LexCult

| ARTIGOS

DOI: https://doi.org/10.30749/2594-8261.v10n1p343-370

TECNOLOGIAS DE VIGILÂNCIA E CONFIGURAÇÕES TERRITORIAIS: IMPACTOS DA VIGILÂNCIA DIGITAL NA SEGURANÇA E NOS DIREITOS FUNDAMENTAIS NO ESPAÇO URBANO

SURVEILLANCE TECHNOLOGIES AND TERRITORIAL CONFIGURATIONS: IMPACTS OF DIGITAL SURVEILLANCE ON SECURITY AND FUNDAMENTAL RIGHTS IN URBAN SPACE

Alice De Souza Araujo Barros [1]
Gilmar Felipe Meireles Vital [2]

Resumo: O presente trabalho analisa o uso das tecnologias de vigilância na segurança pública e suas implicações nas reconfigurações territoriais urbanas, examinando como ferramentas de monitoramento têm sido incorporadas às políticas de prevenção e controle da criminalidade. A pesquisa problematiza os benefícios e os limites do uso de videomonitoramento, reconhecimento facial, inteligência artificial e plataformas de integração de dados (Big Data) na gestão dos espaços urbanos. Busca-se compreender de que maneira esses dispositivos contribuem para a eficiência tática e a prevenção de riscos, bem como as vulnerabilidades associadas à violação da privacidade, ao efeito inibidor (chilling effect) e à reprodução de seletividades sociais e raciais no território. A análise mobiliza, além das perspectivas da vigilância e do controle social, uma lente espacial e territorial, considerando o espaço urbano como dimensão dinâmica das relações sociais, técnicas e de poder. A metodologia adota abordagem qualitativa, de caráter exploratório e descritivo, pautada em revisão bibliográfica e documental interdisciplinar. Os resultados demonstram que, embora ampliem a capacidade operacional do Estado, as tecnologias de vigilância não reduzem automaticamente a criminalidade e tendem a intensificar assimetrias territoriais e raciais quando desprovidas de salvaguardas regulatórias. Conclui-se pela necessidade de consolidação de uma governança democrática da vigilância urbana, pautada em Relatórios de Impacto à Proteção de Dados, auditorias algorítmicas e na preservação intransigente dos direitos fundamentais.

Palavras-chave: Território urbano. Tecnologias de vigilância. Segurança pública.

[1] Mestra em Administração pela UNIGRANRIO, graduada em Administração, Logística e Pedagogia, além de especializações em Auditoria e Controladoria, Consultoria e Planejamento Empresarial, Gestão em Logística e Docência no Ensino Superior. Docente pelo UNIABEU - Centro Universitário. http://orcid.org/0000-0003-0763-5503

[2] Bacharel em Direito pelo UNIABEU – Centro Universitário, Esp. Direito Penal e Processual penal. http://orcid.org/0009-0003-4204-6242

Seletividade algorítmica. Direitos fundamentais.

Abstract: This study analyzes the use of surveillance technologies in public security and their implications for urban territorial reconfigurations, examining how monitoring tools have been incorporated into crime prevention and control policies. The research addresses the benefits and limitations of using video surveillance, facial recognition, artificial intelligence, and integrated data platforms (Big Data) in urban space management. It aims to understand how these devices contribute to tactical efficiency and risk prevention, while also examining vulnerabilities related to privacy infringement, the chilling effect, and the reproduction of social and racial selectivities within the territory. In addition to perspectives on surveillance and social control, the analysis adopts a spatial and territorial lens, considering urban space as a dynamic dimension of social, technical, and power relations. The methodology adopts a qualitative, exploratory, and descriptive approach, grounded in an interdisciplinary bibliographic and documentary review. The findings demonstrate that although these technologies enhance state operational capacity, they do not automatically reduce crime and tend to intensify territorial and racial asymmetries when proper regulatory safeguards are lacking. The study concludes that establishing democratic governance of urban surveillance is essential, requiring Data Protection Impact Assessments, algorithmic audits, and strict adherence to fundamental rights.

Keywords: Urban territory. Surveillance Technologies. Public security. Algorithmic selectivity. Fundamental rights.

Recebido em: 04/09/2026
Aceito para publicação em: 01/10/2026

1. INTRODUÇÃO

O crescimento acelerado das cidades e a complexidade das relações sociais nos espaços urbanos têm produzido novos desafios para a segurança pública. A violência, a criminalidade e a crescente sensação de insegurança estimulam o poder público a buscar estratégias capazes de aprimorar a prevenção e o controle de ocorrências. Nesse cenário, o desenvolvimento tecnológico passou a ocupar espaço relevante nas políticas de segurança urbana, especialmente por meio da utilização de recursos destinados ao monitoramento, à identificação e à análise de informações. Ao mesmo tempo, a incorporação dessas tecnologias ao espaço urbano não ocorre de forma dissociada das características sociais e territoriais das cidades, uma vez que sua implementação pode produzir diferentes efeitos conforme os territórios e os grupos sociais alcançados.

Entre as principais ferramentas empregadas nesse contexto destacam-se as câmeras de videomonitoramento, os sistemas de reconhecimento facial, os drones, os sensores urbanos, os bancos de dados integrados e os recursos de inteligência

artificial. Essas tecnologias possibilitam ampliar a capacidade de observação dos espaços públicos, favorecer a integração de informações e proporcionar maior agilidade na atuação das forças de segurança. Entretanto, sua utilização também suscita discussões relacionadas à privacidade, à proteção de dados pessoais, à vigilância excessiva, à discriminação e aos limites da atuação estatal, tornando necessária uma análise que considere tanto suas possibilidades quanto seus riscos para a sociedade. Nesse sentido, a dimensão territorial torna-se relevante para compreender como os mecanismos tecnológicos de vigilância participam das formas contemporâneas de gestão, controle e organização do espaço urbano.

Diante desse contexto, o presente estudo delimita-se à análise do uso de tecnologias de vigilância no âmbito da segurança urbana, considerando seus efeitos sobre a prevenção e o controle da criminalidade e sua relação com a proteção dos direitos fundamentais. A análise considera, ainda, a dimensão territorial da vigilância, buscando compreender de que maneira a utilização desses recursos se relaciona com as diferentes configurações do espaço urbano e com possíveis desigualdades sociais e territoriais. Assim, estabelece-se como problema de pesquisa a seguinte questão: de que maneira o uso de tecnologias de vigilância pode contribuir para a segurança urbana e quais são os principais limites e riscos decorrentes de sua utilização em relação à proteção dos direitos fundamentais?

Como possíveis respostas ao problema proposto, parte-se de duas hipóteses principais. A primeira considera que as tecnologias de vigilância podem contribuir para o fortalecimento da segurança urbana, especialmente ao ampliar a capacidade de monitoramento, prevenção, identificação de ocorrências e atuação das forças de segurança. A segunda pressupõe que os benefícios dessas tecnologias não são automáticos e podem ser acompanhados de riscos relacionados à privacidade, à proteção de dados pessoais, à vigilância excessiva e à reprodução de desigualdades sociais e raciais, especialmente quando inexistem mecanismos adequados de regulamentação, transparência, controle e fiscalização. Considera-se, nesse sentido, que tais riscos podem assumir expressão territorial quando a distribuição, a intensidade ou as formas de utilização dos mecanismos de vigilância incidem de maneira diferenciada sobre determinados espaços urbanos e grupos sociais.

Dessa forma, o objetivo geral deste trabalho é analisar o uso de tecnologias de vigilância no contexto da segurança urbana, considerando suas contribuições para

a prevenção da criminalidade e os desafios relacionados à proteção dos direitos fundamentais. Para alcançar esse propósito, busca-se identificar as principais tecnologias utilizadas na segurança urbana; analisar suas contribuições para a prevenção e o controle da criminalidade; examinar os riscos relacionados à privacidade, à proteção de dados e à discriminação; analisar o papel das políticas públicas e da legislação na regulamentação dessas tecnologias; e discutir os desafios éticos, sociais e territoriais relacionados à utilização da vigilância tecnológica nos espaços urbanos.

