; Richardson et al., 2019). Outro ponto discutido ao longo do capítulo refere-se à tensão entre eficiência operacional e garantias democráticas. Embora o policiamento preditivo seja frequentemente apresentado como uma solução para a escassez de recursos e o aumento da criminalidade, os dados analisados demonstram que sua eficácia não é garantida e, quando mal regulado, pode intensificar o ciclo de repressão sobre populações já marginalizadas. A experiência de cidades norte-americanas como Los Angeles e Chicago, onde programas como o PredPol foram descontinuados após denúncias de discriminação racial, reforça a importância de uma abordagem cautelosa e baseada em evidências (Nakashima, 2024).

No caso brasileiro, as poucas iniciativas implementadas seguem uma lógica de segurança pública centrada na repressão, com escassa articulação com políticas sociais e ausência de mecanismos de escuta das comunidades impactadas. Essa lacuna evidencia a necessidade de um modelo de segurança cidadã, que considere os determinantes sociais da violência e valorize o diálogo com os territórios. A justiça algorítmica, nesse contexto, demanda mais do que ajustes técnicos: requer uma reconfiguração das prioridades do Estado em relação à gestão da segurança, priorizando direitos, inclusão e justiça social.

Por fim, os resultados sugerem que a adoção de tecnologias preditivas na segurança pública da Amazônia deve ser precedida de um amplo debate público e da construção de instrumentos jurídicos que assegurem o controle social e a accountability das instituições. Sem isso, o risco é o aprofundamento da vigilância seletiva, da criminalização automatizada e da exclusão digital, fenômenos que ameaçam não apenas os direitos das populações vulneráveis, mas também a legitimidade do próprio Estado democrático de direito.

CONSIDERAÇÕES FINAIS

O presente estudo analisou criticamente os impactos do policiamento preditivo na Amazônia urbana, destacando como a aplicação de tecnologias baseadas em IA e algoritmos de análise de dados pode não apenas reproduzir, mas também intensificar desigualdades estruturais historicamente presentes nas periferias brasileiras. A partir de uma revisão crítica da literatura nacional e internacional, da análise de experiências comparadas e da consideração das especificidades socioespaciais amazônicas, foi possível construir uma compreensão aprofundada dos riscos éticos, jurídicos e sociais envolvidos no uso de tecnologias preditivas na segurança pública.

Conforme demonstrado ao longo do texto, os sistemas de policiamento algorítmico são construídos a partir de dados históricos que, por sua vez, refletem práticas de policiamento seletivas e marcadas por estigmas sociais. Em contextos como o da Amazônia urbana, onde a ação do Estado frequentemente se dá por meio da repressão e da vigilância, e onde a presença institucional é limitada às forças de segurança, a adoção de ferramentas preditivas tende a consolidar padrões de criminalização automatizada de grupos vulnerabilizados — particularmente populações negras, indígenas, ribeirinhas e periféricas. A chamada "neutralidade tecnológica" revela-se, assim, um mito perigoso, pois mascara os vieses e as estruturas de poder embutidas nos algoritmos e nos bancos de dados. A ausência de um marco regulatório nacional específico sobre o uso de tecnologias algorítmicas pela administração pública agrava o cenário. A inexistência de parâmetros legais claros compromete a transparência, o controle social e a responsabilização das

instituições que fazem uso dessas ferramentas. Casos internacionais como o SyRI, na Holanda — onde um sistema preditivo foi considerado inconstitucional por violar o princípio da não discriminação e o direito à privacidade —, demonstram a urgência de incorporar salvaguardas jurídicas que antecipem riscos e assegurem os direitos fundamentais dos cidadãos. No Brasil, por sua vez, ainda são incipientes os debates sobre accountability algorítmica no campo da segurança pública, o que expõe a população a práticas opacas, com potenciais graves violações ao devido processo legal.

Os dados analisados sugerem que, sem mecanismos de governança democrática, os sistemas de policiamento preditivo correm o risco de ampliar o fosso entre inovação tecnológica e justiça social. Isso se verifica especialmente nas cidades da Amazônia Legal, onde a precariedade de serviços públicos, a baixa inclusão digital e a invisibilidade estatística das populações mais pobres criam um cenário de assimetrias múltiplas, incompatível com a lógica de decisões automatizadas. A governança algorítmica, portanto, não pode ser dissociada da realidade territorial em que se insere. Pelo contrário, deve ser sensível às desigualdades locais e comprometida com o fortalecimento da cidadania e da equidade.

Diante desse panorama, os desafios futuros envolvem tanto a produção de conhecimento científico capaz de iluminar as zonas de opacidade do uso de tecnologias na segurança pública quanto o engajamento político-institucional necessário para a construção de marcos legais protetivos. É preciso que a academia, a sociedade civil e os órgãos de controle avancem em ações coordenadas para promover a transparência dos sistemas preditivos, estabelecer diretrizes técnicas para sua utilização e garantir a participação dos territórios afetados nas decisões sobre sua aplicação. A auditoria de algoritmos, a exigência de avaliações de impacto em direitos humanos e a criação de conselhos de controle social sobre tecnologias de segurança devem fazer parte de uma nova agenda pública para o tema. Além disso, é imperativo investir em alternativas que priorizem a prevenção da violência por meio de políticas sociais, urbanas e educacionais. O uso de tecnologia não pode substituir a presença do Estado em sua dimensão cidadã, tampouco suprimir o papel das políticas públicas estruturantes no enfrentamento das causas da violência. A redução da criminalidade não será alcançada apenas por meio da sofisticação técnica, mas sim pela garantia de direitos e pela superação das desigualdades históricas que estruturam o espaço urbano amazônico.

