PROGRAMA MURALHA PAULISTA: NOVOS DESAFIOS NA PROTEÇÃO DE DADOS E EMPREGO DE TECNOLOGIAS NA SEGURANÇA PÚBLICA PAULISTA

Fernanda Soares de Lima (IC[1]) e Prof. Dr. Marco Aurelio Barberato Genghini (Orientador)

Apoio: PIBIC Mackenzie

RESUMO

A evolução digital do Estado tem avançado de forma significativa na formulação e implementação de políticas públicas, especialmente no âmbito da segurança pública, que é marcado pela crescente incorporação de tecnologias de monitoramento e análise de dados. Partindo dessa premissa, o Estado de São Paulo instituiu o Programa Muralha Paulista, regido pelo Decreto Estadual nº 68.828/2024, política pública voltada ao aprimoramento das estratégias de segurança por meio da integração de bases de dados, sistemas de monitoramento e inteligência artificial. Nesse sentido, a presente pesquisa tem como objetivo analisar os impactos jurídicos decorrentes da utilização dessas tecnologias, especialmente quanto à proteção de dados pessoais, à transparência, à governança da inteligência artificial e à preservação dos direitos fundamentais. Metodologicamente, a pesquisa possui uma abordagem qualitativa, desenvolvida mediante revisão bibliográfica, pesquisa documental e estudo de caso, fundamentando-se na legislação vigente, na doutrina especializada, em documentos oficiais, dados públicos, informações referentes ao Programa Muralha Paulista e parâmetros internacionais, como o AI Act da União Europeia. Diante disso, a análise evidencia que a incorporação da inteligência artificial e de sistemas avançados de tratamento de dados pode representar um importante instrumento de evolução das políticas de segurança, ao possibilitar maior integração entre bases informacionais, otimização de recursos e ampliação da capacidade de atuação estatal. Entretanto, a utilização dessas ferramentas também apresenta desafios relacionados aos limites da vigilância tecnológica, exigindo a adoção de mecanismos efetivos de governança, transparência, supervisão humana e responsabilização quanto ao seu uso. Por fim, a inovação tecnológica deve ser acompanhada de garantias capazes de assegurar o uso legítimo e proporcional dos dados pessoais, preservando os direitos fundamentais e evitando que a busca por eficiência comprometa as salvaguardas previstas no ordenamento jurídico brasileiro.

Palavras-chave: Programa Muralha Paulista; Proteção de Dados; Inteligência Artificial.

[1] Graduanda em Direito pela Faculdade de Direito da Universidade Presbiteriana Mackenzie e integrante do Programa Institucional de Bolsas de Iniciação Científica (PIBIC), sob orientação do Prof. Dr. Marco Aurelio Barberato Genghini.

ABSTRACT

The digital evolution of the State has advanced significantly in the formulation and implementation of public policies, particularly in the field of public security, which is increasingly marked by the incorporation of monitoring and data analysis technologies. Based on this premise, the State of São Paulo established the Muralha Paulista Program, governed by State Decree No. 68.828/2024, a public policy aimed at improving security strategies through the integration of databases, monitoring systems, and artificial intelligence. In this context, the present research aims to analyze the legal impacts arising from the use of these technologies, particularly with regard to the protection of personal data, transparency, artificial intelligence governance, and the preservation of fundamental rights. Methodologically, the research adopts a qualitative approach, developed through a literature review, documentary research, and a case study, based on current legislation, specialized literature, official documents, public data, information concerning the Muralha Paulista Program, and international parameters, such as the European Union's AI Act. The analysis shows that the incorporation of artificial intelligence and advanced data processing systems may represent an important instrument for the development of security policies by enabling greater integration between information databases, optimization of resources, and expansion of the State's capacity to act. However, the use of these tools also presents challenges related to the limits of technological surveillance, requiring effective mechanisms for governance, transparency, human oversight, and accountability regarding their use. Finally, technological innovation must be accompanied by safeguards capable of ensuring the legitimate and proportionate use of personal data, preserving fundamental rights and preventing the pursuit of efficiency from compromising the safeguards established by the Brazilian legal system.

Keywords**:** Muralha Paulista Program; Data protection; Artificial intelligence.

1. INTRODUÇÃO

A incorporação de novas tecnologias à gestão estatal reconfigurou os processos de formulação e execução de políticas públicas, especialmente no campo da segurança pública. O uso de inteligência artificial, sistemas de monitoramento, reconhecimento biométrico e ferramentas de tratamento de dados amplia as possibilidades de coleta, integração e análise de informações, permitindo novas formas de prevenção e enfrentamento da criminalidade. Ao mesmo tempo, a expansão dessas tecnologias evidencia questões que ultrapassam a busca por eficiência, envolvendo a proteção de dados pessoais, a privacidade, a transparência, a participação social e os limites da atuação estatal diante dos direitos fundamentais.

Partindo dessa premissa, insere-se o Programa Muralha Paulista, instituído pelo Estado de São Paulo por meio do Decreto Estadual nº 68.828 (São Paulo, 2024). O programa tem como objetivo restringir a mobilidade criminal e aumentar a probabilidade de prisão durante seus deslocamentos no território paulista, sendo estruturado por um conjunto integrado de soluções tecnológicas de infraestrutura física, operação em nuvem, sensores e sistemas de inteligência artificial. Além disso, o decreto também prevê a utilização dos dados e informações produzidos pelo programa para a localização de pessoas desaparecidas e estabelece, entre seus princípios, o compromisso com a proteção de dados pessoais.

Segundo informações divulgadas pelo Governo do Estado de São Paulo em fevereiro de 2026, o Programa Muralha Paulista contava com aproximadamente 94 mil câmeras integradas em mais de 300 municípios paulistas. Essa estrutura reúne leitores automáticos de placas, equipamentos de reconhecimento facial e dispositivos de monitoramento em tempo real, integrando câmeras e sensores de órgãos públicos e privados e permite o cruzamento de informações com bases utilizadas pelas forças de segurança, incluindo o Banco Nacional de Mandados de Prisão (São Paulo, 2026c).

