Capítulo 10

O Papel da Tecnologia na Segurança Pública: Vigilância Inteligente, Reconhecimento Facial e Dilemas Éticos

The Role of Technology in Public Security: Intelligent Surveillance, Facial Recognition, and Ethical Dilemmas

Maikel Schneider
Bruno Rech
Jardel Zorzo
Ricardo José Konzen
Taynara de Azevedo
Sebastião Braz Martins Neto

Resumo: O avanço das tecnologias digitais tem transformado de maneira significativa as políticas de segurança pública, especialmente por meio da adoção de sistemas de vigilância inteligente, uso massivo de dados e reconhecimento facial. Este estudo analisa, a partir de uma revisão teórica, como essas tecnologias vêm sendo incorporadas às estratégias de prevenção do crime e quais dilemas éticos, jurídicos e sociais emergem desse processo. Discute-se a relação entre eficiência operacional e proteção de direitos fundamentais, destacando questões como privacidade, proteção de dados, viés algorítmico e discriminação. A análise evidencia que, embora a tecnologia amplie a capacidade de monitoramento do Estado, sua utilização sem regulação adequada pode reforçar desigualdades e comprometer garantias democráticas. Conclui-se que a incorporação de tecnologias na segurança pública deve estar acompanhada de marcos regulatórios claros, transparência institucional e mecanismos de controle social, de modo a assegurar que a inovação tecnológica contribua para a segurança sem fragilizar direitos fundamentais.

Palavras-chave: tecnologia; segurança pública; vigilância.

Abstract: The advancement of digital technologies has significantly transformed public security policies, particularly through the adoption of intelligent surveillance systems, large-scale data use, and facial recognition technologies. This article analyzes, based on a theoretical review, how these tools have been incorporated into crime prevention strategies and the ethical, legal, and social dilemmas arising from their use. The discussion addresses the relationship between operational efficiency and the protection of fundamental rights, highlighting issues such as privacy, data protection, algorithmic bias, and discrimination. The analysis indicates that, while technology expands the State's monitoring capacity, its unregulated use may reinforce inequalities and undermine democratic guarantees. The study concludes that the incorporation of technology into public security must be accompanied by clear regulatory frameworks, institutional transparency, and social oversight mechanisms to ensure that technological innovation enhances security without weakening fundamental rights.

Keywords: technology; public security; surveillance.

DOI: 10.47573/aya.5379.3.32.10

INTRODUÇÃO

A incorporação de tecnologias digitais às políticas de segurança pública tem se intensificado nas últimas décadas, impulsionada pela promessa de maior eficiência na prevenção e no combate ao crime. Ferramentas como sistemas de vigilância inteligente, monitoramento em tempo real, análise massiva de dados e reconhecimento facial passaram a integrar o cotidiano de diversas instituições de segurança, sendo frequentemente apresentadas como soluções capazes de ampliar a capacidade do Estado de identificar suspeitos, antecipar riscos e otimizar a alocação de recursos. Esse avanço tecnológico, no entanto, não ocorre de forma neutra nem isenta de controvérsias, especialmente quando envolve a coleta, o tratamento e o cruzamento de dados pessoais em larga escala.

No contexto brasileiro, a adoção dessas tecnologias ocorre em meio a desafios históricos relacionados à violência urbana, à desigualdade social e à fragilidade institucional. Em muitos casos, a tecnologia é incorporada como resposta rápida a demandas por segurança, sem que haja um debate aprofundado sobre seus impactos sociais, éticos e jurídicos. Sistemas de reconhecimento facial, por exemplo, têm sido utilizados em espaços públicos com o argumento de aumentar a eficácia policial, mas também levantam questionamentos sobre erros de identificação, seletividade racial e ausência de transparência nos critérios de funcionamento. Assim, o que se apresenta como inovação pode, se mal regulado, reproduzir ou até intensificar práticas discriminatórias já existentes.