A relevância deste estudo está relacionada à crescente incorporação de tecnologias de vigilância às estratégias de segurança pública e aos impactos que essa utilização pode produzir sobre a sociedade e sobre a organização dos espaços urbanos. A discussão mostra-se importante tanto para a comunidade acadêmica quanto para gestores e profissionais da área de segurança pública, uma vez que permite refletir sobre as possibilidades de utilização dos recursos tecnológicos sem desconsiderar os direitos fundamentais e as especificidades dos territórios nos quais essas tecnologias são implementadas. Nesse sentido, compreender os benefícios, limites e riscos associados à vigilância tecnológica pode contribuir para o desenvolvimento de políticas públicas mais responsáveis, transparentes e compatíveis com os princípios democráticos, especialmente no que se refere à proteção da privacidade, à proteção de dados, ao controle social e à redução de desigualdades territoriais.

Para o desenvolvimento da pesquisa, adotou-se uma abordagem qualitativa, de natureza exploratória e descritiva, fundamentada em pesquisa bibliográfica e documental. Foram considerados livros, artigos científicos, teses, dissertações, relatórios técnicos, documentos institucionais e legislações relacionados à segurança pública, às tecnologias de vigilância, à proteção de dados, aos direitos fundamentais e às configurações territoriais urbanas. O material selecionado foi analisado de forma temática, buscando identificar e discutir aspectos relacionados à eficiência da vigilância tecnológica, à prevenção da criminalidade, à sensação de segurança, à privacidade, à seletividade social e territorial e aos desafios éticos e jurídicos decorrentes de sua utilização.

2. REFERENCIAL TEÓRICO

2.1. VIGILÂNCIA, CONTROLE SOCIAL E TRANSFORMAÇÃO DOS ESPAÇOS URBANOS

O avanço das tecnologias digitais tem provocado transformações significativas na organização da sociedade contemporânea e na forma de gestão dos espaços urbanos. A expansão dos sistemas de informação, a integração de diferentes dispositivos tecnológicos e a utilização de dados para orientar decisões públicas contribuíram para o desenvolvimento de novas formas de gerenciamento das cidades. Nesse contexto, o conceito de cidades inteligentes (smart cities) está associado à utilização de tecnologias digitais para aprimorar serviços, processos de gestão e mecanismos de monitoramento urbano. A Autoridade Nacional de Proteção de Dados (ANPD, 2024) reconhece a crescente utilização dessas tecnologias e destaca que a expansão dos recursos digitais nas cidades deve ser acompanhada da análise dos impactos decorrentes do tratamento de dados pessoais.

A compreensão dessas transformações exige, entretanto, que o espaço urbano não seja considerado apenas como o local físico no qual as tecnologias são instaladas. Santos (2006) compreende o espaço geográfico a partir da relação entre sistemas de objetos e sistemas de ações, evidenciando que os objetos técnicos e as práticas sociais participam conjuntamente da produção e da transformação do espaço. Sob essa perspectiva, câmeras, sensores, sistemas biométricos, redes de comunicação e plataformas de processamento de dados podem ser compreendidos como elementos técnicos que passam a integrar a configuração dos espaços urbanos, enquanto as decisões institucionais e as práticas de vigilância definem formas específicas de utilização desses recursos. A contribuição de Santos permite, assim, compreender que a incorporação tecnológica não ocorre de maneira neutra ou homogênea, mas se articula às condições e às relações sociais existentes em cada território.

A perspectiva territorial também permite compreender que os espaços urbanos apresentam diferentes níveis de infraestrutura, informação e capacidade técnica. Na formulação de Santos (2006), os chamados espaços luminosos correspondem àqueles que concentram maiores densidades técnicas e informacionais, enquanto os espaços opacos apresentam menor presença dessas

condições. Essa diferenciação é relevante para a análise das tecnologias de vigilância porque demonstra que a modernização técnica das cidades não necessariamente ocorre de maneira uniforme. A distribuição dos equipamentos, das redes e dos sistemas de informação pode acompanhar desigualdades territoriais previamente existentes, produzindo diferentes condições de acesso, monitoramento e controle nos espaços urbanos.

A vigilância constitui um importante mecanismo de controle social e pode ser compreendida a partir da análise do poder e do disciplinamento desenvolvida por Foucault (1987). Ao discutir o modelo panóptico, o autor demonstra que a possibilidade permanente de observação produz efeitos sobre o comportamento dos indivíduos, uma vez que a percepção de estar sob vigilância pode favorecer a autorregulação das condutas. Dessa maneira, o exercício do poder não depende necessariamente da intervenção direta e permanente de uma autoridade, podendo ocorrer mediante mecanismos que induzem comportamentos e estabelecem padrões de normalidade (Foucault, 1987).

A perspectiva de Foucault (1987) permanece relevante diante das transformações produzidas pelas tecnologias digitais, embora os mecanismos contemporâneos de vigilância apresentem características mais amplas do que aquelas observadas nos modelos tradicionais de controle. Lyon (2018) destaca que a vigilância contemporânea envolve a coleta, o processamento, o armazenamento e a análise sistemática de informações, permitindo que os indivíduos sejam monitorados por meio de diferentes dispositivos e sistemas tecnológicos. Assim, a vigilância deixa de depender exclusivamente da observação direta e passa a incorporar processos automatizados de tratamento de dados (Foucault, 1987; Lyon, 2018).

O diálogo entre Foucault (1987), Lyon (2018) e Santos (2006) permite ampliar a compreensão do fenômeno, uma vez que a vigilância digital pode ser analisada simultaneamente como mecanismo de controle social e como elemento de transformação territorial. Enquanto Foucault evidencia as relações de poder produzidas pela possibilidade de observação, Lyon demonstra a ampliação dessas práticas por meio da coleta e do processamento de dados, e Santos contribui para compreender como os objetos técnicos e as ações institucionais se incorporam à produção do espaço. Dessa forma, a vigilância não se restringe à relação entre Estado e indivíduo, mas também envolve a maneira como determinados recursos

tecnológicos são distribuídos, organizados e utilizados nos diferentes territórios urbanos (Foucault, 1987; Lyon, 2018; Santos, 2006).

A transformação tecnológica dos espaços urbanos também pode ser observada na utilização de sistemas destinados ao monitoramento e à gestão das cidades. A ANPD (2024) destaca que a expansão das cidades inteligentes envolve a utilização crescente de tecnologias capazes de processar informações sobre pessoas e ambientes urbanos. Embora esses recursos possam favorecer a melhoria dos serviços públicos, sua utilização exige atenção aos riscos associados à coleta e ao tratamento de dados pessoais, especialmente quando os sistemas são empregados em espaços públicos e em atividades de monitoramento (ANPD, 2024).

A partir da perspectiva territorial, essa expansão tecnológica também demanda atenção às diferenças existentes entre os espaços urbanos. A presença de equipamentos e sistemas de vigilância pode depender da infraestrutura disponível, das prioridades das políticas públicas e da capacidade institucional dos diferentes territórios. Assim, a análise da vigilância tecnológica deve considerar não apenas quais tecnologias são utilizadas, mas também onde são instaladas, quais áreas são priorizadas e quais grupos sociais podem ser mais frequentemente submetidos aos mecanismos de monitoramento. Essa abordagem não pressupõe que todos os territórios sejam submetidos aos mesmos níveis de vigilância, mas permite investigar criticamente a possibilidade de que desigualdades espaciais preexistentes influenciem a distribuição e os efeitos dessas tecnologias (Santos, 2006).