A expansão dessa infraestrutura demonstra que os dados passaram a ocupar posição central na execução das políticas públicas de segurança. A coleta e o tratamento de grandes volumes de informações permitem a integração de diferentes bases e o desenvolvimento de ferramentas capazes de auxiliar a identificação de pessoas, veículos e situações consideradas relevantes para a atuação policial. Com isso, observa-se uma transformação na forma de atuação do poder público, na qual as tecnologias digitais passam a participar de diferentes etapas da atividade estatal, desde a produção de informações até o apoio à tomada de decisões.

Esse processo também se relaciona às transformações associadas à chamada Indústria 4.0, marcada pela integração entre tecnologias digitais, conectividade, automação e

tratamento de grandes volumes de dados (Lima; Gomes, 2020). Quando aplicada à segurança pública, essa lógica amplia as possibilidades de utilização de ferramentas tecnológicas pelo Estado, mas também levanta questionamentos sobre a extensão da automação, a participação humana e os mecanismos necessários para acompanhar e controlar os resultados produzidos por esses sistemas.

Entre essas tecnologias, o reconhecimento facial merece atenção particular. Embora possa ser empregado para auxiliar a localização e identificação de pessoas, sua utilização também envolve discussões sobre precisão, vieses e possíveis impactos desiguais sobre diferentes grupos. Joy Buolamwini e Timnit Gebru, ao estudarem sistemas de análise facial, identificaram diferenças de desempenho relacionadas a características como tom de pele e gênero, contribuindo para o debate sobre vieses algorítmicos e sobre a necessidade de avaliação e supervisão dessas ferramentas (Buolamwini; Gebru, 2018). Essa referência não permite concluir, por si só, que o sistema utilizado pelo Programa Muralha Paulista apresente os mesmos resultados, mas demonstra a importância de avaliar os riscos associados às tecnologias antes e durante sua utilização.

No ordenamento jurídico brasileiro, essas questões devem ser consideradas em conjunto com o fortalecimento da proteção dos dados pessoais. A Emenda Constitucional nº 115, de 2022, incluiu expressamente o direito à proteção de dados pessoais, inclusive nos meios digitais, entre os direitos e garantias fundamentais previstos no artigo 5º, LXXIX, da Constituição Federal de 1988 (Brasil, 1988; Brasil, 2022). A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), por sua vez, estabelece princípios relacionados ao tratamento de dados pessoais, como finalidade, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização (Brasil, 2018). Portanto, o art. 4º, III, da lei estabelece tratamento específico para as atividades realizadas exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado e investigação e repressão de infrações penais, enquanto o § 1º determina que essa matéria seja disciplinada por legislação específica e observe medidas proporcionais e estritamente necessárias. Essa particularidade torna ainda mais relevante a análise dos limites jurídicos aplicáveis ao tratamento de dados no âmbito da segurança pública.

A análise do Programa Muralha Paulista parte, portanto, da relação entre tecnologia, gestão de dados, políticas públicas e proteção de direitos fundamentais. Nesse sentido, as contribuições de Marco Aurélio Barberato Genghini são relevantes para compreender os riscos e limites associados à gestão de dados e as transformações decorrentes da incorporação de inteligência artificial na atual segurança pública (Genghini, 2024). A perspectiva de Maria Paula Dallari Bucci contribui para a compreensão das políticas públicas em sua dimensão jurídica e institucional, especialmente a partir da relação entre formulação,

implementação e avaliação (Bucci, 2013). Por outro lado, as reflexões de Przemyslaw Palka permitem aprofundar questões relacionadas à privacidade, aos dados e aos efeitos da transformação tecnológica sobre a relação entre Estado e indivíduo. Apresentadas no referencial de Genghini, essas reflexões complementam a abordagem ao tratar dos efeitos da correlação de dados em larga escala (Palka, 2020 apud Genghini, 2024, p. 24). Esses referenciais permitem analisar o Muralha Paulista não apenas como uma iniciativa tecnológica, mas como uma política pública inserida em um processo mais amplo de transformação da atuação estatal.

No âmbito internacional, o *AI Act* da União Europeia constitui um parâmetro comparativo relevante para a análise dos riscos relacionados ao uso de inteligência artificial. O regulamento adota uma abordagem baseada em riscos, na qual as exigências impostas aos sistemas variam conforme o potencial de impacto sobre a saúde, a segurança e os direitos fundamentais, estabelecendo obrigações mais rigorosas para aplicações consideradas de maior risco[2]. No caso da identificação biométrica remota em tempo real para fins de aplicação da lei, o art. 5º estabelece hipóteses específicas e excepcionais de utilização, condicionadas à necessidade e à proporcionalidade da medida, com limitações quanto ao período, ao alcance geográfico e às pessoas abrangidas, além da realização de avaliação de impacto sobre os direitos fundamentais.[3]O uso também está sujeito, em regra, à autorização prévia de autoridade judicial ou administrativa independente, ressalvadas as situações de urgência previstas no próprio regulamento. Embora o *AI Act* não seja diretamente aplicável ao Programa Muralha Paulista, sua utilização como parâmetro comparativo permite discutir mecanismos de governança, supervisão, avaliação de riscos e proteção de direitos fundamentais diante da expansão dessas tecnologias (União Europeia, 2024, considerando 26, art. 5º, § 1º, 'h', §§ 2º, 3º, 9º, 27, 49).

Diante desse contexto, a presente pesquisa tem como objetivo analisar os impactos jurídicos decorrentes da utilização de tecnologias de monitoramento, integração de dados e inteligência artificial no Programa Muralha Paulista, especialmente quanto à proteção de dados pessoais, à transparência, à governança da inteligência artificial e à preservação dos direitos fundamentais. Busca-se compreender de que maneira a implementação do programa

[2] A abordagem baseada em riscos adotada pelo Regulamento (UE) 2024/1689 estabelece diferentes níveis de exigência conforme os riscos que os sistemas de inteligência artificial podem representar à saúde, à segurança e aos direitos fundamentais. O considerando 26 explicita essa lógica, enquanto o art. 9º disciplina a gestão contínua dos riscos aplicável aos sistemas de inteligência artificial classificados como de alto risco.