Outro ponto central desse debate diz respeito à relação entre vigilância e privacidade. O uso contínuo de câmeras, bancos de dados integrados e algoritmos de análise preditiva redefine os limites entre segurança e liberdade individual. A ampliação da capacidade de monitoramento estatal coloca em tensão direitos fundamentais, como a intimidade, a proteção de dados pessoais e a presunção de inocência. Nesse cenário, a discussão sobre regulação do uso de dados, especialmente após a promulgação da Lei Geral de Proteção de Dados (LGPD), torna-se indispensável para compreender até que ponto a tecnologia pode ser empregada sem comprometer garantias democráticas.

Além disso, a crescente dependência de sistemas automatizados introduz o problema do viés algorítmico. Algoritmos são construídos a partir de dados históricos que refletem desigualdades sociais e padrões discriminatórios, o que pode resultar em decisões tecnológicas aparentemente neutras, mas socialmente injustas. Quando aplicados à segurança pública, esses vieses podem direcionar a vigilância de forma desproporcional a determinados grupos ou territórios, reforçando estigmas e aprofundando a desconfiança entre população e Estado.

Diante desse cenário, discutir o papel da tecnologia na segurança pública implica ir além da avaliação de sua eficiência operacional. É necessário refletir criticamente sobre os limites éticos, os riscos à privacidade, os impactos sociais do uso de algoritmos e a importância de marcos regulatórios claros e transparentes. Este estudo propõe-se a analisar essas questões a partir de uma revisão teórica, buscando compreender como a tecnologia pode contribuir para a segurança sem

comprometer direitos fundamentais, e quais desafios precisam ser enfrentados para que sua utilização esteja alinhada aos princípios do Estado democrático de direito.

FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica deste estudo reúne contribuições de autores e estudos que analisam a relação entre tecnologia, vigilância e segurança pública, buscando compreender tanto os avanços quanto os limites da incorporação de sistemas digitais na atuação estatal. A revisão dialoga com perspectivas da sociologia, do direito e dos estudos críticos da tecnologia para discutir conceitos como vigilância inteligente, reconhecimento facial, proteção de dados e viés algorítmico. Ao articular essas abordagens, o capítulo oferece o suporte conceitual necessário para problematizar a promessa de eficiência tecnológica à luz dos dilemas éticos, dos direitos fundamentais e dos desafios regulatórios que emergem no uso de tecnologias de monitoramento e análise de dados no campo da segurança pública.

Tecnologia e segurança pública: conceitos e evolução

A relação entre tecnologia e segurança pública não é recente, mas tem se transformado de maneira significativa ao longo do tempo. Desde o uso de instrumentos básicos de comunicação e registro até a adoção de sistemas informatizados e bases de dados integradas, a tecnologia sempre desempenhou um papel relevante na organização e na execução das atividades policiais. Nas últimas décadas, contudo, esse vínculo se intensificou com o avanço das tecnologias digitais, que passaram a ocupar posição central nas estratégias de prevenção, investigação e controle da criminalidade.

Em um primeiro momento, a incorporação tecnológica esteve associada à modernização administrativa e à melhoria dos meios de comunicação, como rádios, centrais telefônicas e sistemas de identificação criminal. Com o desenvolvimento da informática e da internet, especialmente a partir do final do século XX, surgiram ferramentas capazes de armazenar grandes volumes de informações e permitir o cruzamento de dados entre diferentes órgãos estatais. Esse processo ampliou a capacidade de monitoramento do Estado e inaugurou novas formas de vigilância, baseadas não apenas na presença física do agente, mas também na observação contínua mediada por dispositivos técnicos.

A partir do século XXI, a expansão das chamadas tecnologias inteligentes redefiniu o próprio conceito de segurança pública. Sistemas de videomonitoramento com análise automatizada, softwares de reconhecimento facial, algoritmos de previsão criminal e plataformas de big data passaram a ser apresentados como soluções capazes de antecipar comportamentos e otimizar a atuação policial. Nesse contexto, Lyon (2001; 2007) destaca que essas práticas se inserem em uma lógica mais ampla de “sociedade da vigilância”, na qual o controle se torna difuso e permanente, operando por meio da coleta contínua de dados sobre indivíduos, deslocamentos e comportamentos cotidianos.