A utilização de tecnologias de vigilância, portanto, apresenta uma dimensão que ultrapassa a perspectiva meramente técnica. Foucault (1987) possibilita compreender os mecanismos de poder e disciplinamento associados à vigilância, Lyon (2018) evidencia a transformação desses mecanismos diante da digitalização da sociedade, Santos (2006) permite compreender a dimensão espacial e territorial da incorporação técnica, enquanto a ANPD (2024) atualiza essa discussão ao demonstrar que tecnologias como biometria e reconhecimento facial já integram diferentes setores, inclusive a segurança pública, trazendo simultaneamente possibilidades de utilização e desafios relacionados à privacidade e à proteção de dados (Foucault, 1987; Lyon, 2018; Santos, 2006; ANPD, 2024).

Dessa maneira, compreender a vigilância como fenômeno social, político, tecnológico e territorial constitui etapa fundamental para analisar sua utilização na

segurança urbana. A expansão dos dispositivos de monitoramento amplia a capacidade de observação dos espaços públicos, mas também exige reflexão sobre os efeitos produzidos sobre os indivíduos e sobre os territórios nos quais essas tecnologias são implementadas. A discussão teórica apresentada permite, portanto, compreender que a tecnologia pode fortalecer mecanismos de segurança, mas também ampliar formas de controle social e produzir efeitos diferenciados no espaço urbano, tornando necessário analisar os benefícios e os limites de sua utilização a partir das particularidades territoriais e das relações sociais que estruturam as cidades (Foucault, 1987; Lyon, 2018; Santos, 2006; ANPD, 2024).

2.2. TECNOLOGIAS DE VIGILÂNCIA E SEGURANÇA URBANA

A incorporação de tecnologias digitais às políticas de segurança pública tem ampliado as possibilidades de monitoramento, coleta e análise de informações. Entre os principais recursos utilizados encontram-se as câmeras de videomonitoramento, os sistemas de reconhecimento facial, os drones, os sensores urbanos, os bancos de dados integrados e as ferramentas baseadas em inteligência artificial. Esses instrumentos podem contribuir para ampliar a capacidade de observação dos espaços públicos, identificar ocorrências, integrar informações e subsidiar a atuação das instituições responsáveis pela segurança (Pereira, 2019).

A utilização desses recursos está relacionada às transformações ocorridas nas estratégias contemporâneas de prevenção e controle da criminalidade. Garland (2001) identifica uma crescente valorização da gestão do risco nas políticas de segurança, nas quais a prevenção assume importância juntamente com as respostas posteriores à ocorrência dos delitos. Nesse contexto, as tecnologias de vigilância podem fornecer informações destinadas à identificação de padrões, ao monitoramento de áreas e ao direcionamento das ações institucionais, contribuindo para uma atuação orientada pela análise de riscos (Garland, 2001).

A perspectiva de Garland (2001) pode ser articulada à análise de Lyon (2018), uma vez que a gestão contemporânea do risco depende, em grande medida, da capacidade de produzir e processar informações. Enquanto Garland (2001) evidencia a transformação das estratégias de controle da criminalidade, Lyon (2018) demonstra como as tecnologias digitais ampliaram a capacidade de coleta, armazenamento e análise de dados. Assim, os sistemas de vigilância passam a constituir instrumentos

utilizados para produzir informações que podem subsidiar decisões relacionadas à segurança urbana (Garland, 2001; Lyon, 2018).

No contexto brasileiro, Pereira (2019) destaca a utilização de sistemas de videomonitoramento, Centros Integrados de Comando e Controle e mecanismos de inteligência policial como instrumentos incorporados às estratégias de segurança pública. Essas ferramentas podem favorecer a integração entre diferentes instituições, ampliar a capacidade de identificação de ocorrências e auxiliar na atuação dos agentes responsáveis pela segurança. Dessa maneira, a tecnologia pode representar um recurso complementar para aumentar a capacidade operacional das instituições públicas (Pereira, 2019).

A evolução desse cenário pode ser observada em iniciativas contemporâneas do próprio Ministério da Justiça e Segurança Pública. O projeto Data Lake, atualmente associado à reestruturação e ampliação do Sistema Córtex, prevê a integração de bases de dados estruturados e não estruturados e a utilização de recursos como big data, machine learning, reconhecimento facial, reconhecimento de voz, *deep learning* e ferramentas de busca baseadas em inteligência artificial. A iniciativa demonstra que a segurança pública brasileira vem incorporando estruturas tecnológicas destinadas não apenas ao armazenamento de informações, mas também à sua integração e análise em larga escala (Brasil, 2026).

A iniciativa apresentada pelo Ministério da Justiça e Segurança Pública pode ser relacionada à perspectiva de Garland (2001), especialmente porque a utilização de grandes volumes de dados amplia a capacidade institucional de identificar padrões e orientar estratégias de prevenção. Ao mesmo tempo, aproxima-se da discussão de Lyon (2018), uma vez que o funcionamento dessas estruturas depende da coleta, integração e processamento sistemático de informações. O desenvolvimento dessas ferramentas evidencia, portanto, a passagem de modelos de vigilância baseados predominantemente na observação para estruturas integradas de análise de dados e inteligência tecnológica (Garland, 2001; Lyon, 2018; Brasil, 2026).

Entretanto, a existência de tecnologias mais avançadas não significa, por si só, que haverá redução automática da criminalidade. Garland (2001) demonstra que a gestão do risco envolve um conjunto amplo de estratégias e instituições, enquanto Pereira (2019) evidencia que os resultados das tecnologias de vigilância dependem das condições concretas de implementação. Dessa maneira, os recursos tecnológicos

devem ser compreendidos como instrumentos inseridos em políticas de segurança mais amplas, cuja efetividade depende de planejamento, integração institucional e capacidade de utilização das informações produzidas (Garland, 2001; Pereira, 2019).

A utilização dessas tecnologias também apresenta diferenças relacionadas à infraestrutura e à capacidade institucional dos municípios e órgãos públicos. Pereira (2019) destaca que determinadas iniciativas tecnológicas estão concentradas em grandes centros urbanos, o que evidencia desigualdades na implementação dos mecanismos de vigilância. Essa realidade demonstra que a expansão tecnológica não ocorre de maneira uniforme e depende das condições econômicas, institucionais e administrativas disponíveis em cada contexto (Pereira, 2019).

Portanto, as tecnologias de vigilância apresentam potencial para ampliar a capacidade de monitoramento, prevenção e resposta das instituições de segurança pública. Entretanto, a articulação entre Garland (2001), Lyon (2018), Pereira (2019) e as iniciativas contemporâneas do Ministério da Justiça e Segurança Pública demonstra que a tecnologia não deve ser compreendida como solução isolada. Sua efetividade depende da integração entre recursos tecnológicos, planejamento institucional, políticas públicas e mecanismos de controle capazes de assegurar uma utilização adequada dessas ferramentas (Garland, 2001; Lyon, 2018; Pereira, 2019; Brasil, 2026).

2.3. VIGILÂNCIA TECNOLÓGICA, PRIVACIDADE, DISCRIMINAÇÃO E DIREITOS FUNDAMENTAIS

Embora as tecnologias de vigilância possam contribuir para o fortalecimento da segurança urbana, sua expansão também produz questionamentos relacionados à privacidade, à proteção de dados, à liberdade individual e à igualdade. Lyon (2018) destaca que a vigilância contemporânea está diretamente relacionada à coleta e ao processamento de informações, o que amplia significativamente a capacidade de acompanhamento dos indivíduos. Dessa maneira, quanto maior a capacidade de coleta e análise de dados, maior também é a necessidade de estabelecer limites para sua utilização (Lyon, 2018).

A perspectiva de Foucault (1987) contribui para compreender os efeitos sociais decorrentes da expansão da vigilância. A possibilidade de observação constante pode produzir mudanças no comportamento dos indivíduos e favorecer

mecanismos de autorregulação. Quando essa lógica é associada às tecnologias digitais, o monitoramento pode alcançar dimensões mais amplas, especialmente porque câmeras, sensores e sistemas automatizados permitem registrar e processar informações de maneira contínua (Foucault, 1987).