[3] O art. 5º do Regulamento (UE) 2024/1689 estabelece hipóteses e condições específicas para a utilização de identificação biométrica remota em tempo real em espaços acessíveis ao público para fins de aplicação da lei, incluindo requisitos relacionados à necessidade e à proporcionalidade e outras salvaguardas previstas no próprio regulamento.

pode conciliar a utilização de novas tecnologias para o aprimoramento da segurança pública com as garantias estabelecidas pelo ordenamento jurídico brasileiro, considerando também a necessidade de ciência e participação da sociedade diante da expansão de mecanismos de vigilância em larga escala.

A hipótese que orienta o estudo parte da compreensão de que a utilização de tecnologias avançadas pode contribuir para a evolução das políticas públicas de segurança, especialmente ao possibilitar maior integração entre bases informacionais, otimização de recursos e ampliação da capacidade de atuação estatal. Entretanto, a adoção dessas ferramentas também apresenta desafios relacionados aos limites da vigilância tecnológica, ao tratamento de dados pessoais, à transparência dos sistemas e à participação social. Dessa forma, a legitimidade da utilização dessas tecnologias depende da existência de mecanismos efetivos de governança, transparência, supervisão humana e responsabilização, capazes de acompanhar sua implementação e reduzir possíveis riscos aos direitos fundamentais.

Para responder ao problema proposto, a pesquisa adota abordagem qualitativa, desenvolvida mediante revisão bibliográfica, pesquisa documental e estudo de caso. São analisados a legislação aplicável, documentos oficiais, dados públicos, estudos acadêmicos e informações relacionadas ao Programa Muralha Paulista e a iniciativas correlatas. Também são considerados parâmetros internacionais, especialmente o *AI Act* da União Europeia, como instrumento comparativo para a análise dos mecanismos de governança e controle da inteligência artificial.

O artigo está organizado em três eixos principais. Inicialmente, são examinadas as transformações tecnológicas na segurança pública, com destaque para a centralidade dos dados, a automação e a influência da lógica da Indústria 4.0 sobre a atuação estatal. Em seguida, analisa-se o Programa Muralha Paulista e iniciativas correlatas, especialmente o *Smart Sampa*, buscando compreender como essas tecnologias vêm sendo implementadas na prática e quais estruturas de integração e tratamento de dados são utilizadas. Por fim, são discutidos os principais desafios jurídicos decorrentes desse processo, com atenção à expansão da vigilância digital, à transparência e à explicabilidade dos sistemas, aos riscos de vieses e discriminação, à governança, à supervisão humana, à responsabilização, à participação social e à necessidade de avaliação dos impactos dessas tecnologias sobre os direitos fundamentais.

2. TRANSFORMAÇÃO TECNOLÓGICA E GESTÃO DE DADOS NA SEGURANÇA PÚBLICA

A incorporação de tecnologias digitais à atuação estatal tem modificado a forma da formulação e implementação de políticas públicas, especialmente no campo da segurança

pública. O desenvolvimento de sistemas capazes de coletar, armazenar e processar grandes volumes de informações permite a integração de diferentes fontes de dados e amplia a capacidade de atuação dos órgãos públicos. Nesse cenário, ferramentas como inteligência artificial, reconhecimento facial, leitura automática de placas, georreferenciamento e sistemas de monitoramento passam a integrar, de forma cada vez mais frequente, as estratégias de prevenção e enfrentamento da criminalidade.

Essa transformação está relacionada às mudanças associadas à chamada Indústria 4.0, caracterizada pela integração de tecnologias digitais, conectividade, automação e tratamento de grandes volumes de dados (Lima; Gomes, 2020). Nesse sentido, o conceito “Industrie 4.0” surgiu na Alemanha, no contexto de sua estratégia de inovação, e foi apresentado publicamente durante Hannover Messe, em 2011. Embora inicialmente relacionado às transformações dos processos industriais, seus efeitos ultrapassaram o setor produtivo e passaram a alcançar diferentes setores, inclusive a Administração Pública e a segurança pública, que também incorporaram tecnologias digitais, automação e ferramentas de tratamento de dados.

O Plano Nacional de Segurança Pública e Defesa Social 2021-2030, instituído pelo Decreto nº 10.822/2021, demonstra essa preocupação ao estabelecer ações estratégicas, metas e indicadores, além de prever mecanismos de implementação, monitoramento e avaliação das políticas de segurança (Brasil, 2021). A transformação tecnológica, portanto, não se limita à substituição de instrumentos tradicionais por ferramentas digitais; ela modifica a própria forma como o Estado produz, organiza e utiliza informações para a execução das políticas públicas de segurança.

A possibilidade de reunir dados de diversas fontes, integrá-los e analisá-los de forma conjunta permite identificar padrões e estabelecer relações entre informações que podem auxiliar o planejamento e a atuação dos agentes públicos nesse contexto. Diante desse processo, os dados deixam de desempenhar uma função apenas complementar e passam a ocupar posição estratégica na formulação, implementação e avaliação das políticas públicas, especialmente em áreas que dependem do processamento contínuo de informações, como a segurança pública.

2.1. Automação e reconfiguração do papel humano

A expansão das tecnologias digitais também produz mudanças na relação entre o trabalho humano e os processos automatizados. Sistemas digitais passaram a realizar atividades relacionadas à coleta, organização e análise inicial de informações, permitindo que determinadas tarefas sejam executadas com maior velocidade e em uma escala que dificilmente seria alcançada apenas pela atuação humana.

Na segurança pública, esses sistemas podem identificar possíveis correspondências, realizar cruzamentos de informações ou produzir alertas que posteriormente serão analisados pelos agentes públicos. Assim, a tecnologia amplia a capacidade de processamento de informações, mas não afasta a responsabilidade humana sobre as decisões decorrentes dos resultados produzidos.