Em suma, o policiamento preditivo não é neutro nem inevitável. Ele é uma escolha política e técnica que exige regulação, debate público e compromisso com os direitos humanos. A Amazônia urbana, marcada por exclusões múltiplas e por uma profunda assimetria no acesso à justiça e à informação, impõe um chamado à reflexão ética e à prudência regulatória. A inovação tecnológica deve caminhar lado a

lado com a justiça social — e não contra ela. Por isso, este capítulo reforça a urgência de se repensar o modelo de segurança pública à luz de princípios democráticos, que respeitem a dignidade humana e reconheçam a complexidade dos territórios onde se pretende aplicar qualquer ferramenta de vigilância digital.

REFERÊNCIAS

BATISTA, Nilo. **Introdução crítica ao direito penal brasileiro.** Rio de Janeiro: Revan, 1990.

BECKER, Bertha K. **Amazônia: geopolítica na virada do III milênio.** Editora Garamond, 2004.

BRANTINGHAM, Paul; BRANTINGHAM, Patricia. Crime pattern theory. In: Environmental criminology and crime analysis. Willan, p. 100-116, 2013.

BRASIL. **Constituição da República Federativa do Brasil.** Texto constitucional promulgado em 5 de outubro de 1988. Disponível em: <https://www.planalto.gov. br/ccivil_03/ constituicao/constituicao.htm>. Acesso em: 05 jan. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 1, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 5 ago. 2025.

BRASIL. **Projeto de Lei nº 2.338, de 3 de maio de 2023.** Dispõe sobre o desenvolvimento, fomento e uso ético e responsável da inteligência artificial, com base na centralidade da pessoa humana. Autoria: Senador Rodrigo Pacheco (PSD/MG). Senado Federal (Brasília, DF), autuado em 3 mai. 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 5 ago. 2025.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005; e revoga dispositivos do Decreto nº 7.724, de 16 de maio de 2012. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 18 nov. 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 5 ago. 2025.

BRAYNE, Sarah. **Predict and surveil: Data, discretion, and the future of policing.** Oxford University Press, 2021.

DE FARIAS, Bruno Gomes. Tecnologia e vigilância: uso da tecnologia como instrumento de controle social no Brasil. **Revista Políticas Públicas & Cidades,** v. 14, n. 3, p. e1860-e1860, 2025.

DE OLIVEIRA, Victória Maria Américo; DE PAULO, Alexandre Ribas. O cárcere como instrumento de gestão penal da pobreza. **Revista da Faculdade de Direito da UFRGS,** n. 40, 2019.

DE OLIVEIRA, Helbert Michel Pampolha. HARVEY, David. Cidades rebeldes: do direito à cidade à revolução urbana. Tradução Jeferson Camargo. São Paulo: Martins Fontes, 2014. 294 p. **Novos Cadernos NAEA,** v. 23, n. 3, 2020.

EUBANKS, Virginia. **Automating inequality: How high-tech tools profile, police, and punish the poor.** St. Martin's Press, 2018.

ELEY, Louise; RAMPTON, Benjamin. Everyday surveillance, Goffman and unfocused interaction. **Surveillance and Society,** 2019.

FERGUSON, Andrew Guthrie. The rise of big data policing: Surveillance, race, and the future of law enforcement. **In:** The rise of big data policing. New York University Press, 2017.

FERNANDES, Milena Seibert et al. **Inteligência artificial explicável aplicada a aprendizado de máquina: Um estudo para identificar estresse ocupacional em profissionais da saúde.** 2022.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA (FBSP). **Anuário Brasileiro de Segurança Pública 2022.** São Paulo: FBSP, 2022. Disponível em: <https://publicacoes.forumseguranca.org.br/items/4f923d12-3cb2-4a24-9b63-e4178958 1d30>. Acesso em: 03 jan. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA (FBSP). **Anuário Brasileiro de Segurança Pública 2023.** São Paulo: FBSP, 2023. Disponível em: <https://publicacoes.forumseguranca.org.br/items/6b3e3a1b-3bd2-40f7-b280-7419c8eb 3b39>. Acesso em: 03 jan. 2025.

INSTITUTO IGARAPÉ**. Infográfico: Reconhecimento facial no Brasil.** Rio de Janeiro: Instituto Igarapé, 2021. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil Acesso em: 5 ago. 2025.

IPEA – Instituto de Pesquisa Econômica Aplicada. **Atlas da Violência 2023.** Brasília: Ipea, 2023. Disponível em: <https://www.ipea.gov.br/atlasviolencia/arquivos /artigos/9350-223443riatlasdaviolencia2023-final.pdf>. Acesso em: 30 jan. 2025.