Lyon (2018) amplia essa discussão ao demonstrar que a vigilância contemporânea não depende exclusivamente da observação física. Dados produzidos em diferentes contextos podem ser reunidos, processados e utilizados para classificar indivíduos e orientar decisões. Essa transformação amplia a capacidade de vigilância e cria novos desafios relacionados ao controle das informações e à proteção da privacidade (Lyon, 2018).

Bauman e Lyon (2013) aprofundam essa reflexão ao analisarem as relações entre vigilância e transformações sociais contemporâneas. A expansão dos mecanismos de monitoramento pode favorecer formas mais intensas de classificação e controle, especialmente quando informações pessoais passam a ser utilizadas para identificar, categorizar ou acompanhar indivíduos. Dessa forma, a busca por segurança precisa ser equilibrada com a preservação das liberdades individuais e dos direitos fundamentais (Bauman; Lyon, 2013).

Os riscos relacionados à vigilância tecnológica tornam-se particularmente relevantes no caso do reconhecimento facial. A ANPD (2024) destaca que a expansão dessa tecnologia ocorre em diferentes setores, inclusive na segurança pública, mas também suscita preocupações relacionadas à privacidade, à proteção de dados e ao risco de discriminação. A autoridade ressalta ainda que o uso de reconhecimento facial em espaços públicos pode ocorrer sem que os indivíduos tenham necessariamente conhecimento de que estão sendo monitorados ou de que seus dados biométricos estão sendo tratados (ANPD, 2024).

A dimensão técnica dos riscos relacionados ao reconhecimento facial também é evidenciada pelo National Institute of Standards and Technology (NIST). As avaliações realizadas pelo órgão demonstram que as taxas de falsos positivos e falsos negativos podem apresentar variações entre grupos demográficos, considerando fatores como idade, sexo e região de nascimento. O NIST também aponta que diferenças de desempenho podem estar relacionadas, entre outros fatores, à qualidade das imagens e à representatividade dos grupos nos conjuntos de dados utilizados para treinamento dos algoritmos (NIST, 2026).

A constatação apresentada pelo NIST contribui para aprofundar a discussão sobre discriminação algorítmica desenvolvida por Silva e Bruno (2020). Enquanto esses autores chamam atenção para os riscos sociais decorrentes de sistemas tecnológicos que podem reproduzir desigualdades, as avaliações técnicas do NIST demonstram que diferenças de desempenho entre grupos demográficos podem ser empiricamente mensuradas. Dessa maneira, o debate sobre vieses algorítmicos não se limita a uma questão teórica, podendo ser analisado também a partir de indicadores técnicos de desempenho (Silva; Bruno, 2020; NIST, 2026).

As informações apresentadas pelo NIST também demonstram que a qualidade dos dados e das imagens utilizadas pelos sistemas constitui elemento importante para o desempenho dos algoritmos. O órgão identifica situações nas quais condições inadequadas de iluminação ou diferenças na representação de determinados grupos podem contribuir para variações nas taxas de erro. Essa constatação reforça a necessidade de avaliação técnica dos sistemas antes de sua utilização em contextos nos quais uma identificação equivocada possa produzir consequências relevantes para os indivíduos (NIST, 2026).

A ANPD (2024) complementa essa perspectiva técnica ao destacar a necessidade de adoção de medidas técnicas e administrativas destinadas à proteção dos dados pessoais e à mitigação dos riscos associados ao tratamento de dados biométricos. A autoridade também ressalta a importância da proteção dos direitos dos titulares e da segurança da informação. Assim, a discussão sobre reconhecimento facial envolve simultaneamente dimensões tecnológicas, jurídicas e sociais (ANPD, 2024).

O diálogo entre Foucault (1987), Lyon (2018), Bauman e Lyon (2013), Silva e Bruno (2020), ANPD (2024) e NIST (2026) permite compreender que os riscos associados às tecnologias de vigilância não se limitam à possibilidade de invasão da privacidade. Também envolvem relações de poder, classificação de indivíduos, diferenças de desempenho entre grupos, possibilidade de discriminação e utilização de dados pessoais em larga escala. Dessa maneira, a expansão tecnológica da segurança pública deve ser acompanhada de mecanismos capazes de preservar os direitos fundamentais e reduzir os riscos de utilização inadequada dessas ferramentas (Foucault, 1987; Bauman; Lyon, 2013; Lyon, 2018; Silva; Bruno, 2020;

ANPD, 2024; NIST, 2026).

2.4. REGULAMENTAÇÃO, POLÍTICAS PÚBLICAS E GOVERNANÇA DEMOCRÁTICA DA VIGILÂNCIA

A expansão das tecnologias de vigilância evidencia a necessidade de estabelecer mecanismos de regulamentação e controle capazes de delimitar sua utilização. A busca por maior eficiência na segurança pública deve estar acompanhada da proteção da privacidade, dos dados pessoais e dos demais direitos fundamentais. Nesse sentido, a regulamentação constitui instrumento importante para definir finalidades, responsabilidades, limites e mecanismos de fiscalização relacionados ao uso das tecnologias de vigilância (Brasil, 2018; ANPD, 2024).

A Lei Geral de Proteção de Dados Pessoais estabelece princípios relacionados ao tratamento de dados pessoais, entre os quais se destacam a finalidade, a adequação, a necessidade, a segurança e a transparência. Esses parâmetros assumem importância diante da utilização de tecnologias capazes de coletar e processar informações sobre indivíduos. No caso da vigilância tecnológica, a observância desses princípios contribui para estabelecer limites ao tratamento de dados e para fortalecer a proteção dos titulares (Brasil, 2018).

A necessidade de regulamentação pode ser relacionada às preocupações apresentadas por Lyon (2018) acerca da expansão da sociedade da vigilância. Quanto maior a capacidade tecnológica de coletar, armazenar e processar informações, maior também é a necessidade de mecanismos capazes de controlar sua utilização. A regulamentação, nesse sentido, não deve ser entendida necessariamente como obstáculo ao desenvolvimento tecnológico, mas como instrumento de equilíbrio entre inovação, segurança e proteção dos direitos individuais (Lyon, 2018).

A discussão de Bauman e Lyon (2013) também contribui para compreender a importância de estabelecer limites para a expansão dos mecanismos de monitoramento. A vigilância pode produzir formas de classificação e controle que ultrapassam sua finalidade inicial quando não existem mecanismos adequados de fiscalização. Por essa razão, a utilização de tecnologias de vigilância deve estar submetida a critérios de proporcionalidade, transparência e responsabilidade institucional (Bauman; Lyon, 2013).

No contexto brasileiro, a ANPD (2024) demonstra que a biometria e o reconhecimento facial constituem tecnologias de crescente relevância, mas que também envolvem riscos específicos relacionados à privacidade, à proteção de dados

e à discriminação. O estudo da autoridade destaca a necessidade de medidas técnicas e administrativas capazes de mitigar riscos e assegurar os direitos dos titulares. Essa perspectiva reforça a necessidade de que a expansão das tecnologias de vigilância seja acompanhada por mecanismos institucionais de governança e controle (ANPD, 2024).

A necessidade de governança também se torna evidente diante do desenvolvimento de novas estruturas tecnológicas na segurança pública brasileira. O Ministério da Justiça e Segurança Pública, por meio do projeto Data Lake, prevê a ampliação da integração de bases de dados e a utilização de tecnologias de big data, machine learning, reconhecimento facial, reconhecimento de voz e deep learning no

Sistema Córtex. O desenvolvimento dessas ferramentas demonstra a crescente capacidade de processamento de informações pelas instituições de segurança e, consequentemente, a importância de mecanismos de governança capazes de estabelecer finalidades e limites para sua utilização (Brasil, 2026).