No Brasil, a adoção dessas tecnologias ocorre de forma desigual e, muitas vezes, fragmentada, dependendo de investimentos pontuais e parcerias com empresas privadas de tecnologia. Em diversos estados e municípios, a inovação tecnológica é incorporada como resposta imediata às pressões sociais por segurança, sem planejamento de longo prazo ou avaliação sistemática de impactos. Esse movimento tende a privilegiar a eficiência operacional e a capacidade de vigilância, deixando em segundo plano discussões sobre transparência, proteção de dados e limites éticos do monitoramento estatal.

Assim, compreender a evolução da tecnologia na segurança pública exige reconhecer que ela não se restringe a um conjunto de ferramentas neutras. Trata-se de um processo historicamente construído, que reflete concepções específicas sobre crime, risco e controle social. As escolhas tecnológicas feitas pelo Estado influenciam diretamente a forma como a população é observada, classificada e governada, tornando indispensável uma análise crítica sobre os caminhos adotados e seus efeitos sobre a democracia e os direitos fundamentais.

Vigilância inteligente e uso de dados na prevenção do crime

A noção de vigilância inteligente está associada ao uso integrado de tecnologias digitais capazes de coletar, armazenar e analisar grandes volumes de dados com o objetivo de apoiar ações de prevenção e controle do crime. Diferentemente dos modelos tradicionais de vigilância, baseados majoritariamente na observação humana direta, a vigilância inteligente opera por meio de sistemas automatizados que combinam câmeras, sensores, bancos de dados e algoritmos analíticos. Esse modelo tem sido apresentado como uma evolução das práticas de segurança pública, ao prometer maior eficiência, rapidez na tomada de decisões e melhor direcionamento dos recursos estatais.

No campo da prevenção criminal, o uso de dados tornou-se um elemento central das políticas de segurança. A análise de padrões de ocorrências, horários, territórios e perfis estatísticos permite identificar áreas consideradas de maior risco e antecipar intervenções policiais. Autores como Lyon (2007) destacam que essa lógica de monitoramento contínuo redefine a forma como o Estado exerce o controle social, deslocando o foco da repressão posterior para a antecipação do comportamento considerado suspeito. Nesse contexto, a vigilância deixa de ser episódica e passa a se tornar permanente, sustentada por fluxos constantes de informação.

No Brasil, a vigilância inteligente tem sido implementada principalmente por meio de centros integrados de comando e controle, sistemas de videomonitoramento urbano e plataformas de análise criminal baseadas em dados estatísticos. Esses sistemas são frequentemente justificados pelo argumento da eficiência e da racionalização das ações policiais. Entretanto, como aponta Bruno (2013), a coleta massiva de dados não garante, por si só, melhores resultados em termos de segurança, especialmente quando não há critérios claros sobre o uso das informações, nem mecanismos de avaliação sobre os impactos dessas tecnologias nos direitos dos cidadãos.

Outro aspecto relevante diz respeito à natureza dos dados utilizados. Grande parte das informações empregadas nos sistemas de vigilância inteligente deriva de registros históricos de criminalidade, que refletem desigualdades sociais e padrões seletivos de policiamento. Segundo Zuboff (2019), a lógica da vigilância baseada em dados tende a transformar comportamentos em insumos para sistemas de previsão, muitas vezes sem que os indivíduos tenham conhecimento ou controle sobre como suas informações são utilizadas. Quando aplicada à segurança pública, essa lógica pode reforçar a concentração da vigilância sobre determinados territórios e grupos sociais, aprofundando estigmas já existentes.