A incorporação dessas tecnologias à segurança pública modifica, contudo, a relação entre informação, automação e atuação estatal. Sistemas capazes de coletar, integrar e processar dados em larga escala passam a auxiliar a identificação de ocorrências e a produção de alertas, tornando necessária a definição de mecanismos de supervisão e controle sobre os resultados produzidos.

O debate ganha relevância crítica quando os sistemas são utilizados para identificação de pessoas. Um resultado incorreto pode provocar uma abordagem, uma investigação ou outra intervenção estatal sobre alguém que não possui relação com determinado fato. Por essa razão, a participação humana na supervisão não deve ser compreendida como uma mera etapa formal de confirmação do resultado produzido pelo sistema de tecnologia, mas como possibilidade efetiva de análise, revisão e correção, assim evitando problemas posteriores. Essa exigência encontra respaldo no art. 14 do *AI Act,* que prevê mecanismos de supervisão humana capazes de permitir a interpretação dos resultados e a intervenção sobre sistemas de inteligência artificial de alto risco (União Europeia, 2024, art. 14).

Na prática, esse cenário pode ser observado nas experiências recentes de utilização de reconhecimento facial. Segundo os relatórios de transparência do *Smart Sampa*, os alertas produzidos pelo reconhecimento facial passam por análise humana antes do despacho da viatura, incluindo a conferência da compatibilidade facial, a consulta ao Banco Nacional de Mandados de Prisão e a verificação das imagens relacionadas à ocorrência (São Paulo, Município, 2025b). O dado é relevante para a presente pesquisa porque demonstra a existência de uma etapa de supervisão humana em uma política pública que utiliza tecnologia de reconhecimento facial. Entretanto, a existência desse procedimento não permite, isoladamente, concluir que o sistema seja suficiente ou adequado para afastar todos os riscos envolvidos. É necessário verificar, ao decorrer da análise, qual é a efetividade dessa supervisão, quais critérios são utilizados e se o agente público possui condições reais de questionar ou afastar o resultado produzido pela ferramenta tecnológica.

Para além dos relatórios oficiais, pesquisas científicas reforçam a dimensão desse desafio, mapeando vieses em sistemas de análise facial. Buolamwini e Gebru identificaram diferenças significativas de desempenho entre grupos de gênero e tonalidade de pele na avaliação de sistemas comerciais de classificação facial (Buolamwini; Gebru, 2018),

evidenciando que o desempenho dessas tecnologias pode variar conforme as características dos indivíduos analisados. Esses resultados reforçam a necessidade de considerar possíveis vieses e impactos desiguais na utilização dessas ferramentas, sem permitir, contudo, concluir que os sistemas empregados em São Paulo, por exemplo, pelo Muralha Paulista apresentam os mesmos resultados. O estudo demonstra, entretanto, que sistemas de análise facial não devem ser considerados neutros apenas em razão de seu elevado grau de sofisticação tecnológica.

A automação, portanto, modifica a atuação do agente público, mas não afasta a responsabilidade estatal. Quando um sistema tecnológico participa de uma cadeia de decisão capaz de produzir efeitos sobre direitos individuais, torna-se necessário identificar os critérios empregados, os mecanismos de supervisão existentes e as responsabilidades relacionadas à implementação e aos resultados da ferramenta.

2.2. Dados, políticas públicas e governança

A centralidade dos dados constitui outro aspecto fundamental desse desenvolvimento. A utilização de tecnologias digitais não envolve apenas a existência de equipamentos capazes de coletar informações, mas sim todo um processo de produção, armazenamento, integração, tratamento e utilização desses dados. Ou seja, quanto maior a capacidade de reunir informações provenientes de diferentes fontes, maior também é a possibilidade de estabelecer relações entre elas e produzir novos elementos para orientar a atuação estatal.

Na segurança pública, essa característica possui consequências relevantes, pois dados relacionados a pessoas, veículos, deslocamentos e ocorrências podem ser analisados em conjunto, permitindo que os órgãos públicos obtenham informações que não estariam disponíveis a partir da análise isolada de cada base. Dessa forma, a gestão de dados passa a constituir parte importante da própria estratégia de segurança.

Importante ressaltar que a contribuição de Marco Aurélio Barberato Genghini assume especial importância para esta pesquisa, uma vez que sua tese de doutorado, publicada em 2024, propôs uma análise crítica da utilização de novas tecnologias na polícia ostensiva brasileira, discutindo os efeitos da gestão massiva de dados e os limites jurídicos que devem acompanhar a incorporação dessas ferramentas à atividade estatal (Genghini, 2024). Sua análise parte justamente da tensão existente entre, de um lado, os ganhos de eficiência proporcionados pelas novas tecnologias e, de outro, os riscos de comprometimento da privacidade, da intimidade e dos dados pessoais. Sua análise permite deslocar a discussão de uma perspectiva exclusivamente tecnológica, considerando também quais dados são utilizados, quem pode acessá-los e quais mecanismos de controle acompanham sua utilização. Essa perspectiva é diretamente aplicável ao Programa Muralha Paulista, cuja

estrutura reúne diferentes soluções tecnológicas e fontes de informação voltadas à segurança pública, integrando câmeras municipais ao sistema estadual e permitindo o compartilhamento e o cruzamento de informações entre os órgãos de segurança.

Essa integração é relevante porque pode ampliar significativamente a capacidade de vigilância do Estado. Informações que, isoladamente, possuem alcance limitado podem adquirir novo significado quando relacionadas a outros dados. A preocupação, portanto, não está apenas no conteúdo de uma informação individual, mas também nas diversas possibilidades que podem ser criadas pelo seu cruzamento e tratamento.

A discussão desenvolvida por Przemyslaw Palka, incorporada ao referencial teórico de Genghini, chama atenção para os efeitos decorrentes da correlação de dados em larga escala, uma vez que informações aparentemente isoladas podem, quando combinadas com outros dados, permitir a construção de novas formas de conhecimento sobre as pessoas (Palka, 2020 apud Genghini, 2024, p. 24). Essa perspectiva permite compreender um aspecto relevante do Muralha Paulista: a integração de diferentes fontes de informação não amplia apenas a capacidade de armazenamento de dados, mas também as possibilidades de correlação e produção de informações utilizadas na atividade de segurança pública.