A expansão dessas estruturas reforça a necessidade de transparência sobre a finalidade da coleta de dados, os critérios de utilização dos sistemas e os mecanismos de proteção das informações. A ANPD (2024) destaca a importância da implementação de medidas técnicas e administrativas para proteção dos dados biométricos, enquanto o Ministério da Justiça e Segurança Pública evidencia a ampliação das estruturas de integração e análise de informações para fins de segurança. O diálogo entre essas perspectivas demonstra que o desenvolvimento tecnológico precisa ser acompanhado de mecanismos institucionais capazes de reduzir riscos e assegurar o uso responsável dos dados (ANPD, 2024; Brasil, 2026). Além da regulamentação, a utilização das tecnologias de vigilância deve estar integrada a políticas públicas mais amplas de segurança urbana. Garland (2001) demonstra que a gestão contemporânea do risco envolve diferentes estratégias de prevenção e controle, não podendo ser reduzida à utilização de uma única ferramenta tecnológica. A tecnologia pode contribuir para a identificação de padrões e para a orientação das ações institucionais, mas sua efetividade depende de planejamento, integração e capacidade institucional (Garland, 2001).

Pereira (2019) também demonstra que os resultados das tecnologias de vigilância estão relacionados às condições concretas de implementação e à integração entre os órgãos envolvidos. Nesse sentido, o uso de câmeras, sistemas de

reconhecimento facial, centros integrados e bancos de dados deve ser articulado a estratégias mais amplas de segurança pública. A tecnologia representa, portanto, instrumento complementar, cuja efetividade depende de sua inserção em políticas públicas estruturadas (Pereira, 2019).

A governança democrática das tecnologias de vigilância exige, portanto, a articulação entre inovação tecnológica, eficiência na segurança pública, proteção de dados, transparência e controle institucional. Foucault (1987) evidencia as relações de poder presentes nos mecanismos de vigilância; Lyon (2018) demonstra a ampliação desses mecanismos por meio das tecnologias digitais; Bauman e Lyon

(2013) analisam suas consequências sociais; enquanto a ANPD (2024) apresenta os riscos contemporâneos associados à biometria e ao reconhecimento facial. Essa articulação demonstra que a governança tecnológica deve considerar simultaneamente eficiência, direitos fundamentais e mecanismos de controle (Foucault, 1987; Bauman; Lyon, 2013; Lyon, 2018; ANPD, 2024).

Dessa forma, o principal desafio não consiste simplesmente em ampliar a utilização de tecnologias de vigilância, mas em estabelecer condições para que esses recursos sejam empregados de maneira proporcional, transparente e responsável. A segurança urbana pode se beneficiar do desenvolvimento tecnológico, desde que sua implementação esteja vinculada a políticas públicas estruturadas, mecanismos de regulamentação, avaliação dos riscos e proteção dos direitos fundamentais (Garland, 2001; Brasil, 2018; ANPD, 2024).

O diálogo entre as perspectivas apresentadas permite concluir que a tecnologia deve ser compreendida como instrumento complementar das políticas de segurança urbana. Sua efetividade depende não apenas de sua capacidade técnica, mas também da existência de planejamento institucional, critérios de utilização, transparência, fiscalização e proteção dos cidadãos. Nesse sentido, o desafio contemporâneo consiste em conciliar a utilização dos recursos tecnológicos para prevenção e controle da criminalidade com a preservação da privacidade, da igualdade, da liberdade e da dignidade humana (Garland, 2001; Lyon, 2018; ANPD, 2024; NIST, 2026).

3. METODOLOGIA

A metodologia corresponde ao conjunto de procedimentos utilizados para

orientar o desenvolvimento da pesquisa e possibilitar o alcance dos objetivos estabelecidos. Conforme Gil (2010), a pesquisa científica constitui um processo racional e sistemático destinado à produção de conhecimentos e à obtenção de respostas para problemas previamente formulados.

Quanto à abordagem, a presente pesquisa caracteriza-se como qualitativa, uma vez que busca compreender e interpretar aspectos relacionados ao uso das tecnologias de vigilância no contexto da segurança urbana, considerando suas contribuições, limitações e implicações para a proteção dos direitos fundamentais.

Segundo Gil (2010), a abordagem qualitativa permite aprofundar a compreensão de fenômenos sociais a partir da análise de seus significados, características e relações. Marconi e Lakatos (2019) também destacam que a pesquisa qualitativa privilegia a interpretação dos fenômenos investigados, permitindo analisar aspectos que não podem ser reduzidos exclusivamente a dados quantitativos.

Quanto aos objetivos, a pesquisa é classificada como exploratória, pois busca ampliar a compreensão acerca da utilização de tecnologias de vigilância na segurança urbana, identificando suas possibilidades, limitações e principais implicações sociais, jurídicas e territoriais. Para Gil (2010), a pesquisa exploratória é apropriada quando se pretende proporcionar maior familiaridade com determinado problema, permitindo seu aprimoramento e a construção de uma compreensão mais ampla sobre o fenômeno investigado. Marconi e Lakatos (2007) igualmente associam a pesquisa exploratória à aproximação inicial e ao aprofundamento de questões ainda sujeitas a diferentes interpretações.

Quanto aos procedimentos técnicos, o estudo caracteriza-se como pesquisa bibliográfica e documental. A pesquisa bibliográfica foi desenvolvida a partir da consulta a livros, artigos científicos, dissertações, teses e outras produções acadêmicas relacionadas à vigilância, segurança urbana, reconhecimento facial, inteligência artificial, proteção de dados, privacidade, território e direitos fundamentais. Marconi e Lakatos (2019) compreendem a pesquisa bibliográfica como aquela realizada a partir da produção científica e bibliográfica já disponível sobre determinado tema, permitindo ao pesquisador estabelecer contato com o conhecimento produzido anteriormente e utilizá-lo como fundamento para a investigação.

A pesquisa documental, por sua vez, complementou o levantamento bibliográfico mediante a análise de legislações, documentos institucionais, relatórios

técnicos e materiais oficiais relacionados à utilização de tecnologias de vigilância, à segurança pública e à proteção de dados pessoais. Segundo Gil (2010), a pesquisa documental utiliza materiais que podem ser analisados e interpretados de acordo com os objetivos da investigação, possibilitando o acesso a informações relevantes que não necessariamente foram produzidas originalmente para fins científicos. Nesse estudo, a análise documental possibilitou aproximar a discussão teórica da realidade institucional e normativa relacionada à segurança urbana e ao uso de tecnologias de monitoramento.

Para a seleção do material bibliográfico e documental, foram consideradas produções relacionadas diretamente ao problema e aos objetivos da pesquisa. O levantamento contemplou publicações acadêmicas e documentos institucionais disponíveis em bases e repositórios científicos e oficiais, incluindo materiais relacionados às tecnologias de vigilância, videomonitoramento, reconhecimento facial, inteligência artificial, segurança pública, privacidade, proteção de dados, direitos fundamentais, território urbano e desigualdades socioespaciais. Como descritores de busca, foram consideradas combinações dos termos “tecnologias de vigilância”, “vigilância digital”, “segurança urbana”, “videomonitoramento”, “reconhecimento facial”, “inteligência artificial”, “proteção de dados”, “privacidade”, “direitos fundamentais”, “território urbano”, “desigualdade territorial” e “seletividade algorítmica”, de acordo com a pertinência de cada fonte em relação ao problema investigado.

Quanto ao recorte temporal, foram priorizadas produções publicadas entre 2019 e 2026, período adotado como referência para a composição do corpus contemporâneo da pesquisa, sem exclusão de obras anteriores consideradas clássicas e indispensáveis à fundamentação teórica, como Foucault (1987), Garland (2001), Marconi e Lakatos (2007) e Bardin (2011). Essa opção permitiu articular contribuições teóricas consolidadas com estudos e documentos mais recentes sobre vigilância digital, tecnologias aplicadas à segurança pública, proteção de dados e transformação dos espaços urbanos.