HENRI, Lefebvre. **Le droit à la ville.** Anthropos, Paris, 1968.

LUCENA, Pedro Arthur Capelari de. **Policiamento preditivo, discriminação algorítmica e racismo: potencialidades e reflexos no Brasil.** VI Simpósio Internacional Lavits, 2019.

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

MACIEL, Iago Penha. **A Vigilância dos Dados e sua Implicação na Liberdade do Indivíduo ou Privacidade.** Editora Dialética, 2025.

MANTELERO, Alessandro. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. **Computer law & security review,** v. 32, n. 2, p. 238-255, 2016.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor,** v. 120, p. 555-587, 2018.

MELLO, Alex Fiúza de. Dilemas e desafios do desenvolvimento sustentável da Amazônia: O caso brasileiro. **Revista Crítica de Ciências Sociais,** n. 107, p. 91-108, 2015.

MINAYO, Maria Cecília de Souza. **Violência e saúde.** Editora Fiocruz, 2006.

NAKASHIMA, Maurício. Desvendando o potencial e os desafios da inteligência artificial na polícia militar do Paraná: estratégias para predição e prevenção de crimes. **Revista Ibero-Americana de Humanidades, Ciências e Educação,** v. 10, n. 1, p. 1321-1336, 2024.

NU. NAÇÕES UNIDAS. **Pacto Internacional sobre Direitos Civis e Políticos,** adotado pela Assembleia Geral da ONU em 16 de dezembro de 1966, entrada em vigor em 23 de março de 1976. Disponível em: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>. Acesso em: 05 fev. 2025.

OECD. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD Principles on Artificial Intelligence.** Paris: OECD, 2019. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Acesso em: 05 ago. 2025.

O'NEIL, Cathy. **Weapons of math destruction: How big data increases inequality and threatens democracy.** Crown, 2017.

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

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

RICHARDSON, Rashida; SCHULTZ, Jason M.; CRAWFORD, Kate. **Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice.** NYUL Rev. Online, v. 94, p. 15, 2019.

ROLNIK, Raquel. **Guerra dos lugares: a colonização da terra e da moradia na era das finanças.** Boitempo Editorial, 2017.

SELBST, Andrew D.; BAROCAS, Solon. The intuitive appeal of explainable machines. **Fordham L. Rev.,** v. 87, p. 1085, 2018.

SILVA, Tarcízio. **Racismo algorítmico: inteligência artificial e discriminação nas redes digitais.** Edições Sesc SP, 2022.

SOLOVE, Daniel J. **Understanding privacy.** Harvard university press, 2010.

SOUZA, Rosandro Barros da Silva. **Governança pública: uma análise sobre o Plano Nacional de Segurança Pública e Defesa Social (2021-2030).** 2022.

SSP-AM. SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA DO AMAZONAS. **Sistema Paredão: Cerco inteligente de videomonitoramento.** Manaus: SSP-AM, 16 jun. 2025. Disponível em: <https://www.ssp.am.gov.br/festival-de-parintins-2025-ssp-am-instala-cerca-de-80-cameras-com-tecnologia-de-reconhecimento -facial-e-de-placas/> Acesso em: 5 ago. 2025.

UE. UNIAO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados (GDPR).** Bruxelas: Parlamento Europeu, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 02 jul. 2025.

UNESCO. ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. **Recomendação sobre a Ética da Inteligência Artificial.** Paris: UNESCO, 2021. Disponível em: <https://unesdoc.unesco.o rg/ark:/48223/pf0000381137>. Acesso em: 05 ago. 2025.

VAN OIRSOUW, Charlotte et al. Constitutional Law in the Digital Era. **In:** European Yearbook of Constitutional Law 2023: Constitutional Law in the Digital Era. The Hague: TMC Asser Press, 2024. p. 1-14.

VIEIRA, Flávia do Amaral. **Crimes ambientais na Amazônia: lições e desafios da linha de frente**. Editoras Maiara Folly: Rio de Janeiro, Plataforma CIPÓ, 2024. Disponível em: <https://plataformacipo.org/wp-content/uploads/2024/04/web-na-linha-de-frente-cipo-3.pdf?utm_source=chatgpt.com>. Acesso em: 02 jul. 2025.

VIEIRA, Andrey Bruno Cavalcante; SANTOS, Hugo Leonardo Rodrigues. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo ea admissibilidade de provas digitais. **Revista Brasileira de Direito Processual Penal,** v. 11, n. 1, p. e1072, 2025.

ZAFFARONI, Eugenio Raúl. **Em busca das penas perdidas: a perda de legitimidade do sistema penal.** Revan, 2001.

ZAVRŠNIK, Aleš. Criminal justice, artificial intelligence systems, and human rights. **In:** ERA forum. Berlin/Heidelberg: Springer Berlin Heidelberg, 2020. p. 567-583.

ZUBOFF, Shoshana. The age of surveillance capitalism. In: Social theory re-wired. **Routledge,** p. 203-213, 2023.

WACQUANT, Loïc JD. **Os condenados da cidade: estudos sobre marginalidade avançada.** Revan, 2001.