SMART SAMPA: ENTRE A EFICIÊNCIA E A ÉTICA – ANÁLISE CRÍTICA DO USO DE IA NA SEGURANÇA PÚBLICA DE SÃO PAULO

SMART SAMPA: BETWEEN EFFICIENCY AND ETHICS – A CRITICAL ANALYSIS OF AI USE IN SÃO PAULO'S PUBLIC SECURITY

SMART SAMPA: ENTRE A EFICIÊNCIA E A ÉTICA – ANÁLISE CRÍTICA DO USO DE IA NA SEGURANÇA PÚBLICA DE SÃO PAULO

SMART SAMPA: BETWEEN EFFICIENCY AND ETHICS – A CRITICAL ANALYSIS OF AI USE IN SÃO PAULO'S PUBLIC SECURITY

Liciane Coutinho de Paula[1]
liciane.coutinho.paula@gmail.com

RESUMO
O Programa Smart Sampa, lançado pela Prefeitura de São Paulo em 2023, representa um avanço significativo na modernização da segurança pública por meio da integração de tecnologias inovadoras. Este artigo analisa a implementação do projeto, destacando suas aplicações práticas, como o uso de reconhecimento facial para localizar pessoas desaparecidas e foragidos, a integração de bancos de dados entre diversos órgãos públicos e o potencial de replicação em outras cidades. O estudo tem como objetivo avaliar os impactos do Smart Sampa na eficiência da segurança pública, bem como discutir os desafios relacionados à privacidade e à ética no uso de dados. A metodologia adotada inclui revisão bibliográfica, análise de dados públicos e estudos de caso. Os resultados demonstram que o programa já contribuiu para a captura de foragidos, a identificação de crimes em flagrante e a localização de desaparecidos, além de facilitar a integração entre instituições. Conclui-se que o *Smart Sampa* é uma iniciativa promissora para aprimorar a segurança pública, desde que seja acompanhada de regulamentações robustas que garantam a proteção de dados e a transparência no uso das tecnologias. Recomenda-se a realização de estudos adicionais sobre os impactos sociais e éticos do programa, bem como a expansão de suas funcionalidades para outras áreas, como o monitoramento de violência doméstica.

Palavras-chave: Smart Sampa; Inteligência Artificial; Segurança Pública; Reconhecimento Facial.

ABSTRACT
The Smart Sampa Program, launched by the City of São Paulo in 2023, represents a significant advancement in the modernization of public security through the integration of innovative technologies. This article examines the implementation of the project, highlighting its practical applications, such as the use of facial recognition to locate missing persons and fugitives, the integration of databases among various public agencies, and the potential for replication in other cities. The study aims to evaluate the impacts of Smart Sampa on the efficiency of public security, as well as to discuss the challenges related to privacy and ethics in data usage. The methodology adopted includes a literature review, analysis of public data, and case studies. The results demonstrate that the program has already contributed to the capture of fugitives, the identification of crimes in progress, and the location of missing persons, in addition to facilitating integration among institutions. It is concluded that Smart Sampa is a promising initiative to enhance public security, provided it is accompanied by robust regulations that ensure data protection and transparency in the use of technologies. Further studies on the social and ethical impacts of the program are recommended, as well as the expansion of its functionalities to other areas, such as monitoring domestic violence.

Keywords**:** Smart Sampa; Artificial Intelligence; Public Security; Facial Recognition.

[1]Especialista em Gestão Pública na Educação Profissional e Tecnológica pelo Instituto Federal de Santa Catarina. Pesquisadora nas áreas de segurança pública, educação e literatura. E-mail: **liciane.coutinho.paula@gmail.com**. Currículo Lattes: http://lattes.cnpq.br/7127178754920471. ORCID: https://orcid.org/0009-0006-4878-6227.