A análise do material selecionado foi realizada de forma qualitativa e temática, buscando identificar, organizar e interpretar os principais argumentos presentes nas fontes consultadas. Para Bardin (2011), a análise de conteúdo constitui um conjunto de técnicas destinado à análise das comunicações, possibilitando identificar

categorias, temas e sentidos presentes no material investigado. Dessa forma, o procedimento adotado permitiu organizar a literatura e os documentos selecionados em eixos relacionados às contribuições das tecnologias para a segurança urbana, aos mecanismos de vigilância e controle, aos riscos relacionados à privacidade e à discriminação, às desigualdades territoriais e aos mecanismos de regulamentação e governança.

A análise foi estruturada de maneira articulada ao problema de pesquisa, procurando estabelecer relações entre os diferentes autores e perspectivas identificados na literatura. Nesse processo, foram consideradas, de forma integrada, as contribuições das tecnologias de vigilância para a prevenção e o controle da criminalidade e os possíveis riscos decorrentes de sua utilização, especialmente aqueles relacionados à privacidade, à proteção de dados, à discriminação algorítmica, às desigualdades territoriais e aos direitos fundamentais. A dimensão territorial foi incorporada como categoria analítica transversal, buscando compreender de que maneira a utilização dessas tecnologias se relaciona com as diferentes configurações do espaço urbano e com as desigualdades socioespaciais nele existentes. Assim, a metodologia adotada possibilitou desenvolver uma análise crítica do fenômeno, evitando limitar o estudo à descrição das tecnologias existentes.

Por fim, os resultados obtidos a partir da pesquisa bibliográfica e documental foram confrontados e interpretados à luz do referencial teórico, buscando estabelecer relações entre as diferentes perspectivas encontradas na literatura e os documentos analisados. Esse procedimento permitiu discutir em que medida as tecnologias de vigilância podem contribuir para a segurança urbana e quais limites devem ser considerados para que sua utilização seja compatível com a proteção dos direitos fundamentais, considerando também seus possíveis efeitos sobre as configurações territoriais e sobre grupos e espaços urbanos submetidos a diferentes condições de vigilância e controle.

4. ANÁLISE E DISCUSSÃO DOS RESULTADOS

A análise do *corpus* bibliográfico e documental selecionado revela que a incorporação de tecnologias de vigilância na segurança urbana brasileira não constitui mero reaparelhamento técnico das corporações policiais. Trata-se de uma reconfiguração profunda das dinâmicas de gestão do espaço urbano e de controle

social.

Para conferir rigor analítico aos achados da pesquisa, os resultados das fontes normativas, relatórios institucionais e literatura especializada foram sistematizados em quatro eixos temáticos centrais, conforme demonstrado na síntese analítica do Quadro 1.

Quadro 1 - *Matriz de Categorização Temática e Evidências da Pesquisa*

Categoria Analítica	**Evidências extraídas do Corpus Bibliográfico e Documental**	**Articulação Teórica e Normativa**	**Implicações para a Segurança Urbana e Direitos**
1. Eficiência Operacional e Gestão do Risco	Expansão de redes integradas de CFTV, biometria e plataformas de *Big Data* (Sistema Córtex/Data Lake) para aprimorar a atuação ostensiva e investigativa.	Garland (2001); Pereira (2019); Brasil (2026).	Transição do policiamento reativo para a gestão preventiva do risco; maior capacidade de resposta e dissuasão local.
2. Vieses Algorítmicos e Seletividade Penal	Registros empíricos de disparidades demográficas e taxas elevadas de erro no reconhecimento facial aplicado a grupos vulneráveis.	Silva e Bruno (2020); NIST (2026); ANPD (2024); Foucault (1987); Santos (2006).	Reprodução e automação de desigualdades e racismo estrutural em abordagens policiais e Prisões injustas por falsos positivos.
3. Lacunas Normativas e Proteção de Dados	Exceção contida no art. 4º, III, da LGPD; ausência de regulamentação específica (*LGPD Penal*) e opacidade na coleta massiva em vias públicas.	Brasil (2018); Bauman e Lyon (2013); UNESCO (2023).	Insegurança jurídica; risco de vigilância massiva desproporcional e ameaça à autodeterminação informativa.
4. Governança Democrática e Transparência	Exigência institucional de Relatórios de Impacto à Proteção de Dados (RIPD), auditorias algorítmicas e participação social na formulação de políticas.	Lyon (2018); ANPD (2024); UNESCO (2023).	Condicionamento da utilidade da tecnologia ao estrito respeito às garantias constitucionais e ao controle social.

Fonte: Elaborado pelos autores (2026)

4.1. EFICIÊNCIA OPERACIONAL E A LÓGICA DE GESTÃO DO RISCO

Os documentos examinados apontam que a expansão dos sistemas de videomonitoramento, dos sensores urbanos e das plataformas de análise de dados orienta-se pela promessa de elevar a eficiência estatal na prevenção e repressão a

infrações penais. A literatura correlata sustenta que a presença visível de dispositivos de monitoramento e a atuação ostensiva balizada por dados podem produzir potencial de dissuasão em perímetros delimitados.

Essa constatação alinha-se diretamente ao modelo de "cultura do controle" fundamentado por Garland (2001), no qual a segurança pública migra da reabilitação individual para a gestão de riscos e a contenção sistêmica de danos. Sob essa ótica, as tecnologias de vigilância funcionam como otimizadoras de recursos escassos, permitindo o direcionamento tático das forças policiais.

No entanto, o confronto entre as diretrizes do Ministério da Justiça e Segurança Pública (Brasil, 2026) e a crítica sociológica de Pereira (2019) demonstra que o ganho operacional trazido por iniciativas como o Sistema Córtex e seu *Data Lake* não garante, isoladamente, a redução sustentável da criminalidade em âmbito macroestrutural. A literatura analisada reforça que a eficiência puramente técnica não substitui políticas públicas integradas de desenvolvimento social, habitação e iluminação urbana.

Além disso, a asserção frequentemente reproduzida no senso comum de que a vigilância ostensiva amplia a "sensação de segurança" deve ser lida com reserva científica: a literatura aponta que a sensação de segurança é um fenômeno multifatorial e subjetivo que não decorre automaticamente da instalação de equipamentos tecnológicos, podendo, em determinados cenários de hipervigilância, aumentar a percepção comunitária de ameaça constante.

4.2. DISCRIMINAÇÃO ALGORÍTMICA, SELETIVIDADE E VULNERABILIDADE

A análise conjunta dos estudos sobre impactos sociais e dos relatórios técnicos internacionais elucida que a tecnologia de vigilância não é neutra. A articulação entre os ensaios de Silva e Bruno (2020) e as avaliações empíricas do *National Institute of Standards and Technology* (NIST, 2026) confirma que algoritmos de reconhecimento facial carregam disparidades demográficas de desempenho significativas. Essa não neutralidade também pode ser compreendida a partir da dimensão territorial, uma vez que, conforme Santos (2006), o espaço resulta da articulação entre sistemas de objetos e sistemas de ações, de modo que as tecnologias incorporadas ao espaço urbano se relacionam às formas pelas quais os territórios são organizados, utilizados e controlados.

O NIST (2026) aponta que a acurácia dos sistemas varia em função de variáveis como raça, sexo e idade, apresentando margens de erro consideravelmente mais altas na identificação de pessoas negras, mulheres e jovens. Quando transpostos sem filtro crítico para a segurança pública, esses vieses técnicos traduzem-se em graves injustiças sociais, corroborando as teses de Foucault (1987) quanto à atualização de mecanismos de classificação e punição.

Como bem alertam Silva e Bruno (2020), a utilização desprovida de validação prévia automatiza o racismo estrutural e a seletividade penal já presentes no sistema de justiça. A ocorrência de prisões equivocadas fundadas em incompatibilidades de leitura biométrica evidencia que a suposta "precisão matemática" da inteligência artificial pode atuar como um véu de objetividade sobre práticas históricas de estigmatização de territórios periféricos.