Além disso, a dependência crescente de sistemas automatizados desloca decisões sensíveis para ambientes técnicos pouco transparentes. A definição de critérios, pesos e correlações algorítmicas raramente é acessível ao público ou mesmo aos operadores do sistema. Isso cria uma assimetria de informação que dificulta a responsabilização do Estado e limita o debate democrático sobre as estratégias de prevenção adotadas. Assim, embora a vigilância inteligente seja frequentemente apresentada como ferramenta de modernização da segurança pública, seu uso levanta questionamentos fundamentais sobre privacidade, controle social e legitimidade do poder estatal.

Dessa forma, a vigilância inteligente e o uso de dados na prevenção do crime devem ser analisados com cautela, considerando não apenas seus potenciais benefícios operacionais, mas também seus riscos sociais e políticos. A incorporação dessas tecnologias exige marcos regulatórios claros, transparência institucional e mecanismos de controle capazes de assegurar que a prevenção criminal não ocorra à custa de direitos fundamentais e da ampliação de práticas discriminatórias.

Reconhecimento facial: funcionamento, aplicações e limites técnicos

O reconhecimento facial constitui uma das tecnologias mais controversas atualmente utilizadas no campo da segurança pública. Trata-se de um sistema baseado em algoritmos capazes de identificar ou verificar a identidade de indivíduos a partir da análise de características faciais, como distância entre olhos, formato do nariz e contornos do rosto. Esses dados biométricos são convertidos em padrões matemáticos e comparados com imagens armazenadas em bancos de dados, permitindo associações automáticas em tempo real ou posteriormente. Embora apresentado como instrumento de precisão e modernização, seu funcionamento técnico envolve etapas complexas que impactam diretamente sua confiabilidade e seus efeitos sociais.

No âmbito da segurança pública, o reconhecimento facial tem sido empregado em espaços públicos, como ruas, estádios, aeroportos e transportes coletivos, com a justificativa de localizar pessoas procuradas pela justiça ou prevenir delitos. No Brasil, experiências desse tipo se intensificaram a partir da segunda metade da década de 2010, especialmente durante grandes eventos, quando o monitoramento em larga escala passou a ser visto como estratégia de controle. No entanto, estudos

apontam que a eficácia desses sistemas depende diretamente da qualidade das bases de dados utilizadas, da atualização das imagens e da calibração adequada dos algoritmos, fatores que nem sempre são observados na prática.

Um dos principais limites técnicos do reconhecimento facial refere-se à taxa de erro dos sistemas. Pesquisas internacionais indicam que os algoritmos apresentam maior índice de falhas na identificação de mulheres, pessoas negras e indivíduos pertencentes a grupos étnicos minoritários. Buolamwini e Gebru (2018) demonstram que esses erros não são aleatórios, mas refletem vieses presentes nos dados utilizados para treinar os sistemas, que frequentemente privilegiam rostos brancos e masculinos. Quando aplicados à segurança pública, esses erros podem gerar abordagens indevidas, constrangimentos e até prisões injustas, ampliando a seletividade já existente na atuação policial.

Além dos problemas de precisão, há limites relacionados à transparência e à auditabilidade dos sistemas. Como observa Pasquale (2015), muitos algoritmos operam como “caixas-pretas”, cujos critérios de funcionamento não são acessíveis ao público, às instituições de controle ou às próprias pessoas afetadas por suas decisões. Essa opacidade dificulta a contestação de erros, a correção de falhas e a responsabilização do Estado por danos causados pelo uso indevido da tecnologia. No caso do reconhecimento facial, isso se torna ainda mais sensível, pois envolve dados biométricos considerados altamente invasivos.

Outro ponto crítico diz respeito à ampliação do monitoramento sem consentimento explícito. Diferentemente de outros instrumentos de identificação, o reconhecimento facial pode ser aplicado de forma silenciosa e contínua, sem que os indivíduos saibam que estão sendo analisados. Lyon (2007) alerta que essa característica reforça práticas de vigilância difusa, nas quais o simples ato de circular em espaços públicos passa a ser monitorado e registrado, alterando a relação entre cidadãos e Estado. O risco, nesse caso, é a normalização de um controle permanente que reduz a esfera de anonimato e liberdade no espaço urbano.