A mudança também interfere na própria compreensão das políticas públicas, porque a utilização de uma tecnologia não constitui uma decisão isolada, mas integra um processo que envolve formulação, implementação, acompanhamento e avaliação, além de aprimoramento constante. Nesse sentido, a contribuição de Maria Paula Dallari Bucci mostra-se relevante para a pesquisa, permitindo compreender a política pública a partir de sua dimensão jurídica e institucional (Bucci, 2013).

A governança assume, nesse contexto, papel fundamental, pois a existência de mecanismos de governança permite estabelecer responsabilidades, acompanhar o funcionamento dos sistemas, avaliar riscos e verificar se a utilização das tecnologias permanece compatível com as finalidades estabelecidas para a política pública. A participação social, por sua vez, não deve ser compreendida como oposição à modernização tecnológica da segurança pública, mas como mecanismo de legitimidade e controle. Quanto maior a capacidade de monitoramento proporcionada por uma política pública, maior a importância de mecanismos que permitam conhecer seus objetivos, acompanhar sua implementação e avaliar seus resultados. Da mesma forma, a modernização da segurança pública não pode ser avaliada apenas pela quantidade de equipamentos instalados ou pelo volume de informações processadas, sendo necessário verificar a existência de mecanismos de supervisão, transparência e responsabilização compatíveis com a dimensão do tratamento de dados realizado.

Essas questões ganham concretude no Programa Muralha Paulista, cuja estrutura reúne soluções tecnológicas de monitoramento e diferentes fontes de informação voltadas à segurança pública. A partir dessa estrutura, a análise do programa deve considerar não apenas sua expansão tecnológica, mas também os mecanismos de transparência, participação, governança e proteção de dados que acompanham sua implementação.

2.3. Programa Muralha Paulista: Implementação, expansão e desafios jurídicos

O Programa Muralha Paulista representa a aplicação concreta das transformações tecnológicas analisadas anteriormente na segurança pública paulista. Instituído pelo Decreto Estadual nº 68.828, de 4 de setembro de 2024, o programa tem como objetivos restringir a mobilidade criminal e aumentar a probabilidade de prisão de criminosos durante seus deslocamentos no território paulista. Para isso, o programa reúne soluções de infraestrutura física, operação em nuvem e inteligência artificial, além de prever a utilização dos dados produzidos para a localização de pessoas desaparecidas e a proteção dos dados pessoais (São Paulo, 2024).

Em termos técnicos, essa infraestrutura não se limita à utilização isolada de câmeras. O decreto prevê a integração de equipamentos de captura audiovisual, sistemas de georreferenciamento, bancos de dados e soluções de inteligência artificial, permitindo o processamento conjunto de informações provenientes de diferentes fontes. Além disso, também estabelece a utilização de inteligência artificial apoiada por curadoria humana e a definição de perfis de acesso conforme as atribuições dos usuários.

O alcance prático do programa, por sua vez, demonstra a escala dessa política pública. Em fevereiro de 2026, o Governo do Estado de São Paulo informou que o Muralha Paulista estava integrado a mais de 300 municípios e com a utilização de aproximadamente 94 mil câmeras. Os equipamentos incluíam cerca de 20 mil leitores automáticos de placas, 7 mil equipamentos de reconhecimento facial e 66 mil dispositivos de monitoramento em tempo real. A rede reúne equipamentos públicos e privados e permite o cruzamento de informações utilizadas pelas forças de segurança (São Paulo, 2026c).

Vale destacar que o crescimento dessa rede já estava previsto no Decreto Estadual nº 68.828/2024, que define como colaboradores do Muralha Paulista as pessoas físicas ou jurídicas que optem por conectar seus sensores de captação audiovisual ou de registro de dados à infraestrutura do programa (São Paulo, 2024). Com a atualização e ampliação da estrutura desse sistema, por conseguinte, a Secretaria da Segurança Pública informou, em setembro de 2025, o início do cadastramento de colaboradores, permitindo que câmeras instaladas em casas, prédios e empresas, quando voltadas para vias públicas, fossem integradas ao Muralha Paulista. Segundo a SSP, as imagens fornecidas passam a alimentar

um banco de dados coordenado pela Secretaria, podendo ser utilizadas no cruzamento de informações e em sistemas de inteligência artificial (São Paulo, 2025a). Essa ampliação demonstra que a expansão do programa não se limita ao aumento do número de câmeras públicas, mas também amplia as fontes de dados que podem ser integradas à sua estrutura.

A utilização dessa estrutura pode contribuir para finalidades legítimas de segurança pública, como a localização de pessoas desaparecidas, a identificação de veículos furtados ou roubados e a localização de indivíduos procurados. Entretanto, quanto maior a capacidade de reunir informações, maior também a necessidade de controlar sua utilização. Uma câmera instalada em espaço público, por exemplo, registra pessoas que não são necessariamente objeto de investigação e, quando essas imagens são posteriormente relacionadas a outras bases, podem produzir informações adicionais sobre indivíduos inicialmente alheios à ocorrência.

Essa questão é especialmente relevante no reconhecimento facial. Em face dessa realidade, os estudos desenvolvidos por Joy Buolamwini e Timnit Gebru demonstram que sistemas de análise facial podem apresentar diferenças de desempenho conforme características dos indivíduos analisados relacionadas ao gênero e a tonalidade da pele (Buolamwini; Gebru, 2018). Embora os resultados não permitam afirmar que o sistema utilizado pelo Muralha Paulista apresente as mesmas características, evidenciam a necessidade de avaliação e supervisão dessas tecnologias.