Assim, a seletividade algorítmica deve ser analisada não apenas pelas características técnicas dos sistemas, mas também pelos territórios nos quais são implementados e pelas populações que neles circulam. A articulação entre tecnologia, espaço e poder evidencia que os efeitos da vigilância digital dependem das condições concretas de sua utilização, tornando necessária uma análise que considere simultaneamente os riscos algorítmicos, as desigualdades sociais e as configurações territoriais.

4.3. O DESAFIO REGULATÓRIO: PROTEÇÃO DE DADOS E O EFEITO INIBIDOR (CHILLING EFFECT)

A análise normativa revela um vácuo regulatório preocupante no ordenamento jurídico brasileiro. Embora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) consolide princípios essenciais como finalidade, necessidade, transparência e segurança, o seu art. 4º, inciso III, excepciona da sua incidência direta o tratamento de dados realizado para fins de segurança pública e persecução penal. No âmbito legislativo, a lacuna deixada pela exceção do art. 4º, III, da LGPD impulsionou a atuação da Comissão de Juristas instituída no âmbito da Câmara dos Deputados, a qual elaborou o Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal (conhecido como Anteprojeto da LGPD Penal ou LGPD-Penal). Inspirada na LGPD e na Diretiva 2016/680 da União Europeia, a proposta busca estabelecer balizas específicas para o tratamento de dados

biométricos, definir os direitos dos titulares e disciplinar o uso de tecnologias de vigilância (como o reconhecimento facial) e de decisões automatizadas na investigação criminal. Embora o anteprojeto forneça diretrizes fundamentais de transparência, proporcionalidade e auditoria de sistemas, sua efetiva conversão em lei ainda tramita no Congresso Nacional, mantendo temporariamente o cenário de incerteza jurídica e assimetria normativa no setor de segurança pública.

Essa ressalva, pendente de regulamentação por meio de legislação específica (*LGPD Penal*), abre margem para a coleta massiva e desproporcional de dados biométricos em espaços públicos. A esse respeito, Bauman e Lyon (2013) sustentam que a vigilância líquida e invisível dilui a fronteira entre a prevenção legítima do crime e a intrusão desmotivada na vida privada.

A convergência entre os posicionamentos da Autoridade Nacional de Proteção de Dados (ANPD, 2024) e da UNESCO (2023) aponta que a captura contínua de imagens e informações comportamentais em vias públicas sem consentimento ou transparência gera o chamado *chilling effect* (efeito inibidor). Trata-se da inibição involuntária do exercício de liberdades civis fundamentais como a liberdade de manifestação, a liberdade de reunião e o direito à livre circulação, uma vez que o cidadão se percebe sob monitoramento e enquadramento constante.

4.4. DIRETRIZES PARA UMA GOVERNANÇA DEMOCRÁTICA DA VIGILÂNCIA

Por fim, a síntese do *corpus* analisado indica que a superação das fragilidades observadas exige a transição de um paradigma puramente eficientista para um modelo de governança democrática da vigilância urbana.

A ANPD (2024) e a UNESCO (2023) convergem ao indicar que a adoção de sistemas tecnológicos avançados pelas forças de segurança deve ser obrigatoriamente precedida pela elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), auditorias algorítmicas independentes e a garantia de explicabilidade das decisões automatizadas.

Conclui-se, em alinhamento com Lyon (2018) e Pereira (2019), que os recursos tecnológicos devem desempenhar papel estritamente complementar no âmbito de políticas públicas estruturadas de segurança. A consolidação de cidades seguras e justas pressupõe o equilíbrio inegociável entre a inovação tecnológica no combate à criminalidade e o respeito intransigente às garantias individuais e ao

Estado Democrático de Direito.

5. CONSIDERAÇÕES FINAIS

O presente estudo analisou o uso de tecnologias de vigilância no âmbito da segurança urbana, buscando compreender de que maneira esses recursos podem contribuir para a prevenção e o controle da criminalidade e quais são os principais limites e riscos decorrentes de sua utilização em relação à proteção dos direitos fundamentais. A partir da análise bibliográfica e documental realizada, verificou-se que a incorporação de tecnologias de monitoramento, reconhecimento facial, sensores, plataformas de integração de dados e recursos de inteligência artificial amplia significativamente a capacidade operacional das instituições responsáveis pela segurança pública. Entretanto, os resultados também demonstram que a expansão tecnológica não produz, de forma automática, maior segurança ou redução sustentável da criminalidade.

Em relação ao problema de pesquisa, conclui-se que as tecnologias de vigilância podem contribuir para a segurança urbana ao ampliar a capacidade de monitoramento dos espaços públicos, favorecer a identificação de ocorrências, integrar informações e proporcionar maior agilidade à atuação das forças de segurança. Todavia, essas contribuições estão condicionadas à forma como os recursos são implementados, utilizados e fiscalizados. A análise realizada evidenciou que a eficiência tecnológica, quando considerada de maneira isolada, não é suficiente para enfrentar a complexidade dos problemas relacionados à criminalidade urbana, sendo necessária sua articulação com políticas públicas mais amplas e com mecanismos de prevenção social.

Quanto aos objetivos específicos, a pesquisa permitiu identificar diferentes tecnologias empregadas no gerenciamento e monitoramento dos espaços urbanos, destacando-se as câmeras de videomonitoramento, os sistemas de reconhecimento facial, os drones, os sensores e as plataformas de integração e análise de dados. Também foi possível examinar suas contribuições para a atuação das forças de segurança, especialmente no que se refere à ampliação da capacidade de observação, à integração de informações e ao direcionamento das ações institucionais. A análise evidenciou, contudo, que tais recursos devem ser compreendidos como instrumentos complementares às políticas de segurança

pública, e não como soluções autônomas para a criminalidade.

No que se refere à primeira hipótese, segundo a qual as tecnologias de vigilância poderiam contribuir para o fortalecimento da segurança urbana por meio da ampliação da capacidade de monitoramento, prevenção, identificação de ocorrências e atuação das forças de segurança, conclui-se que ela foi confirmada parcialmente. A análise realizada indica que os recursos tecnológicos podem otimizar procedimentos operacionais, ampliar a capacidade de resposta e produzir efeitos de dissuasão em determinados contextos. Entretanto, não foram identificados elementos suficientes para sustentar que a simples adoção dessas tecnologias produza redução automática e sustentável da criminalidade em escala mais ampla. Sua efetividade depende de fatores institucionais, sociais, territoriais e políticos que ultrapassam a dimensão estritamente tecnológica.

A segunda hipótese, relacionada à existência de riscos associados à privacidade, à proteção de dados pessoais, à vigilância excessiva e à reprodução de desigualdades sociais e raciais, foi confirmada pela análise desenvolvida. O corpus bibliográfico e documental evidenciou que a expansão de mecanismos de vigilância pode produzir efeitos sobre a privacidade e as liberdades individuais, especialmente quando ocorre sem transparência suficiente, critérios claros de utilização e mecanismos adequados de fiscalização. Também foram identificados riscos relacionados à discriminação algorítmica, particularmente em sistemas que utilizam reconhecimento facial e outras formas automatizadas de identificação.

Outro resultado relevante diz respeito à dimensão territorial da vigilância. A utilização de tecnologias de monitoramento não ocorre de maneira neutra no espaço urbano, uma vez que a escolha dos locais monitorados, dos indivíduos submetidos a determinadas formas de controle e dos dados considerados relevantes pode reproduzir desigualdades previamente existentes. Dessa maneira, a expansão tecnológica pode, em determinadas circunstâncias, reforçar processos de seletividade social e racial, sobretudo quando os sistemas são implementados sem avaliação adequada de seus impactos e sem mecanismos capazes de identificar e corrigir eventuais distorções.