Diante desses limites técnicos e sociais, o uso do reconhecimento facial na segurança pública exige cautela, avaliação rigorosa e regulamentação específica. Sem critérios claros, mecanismos de controle e transparência, essa tecnologia pode produzir mais danos do que benefícios, reforçando desigualdades, ampliando erros institucionais e comprometendo direitos fundamentais. Assim, sua análise não pode se restringir à promessa de eficiência, mas deve considerar os impactos concretos de sua aplicação no cotidiano da população e no funcionamento do Estado democrático de direito.

Privacidade, proteção de dados e direitos fundamentais

A ampliação do uso de tecnologias de vigilância na segurança pública intensifica o debate sobre privacidade e proteção de dados pessoais, colocando em evidência tensões centrais entre eficiência estatal e garantia de direitos fundamentais. A coleta massiva de informações, o monitoramento contínuo de espaços públicos e o cruzamento de dados sensíveis alteram profundamente a relação entre cidadãos

e Estado, exigindo novos parâmetros de controle jurídico e ético. Nesse contexto, a privacidade deixa de ser apenas uma questão individual e passa a assumir caráter coletivo, diretamente relacionado à qualidade da democracia e à preservação das liberdades civis.

Autores como Lyon (2001; 2007) destacam que a expansão das práticas de vigilância redefine os limites do que é considerado público e privado. A vigilância digital não se limita a observar comportamentos criminosos, mas captura rotinas, deslocamentos e interações cotidianas de pessoas que não são suspeitas de qualquer infração. Esse modelo de monitoramento permanente tende a naturalizar a exposição dos indivíduos, reduzindo o espaço de anonimato e transformando dados pessoais em insumos estratégicos para a gestão da segurança. Quando não há salvaguardas adequadas, esse processo pode produzir efeitos de autocensura e conformismo social.

No Brasil, a promulgação da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) representa um marco importante na tentativa de regular o tratamento de dados pessoais, inclusive pelo poder público. A LGPD estabelece princípios como finalidade, necessidade, transparência e responsabilização, que devem orientar a coleta e o uso de informações. No entanto, sua aplicação no campo da segurança pública ainda enfrenta ambiguidades, uma vez que a própria lei prevê exceções para atividades relacionadas à segurança e à investigação criminal. Essa abertura normativa gera um campo de tensão entre a proteção de dados e a ampliação das práticas de vigilância estatal.

Outro aspecto relevante é o caráter sensível dos dados utilizados pelas tecnologias de segurança, especialmente os dados biométricos, como imagens faciais, impressões digitais e padrões comportamentais. Esses dados possuem alto potencial de identificação e, quando utilizados de forma inadequada, podem causar danos irreversíveis aos indivíduos. Zuboff (2019) argumenta que a lógica de extração e exploração de dados, típica do chamado “capitalismo de vigilância”, tende a transformar informações pessoais em recursos estratégicos, muitas vezes sem consentimento ou conhecimento dos sujeitos monitorados. Embora sua análise se concentre no setor privado, suas reflexões ajudam a compreender os riscos de práticas semelhantes no âmbito estatal.

A proteção dos direitos fundamentais também envolve a garantia de mecanismos de controle, acesso à informação e possibilidade de contestação. Quando sistemas de vigilância operam de forma opaca, sem critérios claros ou canais de responsabilização, os cidadãos ficam impedidos de questionar decisões automatizadas que os afetam diretamente. Pasquale (2015) alerta que a falta de transparência algorítmica compromete princípios básicos do Estado de direito, como o devido processo legal e o direito à ampla defesa. No contexto da segurança pública, isso significa que erros ou abusos tecnológicos podem ocorrer sem que haja meios efetivos de correção ou reparação.