O reconhecimento facial permite observar concretamente essa cadeia. Em março de 2026, a Secretaria da Segurança Pública informou que o Programa Muralha Paulista havia sido utilizado em 100 jogos de futebol, com mais de 2 milhões de torcedores monitorados e 270 foragidos da Justiça capturados. Segundo a SSP, as imagens eram cruzadas automaticamente com o Banco Nacional de Mandados de Prisão; após a geração do alerta, as equipes policiais realizavam a abordagem e confirmavam a pendência judicial antes da prisão (São Paulo, 2026a).

O exemplo em epígrafe permite distinguir o resultado produzido pelo sistema automatizado da decisão estatal que efetivamente produz a intervenção. A geração do alerta, portanto, não corresponde, por si só, à confirmação da identidade ou à determinação da prisão, uma vez que a informação é submetida à verificação pelos agentes policiais.

Nesse aspecto, o *Smart Sampa* constitui referência comparativa e relevante no presente trabalho, uma vez que os seus relatórios de transparência descrevem a análise humana dos alertas produzidos pelo reconhecimento facial antes do encaminhamento da ocorrência, com conferência da compatibilidade facial e consulta a bases utilizadas para verificar a existência de mandados. Embora não seja possível afirmar que o Muralha Paulista

adote exatamente o mesmo procedimento, a experiência demonstra a importância de impedir que uma correspondência automatizada seja tratada, isoladamente, como confirmação definitiva da identidade de uma pessoa (São Paulo, Município, 2025b)

Assim, a previsão de utilização de inteligência artificial apoiada por curadoria humana no próprio Decreto nº 68.828/2024 constitui importante mecanismo de controle. Sua efetividade, entretanto, depende de que a supervisão permita efetivamente analisar, questionar e, quando necessário, afastar os resultados produzidos pelos sistemas automatizados (São Paulo, 2024).

2.4. Proteção de dados, transparência e participação social.

A dimensão do Muralha Paulista torna a proteção de dados pessoais inseparável da análise de sua legitimidade. A Emenda Constitucional nº 115, de 2022 reconheceu a proteção de dados pessoais, inclusive nos meios digitais, como direito fundamental (Brasil, 2022), enquanto a Lei Geral de Proteção de Dados Pessoais estabeleceu princípios e regras para o tratamento de informações pessoais (Brasil, 2018).

A LGPD, por sua vez, prevê tratamento específico para atividades relacionadas à segurança pública, defesa nacional, segurança do Estado e investigação e repressão de infrações penais, determinando a observância de legislação específica e de medidas proporcionais e estritamente necessárias (Brasil, 2018, art. 4º, III e § 1º).[4]

No caso do Muralha Paulista, essa preocupação é ampliada pela integração de milhares de equipamentos, fontes de informação e diferentes bases de dados. Como discutido anteriormente a partir de Palka e Genghini, a correlação entre informações pode produzir novos conhecimentos sobre indivíduos a partir de dados que, isoladamente, apresentariam significado limitado. O risco, portanto, não está apenas na informação coletada, mas também nas relações que podem ser estabelecidas entre diferentes informações.

A partir desse funcionamento, a proteção de dados deve ser analisada ao longo de todo o ciclo de tratamento da informação. Não basta verificar se a coleta possui finalidade legítima; também é necessário considerar quais bases podem ser relacionadas, quem pode acessar os dados, como os resultados são utilizados e quais mecanismos permitem revisar eventuais equívocos.

A transparência assume, nesse cenário, função essencial. A divulgação da quantidade de câmeras, municípios integrados e tecnologias utilizadas permite conhecer a dimensão do

[4] O art. 4º, III, da Lei nº 13.709/2018 (LGPD) estabelece um regime de tratamento específico para essas atividades. Paralelamente, o § 1º do mesmo dispositivo determina que o processamento desses dados deve observar legislação específica, adotando medidas proporcionais e estritamente necessárias ao atendimento do interesse público, com estrita observância ao devido processo legal.

programa, mas não responde, por si só, a questões relacionadas aos critérios de acesso, auditoria, tratamento das informações e funcionamento dos sistemas.

Essa preocupação tornou-se ainda mais relevante com o acompanhamento da implementação do programa em 2026. Requerimento de Informação apresentado na Assembleia Legislativa do Estado de São Paulo solicitou esclarecimentos sobre a existência de consulta pública e participação de especialistas e universidades na formulação do programa, bem como informações sobre auditorias dos algoritmos e a metodologia utilizada para atribuir resultados ao Muralha Paulista. O documento, por si só, não permite concluir pela inexistência desses mecanismos, mas demonstra que transparência, participação e avaliação dos sistemas passaram a constituir questões concretas de controle institucional (São Paulo, 2026b)

A relevância da proteção de dados também se evidencia pela atuação da Autoridade Nacional de Proteção de Dados (ANPD), que mantém procedimento de fiscalização específico sobre o tratamento de dados pessoais no contexto da execução do Programa Muralha Paulista, registrado sob o Processo nº 00261.000264/2025-59 (ANPD, 2026). A existência do procedimento demonstra que o tratamento de dados realizado pelo programa já integra a esfera institucional de fiscalização da proteção de dados pessoais.

Esse aspecto é diretamente relacionado ao problema desta pesquisa, porque a participação social não deve ser compreendida como obstáculo à utilização da tecnologia, mas como instrumento de legitimidade e fiscalização da atuação estatal. Quanto maior a capacidade de vigilância e tratamento de informações, maior também a necessidade de que a sociedade disponha de informações suficientes para acompanhar seus efeitos.

O *AI Act* da União Europeia oferece, nesse ponto, um parâmetro comparativo relevante. O regulamento adota uma abordagem baseada em riscos e estabelece requisitos específicos para determinadas aplicações de inteligência artificial, incluindo hipóteses relacionadas à identificação biométrica remota para fins de aplicação da lei (União Europeia, 2024). Embora não seja diretamente aplicável ao Muralha Paulista, o modelo demonstra a possibilidade de vincular o uso de tecnologias sensíveis a mecanismos de avaliação, supervisão e proteção dos direitos fundamentais.