A análise também demonstrou que a proteção dos direitos fundamentais constitui um dos principais desafios relacionados à expansão das tecnologias de vigilância. A utilização de reconhecimento facial, biometria e sistemas integrados de

processamento de dados aumenta a capacidade do Estado de identificar e acompanhar indivíduos, mas também amplia a necessidade de estabelecer limites para a coleta, armazenamento, compartilhamento e utilização dessas informações. Nesse contexto, a segurança pública precisa ser compatibilizada com a privacidade, a proteção de dados pessoais, a liberdade, a igualdade e a dignidade humana.

Outro aspecto identificado refere-se ao chamado efeito inibidor (*chilling effect*), decorrente da percepção de monitoramento permanente. A presença contínua de mecanismos de vigilância pode influenciar o comportamento dos indivíduos e produzir restrições indiretas ao exercício de determinadas liberdades civis. Dessa forma, os impactos da vigilância não devem ser avaliados exclusivamente a partir de indicadores de eficiência operacional ou redução de ocorrências, mas também a partir de seus efeitos sobre a experiência cotidiana dos cidadãos e sobre a utilização democrática dos espaços públicos.

No âmbito normativo, a pesquisa evidenciou a importância da existência de mecanismos específicos de regulamentação e governança. Embora a Lei Geral de Proteção de Dados Pessoais estabeleça princípios relevantes para o tratamento de dados pessoais, a utilização de dados para fins de segurança pública e persecução penal apresenta particularidades que demandam regulamentação própria e mecanismos específicos de controle. Essa situação reforça a necessidade de maior clareza quanto às finalidades do tratamento, às responsabilidades institucionais, aos critérios de acesso e compartilhamento de informações e às formas de fiscalização dos sistemas utilizados pelo poder público.

Diante dos resultados encontrados, entende-se que a governança das tecnologias de vigilância deve superar uma perspectiva exclusivamente eficientista, segundo a qual a expansão tecnológica seria suficiente para produzir maior segurança. A utilização desses recursos deve estar vinculada a políticas públicas estruturadas, planejamento urbano, prevenção social da violência, transparência institucional, participação social e mecanismos permanentes de avaliação. Nesse sentido, a tecnologia deve funcionar como instrumento de apoio às políticas de segurança, permanecendo submetida aos princípios democráticos e às garantias fundamentais.

Como contribuição acadêmica, o estudo possibilita uma compreensão interdisciplinar da relação entre tecnologia, vigilância, segurança urbana, território e

direitos fundamentais. A pesquisa demonstra que o debate sobre tecnologias de vigilância não pode ser restrito à sua eficiência técnica, pois envolve relações de poder, processos de classificação social, proteção de dados, desigualdades territoriais e questões éticas relacionadas à atuação do Estado. Dessa forma, o trabalho contribui para ampliar a reflexão acadêmica sobre os limites e as possibilidades da utilização dessas ferramentas em sociedades cada vez mais orientadas pelo processamento de dados.

No âmbito das políticas públicas e da gestão da segurança, os resultados indicam a necessidade de adoção de mecanismos de governança capazes de acompanhar todo o ciclo de utilização das tecnologias de vigilância. A implementação de novos sistemas deve ser precedida por avaliação de riscos, definição clara de finalidades, estabelecimento de responsabilidades, medidas de segurança da informação, transparência e mecanismos de fiscalização. Também se mostra relevante a realização de avaliações periódicas capazes de verificar a efetividade dos sistemas e identificar eventuais impactos desproporcionais sobre determinados grupos ou territórios.

Como limitação, destaca-se o caráter bibliográfico e documental da pesquisa, que não envolveu coleta de dados diretamente com agentes de segurança, gestores públicos ou comunidades submetidas aos sistemas de vigilância. Consequentemente, os resultados não permitem mensurar empiricamente a percepção da população ou os impactos concretos de determinada tecnologia sobre índices de criminalidade em um município específico. Essa limitação, entretanto, não compromete o alcance dos objetivos propostos, uma vez que o estudo teve como finalidade analisar criticamente a produção acadêmica e documental relacionada ao fenômeno investigado.

Para pesquisas futuras, recomenda-se o desenvolvimento de estudos empíricos capazes de complementar os resultados obtidos. Pesquisas de campo podem investigar a percepção de comunidades monitoradas, a atuação dos agentes de segurança diante de sistemas de reconhecimento facial, os índices de falsos positivos e negativos, os efeitos territoriais da instalação de câmeras e a percepção dos cidadãos sobre privacidade e sensação de segurança. Estudos comparativos entre diferentes municípios e estados também podem contribuir para identificar condições que favoreçam ou dificultem a utilização responsável dessas tecnologias.

Diante do exposto, conclui-se que as tecnologias de vigilância apresentam

potencial relevante para o fortalecimento da segurança urbana, especialmente no monitoramento de espaços públicos, na integração de informações e na ampliação da capacidade de resposta institucional. Entretanto, sua efetividade não pode ser dissociada da proteção de dados, da transparência, da supervisão, da avaliação de riscos e do controle social. Nesse sentido, a governança dessas tecnologias deve ser indiscutivelmente territorial, considerando as peculiaridades locais e as diferentes configurações sociais e espaciais que caracterizam o espaço urbano brasileiro, de modo a prevenir o aprofundamento das vulnerabilidades climáticas e sociais que também participam da produção e organização dos territórios. Assim, a adoção tecnológica deve estar articulada a políticas públicas estruturadas, planejamento urbano e estratégias de prevenção social, garantindo que os ganhos proporcionados pela inovação não ocorram em detrimento dos direitos fundamentais.

Assim, a construção de uma política de segurança urbana tecnologicamente orientada exige o equilíbrio entre inovação, eficiência e proteção dos cidadãos. O principal desafio consiste em assegurar que a ampliação da capacidade de vigilância estatal não resulte na naturalização de mecanismos excessivos de controle ou na reprodução de desigualdades já existentes. Nesse sentido, a consolidação de uma governança democrática da vigilância urbana constitui condição essencial para que os avanços tecnológicos sejam incorporados às políticas públicas de segurança de maneira proporcional, transparente, responsável e compatível com o Estado Democrático de Direito.

REFERÊNCIAS

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Estudo técnico: Reconhecimento facial na segurança pública e proteção de dados pessoais**. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd. Acesso em: 10 ago. 2026.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 jul. 2026.

BRASIL. Câmara dos Deputados. **Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal (LGPD Penal)**. Elaborado pela Comissão de Juristas. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br. Acesso em: 15 ago. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. **Sistema Córtex e integração de dados de segurança pública (Data Lake)**. Brasília, DF: MJSP, 2026. Disponível em: https://www.gov.br/mj. Acesso em: 10 ago. 2026.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Tradução de Raquel Ramalhete. Petrópolis: Vozes, 1987.

GARLAND, David. **The culture of control: crime and social order in contemporary society**. Oxford: Oxford University Press, 2001.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

LYON, David. **The culture of surveillance: watching as a way of life**. Cambridge: Polity Press, 2018.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia do trabalho científico**. 7. ed. São Paulo: Atlas, 2007.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2019.

NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Face Recognition Vendor Test (FRVT): Evaluation of Facial Recognition Technology**. Washington, DC: U.S. Department of Commerce, 2026. Disponível em: https://www.nist.gov. Acesso em: 15 ago. 2026.

PEREIRA, M. A. Tecnologias de vigilância e segurança pública no Brasil: limites e possibilidades. **Revista Brasileira de Segurança Pública**, São Paulo, v. 13, n. 2, p. 45-62, 2019.

SANTOS, Milton. **A natureza do espaço: técnica e tempo, razão e emoção.** 4. ed. 2. reimpr. São Paulo: Editora da Universidade de São Paulo, 2006.

SILVA, Tarcízio; BRUNO, Fernanda. Reconhecimento facial e vieses raciais no Brasil. **Revista Eco-Pós**, Rio de Janeiro, v. 23, n. 3, p. 75-96, 2020.

UNESCO – ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. **Recomendação sobre a Ética da Inteligência Artificial**. Paris: UNESCO, 2023. Disponível em: https://unesdoc.unesco.org. Acesso em: 15 ago. 2026.