Dessa forma, a incorporação de tecnologias de vigilância à segurança pública impõe a necessidade de equilibrar a proteção coletiva com o respeito aos direitos individuais. A privacidade e a proteção de dados não devem ser tratadas como

obstáculos à segurança, mas como condições essenciais para que ela seja exercida de forma legítima. Sem marcos regulatórios claros, fiscalização independente e compromisso com os direitos fundamentais, o uso de tecnologias pode comprometer a própria base democrática que a segurança pública deveria proteger.

Viés algorítmico, discriminação e impactos sociais

O viés algorítmico constitui um dos principais desafios éticos associados ao uso de tecnologias digitais na segurança pública. Embora os algoritmos sejam frequentemente apresentados como instrumentos objetivos e neutros, sua construção depende de dados históricos, escolhas técnicas e critérios definidos por pessoas e instituições. Como resultado, esses sistemas tendem a reproduzir — e, em alguns casos, intensificar — desigualdades sociais já existentes. Quando aplicados à prevenção do crime e à vigilância, os vieses algorítmicos podem gerar impactos significativos sobre grupos sociais específicos, aprofundando processos de discriminação e estigmatização.

Grande parte dos sistemas utilizados na segurança pública é treinada com bases de dados que refletem padrões históricos de policiamento. Esses registros, por sua vez, carregam marcas de seletividade racial, territorial e socioeconômica. Autores como O'Neil (2016) demonstram que algoritmos baseados em dados enviesados tendem a produzir decisões igualmente enviesadas, criando ciclos de retroalimentação nos quais determinados grupos são continuamente classificados como de maior risco. No campo da segurança pública, isso pode significar maior vigilância sobre bairros periféricos, jovens negros e populações vulneráveis, independentemente de evidências concretas de criminalidade.

O reconhecimento facial e os sistemas de análise preditiva são exemplos claros desses riscos. Estudos como os de Buolamwini e Gebru (2018) revelam que algoritmos de identificação facial apresentam taxas de erro significativamente mais altas para mulheres e pessoas negras, em comparação com homens brancos. Quando essas tecnologias são utilizadas para orientar abordagens policiais ou decisões operacionais, erros técnicos se transformam em consequências sociais graves, como abordagens indevidas, constrangimentos públicos e prisões injustas. Assim, o viés algorítmico deixa de ser um problema técnico e passa a configurar uma questão de justiça social.

Além da discriminação direta, os impactos sociais do viés algorítmico incluem a ampliação da desconfiança entre população e Estado. Comunidades submetidas a monitoramento intensivo tendem a perceber a tecnologia como instrumento de controle e repressão, e não como ferramenta de proteção. Benjamin (2019) argumenta que a tecnologia pode funcionar como uma "inovação excludente", mascarando práticas discriminatórias sob a aparência de neutralidade científica. No contexto da segurança pública, isso compromete a legitimidade das políticas adotadas e dificulta a construção de relações baseadas em cooperação e confiança.

Outro problema relevante é a dificuldade de contestar decisões algorítmicas. Sistemas automatizados frequentemente operam com lógicas complexas e pouco

transparentes, o que limita a compreensão pública sobre como classificações e previsões são geradas. Pasquale (2015) destaca que essa opacidade impede o exercício pleno de direitos, como a contestação e a responsabilização, criando um cenário em que decisões que afetam diretamente a vida das pessoas são tomadas sem possibilidade de questionamento efetivo. No âmbito da segurança pública, isso representa um risco adicional à garantia do devido processo legal.

Diante desses desafios, torna-se fundamental reconhecer que a incorporação de tecnologias algorítmicas na segurança pública não pode ocorrer sem critérios rigorosos de avaliação, auditoria e controle social. A mitigação do viés exige transparência nos sistemas, revisão constante das bases de dados, participação de equipes multidisciplinares e marcos regulatórios que assegurem a proteção contra discriminações. Somente a partir desse cuidado será possível evitar que a tecnologia, em vez de promover segurança, aprofunde desigualdades e fragilize direitos fundamentais.

CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste estudo evidencia que a incorporação de tecnologias digitais à segurança pública representa um processo complexo, marcado tanto por promessas de eficiência quanto por desafios éticos, jurídicos e sociais significativos. Ferramentas como vigilância inteligente, análise de dados e reconhecimento facial têm ampliado a capacidade do Estado de monitorar, prevenir e responder a ocorrências criminais, mas também têm redefinido as formas de controle social e a relação entre poder público e cidadãos. Nesse sentido, a tecnologia não pode ser compreendida apenas como instrumento técnico, mas como parte de um modelo de gestão da segurança que produz efeitos diretos sobre direitos e liberdades fundamentais.

Ao longo do referencial teórico, observou-se que a evolução tecnológica na segurança pública tem sido acompanhada por uma intensificação das práticas de vigilância, muitas vezes implementadas de forma acelerada e sem debate público aprofundado. A utilização massiva de dados e sistemas automatizados desloca decisões sensíveis para ambientes técnicos pouco transparentes, o que dificulta a fiscalização democrática e a responsabilização do Estado. Quando essas tecnologias são aplicadas sem critérios claros de regulação e controle, abrem-se brechas para violações de privacidade, uso indevido de informações pessoais e ampliação de práticas discriminatórias.

Os limites técnicos e sociais das tecnologias analisadas também se mostraram centrais para a compreensão do tema. O reconhecimento facial e os sistemas algorítmicos, longe de serem neutros, refletem vieses presentes nas bases de dados e nas escolhas institucionais que orientam seu funcionamento. Esses vieses podem reforçar desigualdades raciais, territoriais e socioeconômicas, ampliando a vigilância sobre grupos historicamente marginalizados e comprometendo a legitimidade das políticas de segurança. Assim, a promessa de neutralidade tecnológica revela-se frágil quando confrontada com a realidade social em que esses sistemas operam.

Diante desse cenário, torna-se evidente que o uso da tecnologia na segurança pública exige marcos regulatórios sólidos, alinhados à proteção da privacidade, à transparência e ao respeito aos direitos fundamentais. A existência de legislações como a Lei Geral de Proteção de Dados representa um avanço importante, mas sua efetividade depende da aplicação rigorosa no campo da segurança e da criação de mecanismos de fiscalização independentes. Além disso, a participação da sociedade civil, de pesquisadores e de órgãos de controle é fundamental para acompanhar, avaliar e questionar o uso dessas tecnologias.

Por fim, conclui-se que a tecnologia pode contribuir para a segurança pública, desde que sua utilização esteja subordinada a princípios democráticos e a uma visão crítica sobre seus impactos sociais. A construção de políticas de segurança baseadas em inovação tecnológica deve priorizar não apenas a eficiência operacional, mas também a justiça, a equidade e a proteção das liberdades individuais. Somente assim será possível evitar que ferramentas desenvolvidas para promover segurança acabem reforçando desigualdades e fragilizando os fundamentos do Estado democrático de direito.

REFERÊNCIAS

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

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

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018.

BRUNO, Fernanda. **Máquinas de ver, modos de ser:** vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

BUOLAMWINI, Joy; GEBRU, Timnit. **Gender shades:** intersectional accuracy disparities in commercial gender classification. Proceedings of the Conference on Fairness, Accountability, and Transparency, New York, p. 77–91, 2018.

LYON, David. **Surveillance society:** monitoring everyday life. Buckingham: Open University Press, 2001.

LYON, David. **Surveillance studies: an overview.** Cambridge: Polity Press, 2007.

O'NEIL, Cathy. **Weapons of math destruction:** how big data increases inequality and threatens democracy. New York: Crown, 2016.

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

ZUBOFF, Shoshana. **The age of surveillance capitalism:** the fight for a human future at the new frontier of power. New York: PublicAffairs, 2019.