1 INTRODUÇÃO

A adoção de Inteligência Artificial (IA) na segurança pública tem gerado debates globais entre eficiência policial e garantias fundamentais. Na era da transformação digital, novas tecnologias têm se mostrado fundamentais para a evolução da segurança pública. Como destacam Vieira *et al.* (2024), a IA tem potencial transformador nas operações policiais, desde que implementada com responsabilidade ética. No Brasil, o Programa *Smart Sampa* (Prefeitura de São Paulo, 2023) emerge como estudo de caso emblemático, ao integrar reconhecimento facial, análise preditiva e interoperabilidade de bancos de dados. O programa em sua essência, busca modernizar a segurança pública através da tecnologia. Desenvolvido a partir do *City* Câmera — programa pioneiro idealizado em 2017 pelo Cel. José Roberto Rodrigues de Oliveira, então secretário municipal de Segurança Urbana de São Paulo (Zucherato, 2018) —, o *Smart Sampa* surge como uma evolução tecnológica para aprimorar a resposta a situações de risco, localizar desaparecidos e integrar as forças de segurança. O *City* Câmera estabeleceu as bases para a interoperabilidade de câmeras públicas e privadas, modelo que o *Smart Sampa* expande com IA e reconhecimento facial.

Os números apresentados no artigo são de:

a) a redução no tempo de localização de desaparecidos;

b) o aumento na resolução de crimes contra o patrimônio;

c) a integração de bancos de dados.

Os resultados são sem dúvida, animadores, eles demonstram que, sim, a tecnologia tem o poder de transformar a realidade da segurança urbana. No entanto, a tecnologia, por mais brilhante que seja, é uma ferramenta. Uma ferramenta poderosa que precisa ser empunhada com sabedoria, ética e, acima de tudo, um profundo respeito pelos direitos e pela dignidade humana.

Este estudo busca analisar seus benefícios, desafios e implicações no contexto do *Smart Sampa*, ecoando a necessidade de equilíbrio entre inovação e direitos fundamentais. Neste foco, mesmo com a promessa de seguir princípios éticos, ainda existem muitos desafios relacionados à proteção dos direitos dos cidadãos. Contudo, ainda persistem na literatura a escassez e quase a total inexistência dos reais impactos operacionais dessas tecnologias em cidades latino-americanas, e sobre como os mecanismos de governança para mitigar riscos éticos.

Este artigo busca respostas para tais ausencias, analisando criticamente os primeiros 18 meses de implementação do Smart Sampa, com base em dados oficiais, revisão normativa e *benchmarking* internacional. Além disso, propõe um *framework* para equilibrar inovação e proteção de direitos, tema urgente frente à expansão de cidades inteligentes no país. Também busca explorar a crescente relevância dessas inovações, analisando como suas capacidades estão transformando as práticas na área de segurança pública.

O objetivo central é esclarecer o papel que essas ferramentas desempenham na melhoria da segurança pública e sua contribuição para a eficácia das operações, com foco no Programa *Smart Sampa*. Um dos principais pontos é a proteção dos dados pessoais. O programa afirma cumprir a Lei Federal nº 13.709/14/8/2018 (Lei Geral de Proteção de Dados-LGPD) (Brasil, 2024), adotando medidas como anonimização das informações e controle de acesso. Além disso, sugere-se a incorporação de avaliações periódicas de impacto à proteção de dados (conforme Art. 20 da LGPD), assegurando que o programa não apenas cumpra a legislação vigente, mas também previna riscos a direitos fundamentais como privacidade e autonomia dos indivíduos.

Apesar disso, ainda não há garantias suficientes de que os sistemas usados evitarão discriminações, especialmente as chamadas "discriminações algorítmicas", que ocorrem quando a tecnologia trata pessoas de forma desigual com base em padrões injustos. Pinheiro (2024) argumenta que o Estado deve garantir que o avanço tecnológico esteja a serviço da justiça social, não da restrição de direitos.