No caso do Muralha Paulista, existem mecanismos relevantes no próprio texto normativo, como a delimitação das finalidades, o controle de acesso, a curadoria humana e a previsão de mecanismos de auditoria e governança de dados. Além das previsões do Decreto nº 68.828/2024, a governança do Muralha Paulista foi regulamentada pela Resolução SSP nº 11/2025, que instituiu Comissão de Governança e estabeleceu atribuições relacionadas ao controle dos acessos e à gestão de dados. Embora esses mecanismos representem

instrumentos formais de governança, sua efetividade deve ser avaliada diante da escala e da natureza das informações tratadas. A expansão do programa demonstra, assim, a necessidade de que essas garantias sejam acompanhadas de transparência, fiscalização, avaliação contínua e participação social (São Paulo, 2024, arts. 5º, 6º, § 2º, art. 10, III, art. 11, II-VIII; São Paulo, 2025b).

Dessa forma, a utilização de tecnologia massiva pode ser compatível com a segurança pública e com o ordenamento jurídico brasileiro, desde que a ampliação da capacidade tecnológica do Estado seja acompanhada pelo fortalecimento de sua capacidade de controle.

3. CONSIDERAÇÕES FINAIS

A presente pesquisa analisou os desafios jurídicos decorrentes da utilização de tecnologias de monitoramento, inteligência artificial e tratamento massivo de dados no Programa Muralha Paulista, especialmente em relação à privacidade, à proteção de dados pessoais, à transparência, à governança e à preservação dos direitos fundamentais.

Nessa problemática, a análise demonstrou que a transformação tecnológica ampliou significativamente a capacidade estatal de produzir, integrar e utilizar informações. O Programa Muralha Paulista representa concretamente esse processo em 2026, o programa alcançou mais de 300 municípios e aproximadamente 94 mil câmeras, reunindo reconhecimento facial, leitura automática de placas, monitoramento em tempo real e integração de equipamentos públicos e privados.

Entretanto, a pesquisa evidenciou que eficiência não se confunde com legitimidade. A mesma estrutura que amplia a capacidade de atuação estatal também aumenta os riscos relacionados à coleta, integração e utilização de informações sobre pessoas que nem sempre são objeto direto de investigação. Por essa razão, a análise do Muralha Paulista não pode se limitar aos resultados operacionais alcançados pelo programa, devendo considerar também as garantias que acompanham o tratamento dessas informações.

Assim, retomando o problema proposto na pesquisa: de que forma o Programa Muralha Paulista pode empregar tecnologia massiva sem comprometer a ciência e a participação da sociedade civil e sem ofender os direitos fundamentais, especialmente no que tange à privacidade e à proteção de dados pessoais? Conclui-se, portanto, que a utilização dessas tecnologias é juridicamente possível, mas não deve ocorrer de forma dissociada de mecanismos efetivos de controle.

Esses mecanismos envolvem a delimitação das finalidades do tratamento, o controle de acesso, a supervisão humana, a transparência, a governança, a responsabilização e a participação social. No caso do reconhecimento facial, a supervisão humana é especialmente

relevante para impedir que resultados automatizados sejam considerados conclusivos sem a devida verificação.

Na presente pesquisa, também ficou evidenciado que a participação social possui uma importância fundamental para a legitimidade da política pública. O Requerimento de Informação nº 150, de 2026, apresentado na Assembleia Legislativa do Estado de São Paulo, ao solicitar esclarecimentos sobre consulta pública, participação de especialistas e universidades, auditoria de algoritmos e metodologia de avaliação do programa, demonstra que questões relacionadas à transparência e ao controle institucional acompanham a expansão tecnológica do Muralha Paulista (São Paulo, 2026b). O documento, contudo, não permite concluir pela inexistência desses mecanismos, mas evidencia a relevância de sua discussão e acompanhamento.

Assim, os resultados da pesquisa corroboram a hipótese apresentada no início do estudo: a utilização de tecnologias avançadas pode contribuir para o aprimoramento da segurança pública, desde que sua implementação seja acompanhada de garantias jurídicas e institucionais capazes de preservar os direitos fundamentais. A tecnologia, portanto, não constitui, por si só, ameaça ou solução para a segurança pública; seus efeitos dependem da forma como é incorporada, regulada, supervisionada e controlada pelo Estado.

O desafio do Muralha Paulista, portanto, não consiste em escolher entre tecnologia e direitos fundamentais. Consiste em desenvolver uma política de segurança capaz de utilizar os benefícios da inovação sem transformar a eficiência tecnológica em justificativa para a redução das garantias constitucionais.

Conclui-se, assim, que a modernização da segurança pública é compatível com o Estado Democrático de Direito quando acompanhada de transparência, governança, supervisão humana, participação social e proteção efetiva dos dados pessoais. Quanto maior for a capacidade tecnológica de vigilância do Estado, maior deve ser também sua responsabilidade na proteção dos indivíduos alcançados pela tecnologia.

4. REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Saiba como fiscalizamos. Brasília, DF, 2026. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao/saiba-como_fiscalizamos. Acesso em: 22 ago. 2026.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 6 maio. 2025.

BRASIL. **Decreto nº 10.822, de 28 de setembro de 2021.** Institui o Plano Nacional de Segurança Pública e Defesa Social 2021-2030. Brasília, DF, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10822.htm. Acesso em 21 mar. 2025

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Brasília, DF, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 6 maio. 2025.

BRASIL. **Lei nº 13.675, de 11 de junho de 2018**. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, cria a Política Nacional de Segurança Pública e Defesa Social e institui o Sistema Único de Segurança Pública. Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13675.htm. Acesso em: 16 ago. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 21 mar. 2025

BUCCI, Maria Paula Dallari. **Fundamentos para uma teoria jurídica das políticas públicas**. São Paulo: Saraiva, 2013.

BUOLAMWINI, Joy; GEBRU, Timnit. **Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.** Proceedings of Machine Learning Research, v. 81, p. 77-91, 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a.html. Acesso em: 21 maio. 2026

GENGHINI, Marco Aurélio Barberato. **Direito de gestão de dados e a polícia ostensiva brasileira: fundamentos jurídicos para formulação de políticas fundadas em novas**

tecnologias. 2024. Tese (Doutorado em Direito Político e Econômico) – Universidade Presbiteriana Mackenzie, São Paulo, 2024.

LIMA, Faíque Ribeiro; GOMES, Rogério. **Conceitos e tecnologias da Indústria 4.0: uma análise bibliométrica.** Revista Brasileira de Inovação, Campinas, v. 19, p. e0200023, 2020. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rbi/article/view/8658766. Acesso em: 20 ago. 2026.

SÃO PAULO (Estado). Agência SP. **Muralha Paulista: Polícia prende 270 foragidos em estádios de SP**. São Paulo, 2 mar. 2026a. Disponível em: https://www.bibliotecajuridica.sp.gov.br/muralha-paulista-policia-prende-270-foragidos-em-estadios-de-sp/ Acesso em: 20 ago. 2026.

SÃO PAULO (Estado). Assembleia Legislativa. **Requerimento de Informação nº 150, de 2026. Requer informações ao Secretário da Segurança Pública sobre o Programa Muralha Paulista**. São Paulo, 2026b. Disponível em: https://www.al.sp.gov.br/propositura/?id=1000687024. Acesso em: 20 maio. 2026.

SÃO PAULO (Estado). **Decreto nº 68.828, de 4 de setembro de 2024**. Institui o Programa Muralha Paulista e dá providências correlatas. São Paulo, 2024. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2024/decreto-68828-04.09.2024.html. Acesso em: 20 mar. 2025.

SÃO PAULO (Estado). **Muralha Paulista inicia nova fase de cadastro de câmeras de pessoas físicas e jurídicas em todo o estado.** São Paulo, 9 set. 2025a. Disponível em: https://www.agenciasp.sp.gov.br/muralha-paulista-inicia-nova-fase-de-cadastro-de-cameras-de-pessoas-fisicas-e-juridicas-em-todo-o-estado/. Acesso em: 22 ago. 2026.

SÃO PAULO (Estado). Muralha Paulista: saiba como integrar a sua câmera no maior sistema de segurança do país. *Governo do Estado de São Paulo*, São Paulo, 5 fev. 2026c. Disponível em: https://www.sp.gov.br/wcm/connect/saopaulo_content/saopaulo/canais+de+comunicacao/noticias/muralha+paulista+saiba+como+integrar+a+sua+camera+no+maior+sistema+de+seguranca+do+pais. Acesso em: 22 jul. 2026.

SÃO PAULO (Estado). **Programa Muralha Paulista.** ***Produtos do Muralha Paulista***. São Paulo. Disponível em: https://www.muralhapaulista.sp.gov.br/servicos/produtos-muralha-paulista. Acesso em: 20 ago. 2026.

SÃO PAULO (Estado). **Secretaria da Segurança Pública. Resolução SSP nº 11, de 6 de março de 2025.** São Paulo, 2025b. Disponível em: https://www.doe.sp.gov.br/executivo/secretaria-da-seguranca-publica/resolucao-n-ssp-11-de-6-de-marco-de-2025-20250306113712209278 22. Acesso em: 22 ago. 2026.

SÃO PAULO (Município). Secretaria Municipal de Segurança Urbana. **Relatório de Transparência – Programa *Smart Sampa***. São Paulo: Prefeitura Municipal de São Paulo, 2025a. Disponível em: Relatório de Transparência Smart Sampa - Secretaria Municipal de Segurança Urbana - Prefeitura. Acesso em: 22 maio. 2026.

SÃO PAULO (Município). Secretaria Municipal de Segurança Urbana. **Segundo Relatório de Transparência – Programa *Smart Sampa***: período de análise de 22 de maio de 2025 a 22 de novembro de 2025. São Paulo: Prefeitura Municipal de São Paulo, 2025b. Disponível em: Relatório de Transparência Smart Sampa - Secretaria Municipal de Segurança Urbana - Prefeitura. Acesso em: 22. maio. 2026.

UNIÃO EUROPEIA. **Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act).** *Official Journal of the European Union*, 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj. Acesso em: 22 jul. 2026.

Contatos: fernandasoarez13@gmail.com e marcoaurelio.genghini@mackenzie.com.br

APÊNDICE A: DECLARAÇÃO DE USO DE INTELIGÊNCIA ARTIFICIAL

Durante a elaboração deste artigo, foram utilizadas as ferramentas de inteligência artificial generativa ChatGPT e Google Gemini como instrumentos auxiliares de pesquisa e redação acadêmica. Seu uso esteve concentrado na revisão linguística, organização das ideias, aprimoramento da clareza e coerência textual, identificação de repetições, estruturação dos argumentos e adequação às normas acadêmicas e da ABNT, bem como no apoio à identificação de pontos que demandavam maior fundamentação ou verificação.

As ferramentas foram utilizadas de forma supervisionada e não substituíram a pesquisa bibliográfica e documental, a consulta às fontes originais, a análise jurídica ou a formulação das conclusões. As fontes encaminhadas pela autora foram analisadas e, quando pertinente, as ferramentas também auxiliaram na identificação ou indicação de fontes complementares, cuja pertinência e conteúdo foram posteriormente conferidos pela autora. A seleção final das fontes, a incorporação das sugestões e a redação do trabalho permaneceram sob responsabilidade da autora.

Orientação geral utilizada nas interações com as ferramentas:

> *“Atue como assistente de pesquisa, auxiliando na revisão e no aprimoramento deste artigo jurídico, preservando seu sentido e autoria. Analise clareza, coerência, estrutura argumentativa, linguagem acadêmica, referências e adequação às normas da ABNT. Identifique repetições, inconsistências e pontos que necessitem de fundamentação ou verificação. Não invente informações, fontes, referências ou dados. Quando houver necessidade de confirmação, indique a consulta à fonte original. As sugestões apresentadas serão analisadas e validadas pela autora antes de sua utilização.”*