Nesse sentido, a Inteligência Artificial (IA) vem sendo cada vez mais aplicada em diversos setores da sociedade, incluindo a segurança pública. Outro aspecto importante é a transparência. Um decreto criou o Conselho de Gestão e Transparência e uma Ouvidoria para fiscalizar o uso dos dados e garantir que o governo preste contas à população. Entretanto, a maior parte das decisões continua sendo tomada apenas pela Secretaria de Segurança Urbana, o que dificulta a efetiva participação da sociedade civil. Este estudo busca analisar seus benefícios, desafios e possíveis implicações, temas amplamente debatidos por Nagata (2024).

Especialistas também chamam a atenção para os riscos de preconceito nos sistemas de inteligência artificial, como no caso do reconhecimento facial, que pode errar mais com determinados grupos sociais, como pessoas negras ou moradores da periferia. Apesar dessas preocupações, o programa ainda não detalha como pretende combater esses problemas. Some-se ainda um receio crescente de que a cidade esteja se aproximando de um cenário de vigilância constante, o que pode prejudicar a liberdade e a privacidade das pessoas no espaço urbano.

Ao implementar câmeras inteligentes e reconhecimento facial em espaços públicos, evoca a profética imagem do 'Grande Irmão' de George Orwell, que 'está de olho em você' (Orwell, 2009, p. 12). Embora a justificativa seja a segurança, redução de crimes e resposta ágil a emergências, a vigilância ubíqua suscita questionamentos éticos: até que ponto a tecnologia reforça a proteção social e quando ela começa a minar liberdades individuais? Em 1984, a vigilância era ferramenta de opressão estatal; no contexto paulistano, o desafio é garantir que a transparência e a LGPD atuem como antídotos contra a distorção orwelliana, impedindo que dados se tornem mecanismos de controle arbitrário. Afinal, como alerta Orwell, o verdadeiro objetivo da vigilância não é apenas ver, mas definir

o que é visto e, no caso das cidades inteligentes, quem define essa narrativa?

Para evitar esse risco, seria necessário criar regras mais específicas e realizar auditorias independentes, como recomendação é a criação de um canal específico para demandas relacionadas à proteção de dados, distinto da ouvidoria geral, conforme boas práticas de governança. Essa medida ampliaria a transparência e a eficiência no atendimento a direitos previstos na LGPD, como acesso e exclusão de dados pessoais.

Em resumo, o *Smart Sampa* tem um potencial imenso para transformar a segurança pública de São Paulo sendo implementado com a devida cautela, com regulamentações robustas, mecanismos de fiscalização independentes e fundamentalmente um compromisso inabalável com a ética e a privacidade, ele será um legado para a cidade. Caso contrário, haverá riscos de que uma ferramenta tão promissora se torne um instrumento de preocupação, comprometendo a confiança entre o Estado e seus cidadãos.

2 BREVE HISTÓRICO DO PROGRAMA

No dia 7 de agosto de 2023, a Prefeitura de São Paulo formalizou o contrato que deu início ao Programa *Smart Sampa*, desenvolvido a partir de um edital público. A licitação foi vencida pelo consórcio *SMART CITY SP*, responsável por implementar o projeto do qual é uma iniciativa da administração municipal voltada para fortalecer a segurança na cidade, com o objetivo de agilizar a resposta a situações de risco e garantir maior proteção aos cidadãos. Para isso, o programa promove a integração entre diferentes órgãos, como o SAMU, o Corpo de Bombeiros e a Secretaria Municipal de Direitos Humanos e Cidadania (SMDHC), que disponibilizou seu banco de dados de pessoas desaparecidas. Essa integração tem sido fundamental para o sucesso de diversas operações, permitindo a localização de desaparecidos por meio de tecnologias de reconhecimento facial.

Além disso, em 5 de setembro de 2023, a Secretaria de Segurança Pública do Estado (SSP) firmou parceria com o programa, integrando seu banco de dados de foragidos da justiça. Essa colaboração já resultou em casos bem-sucedidos de localização de indivíduos procurados. A metodologia deste estudo utiliza uma abordagem mista que inclui revisão bibliográfica, análise de dados públicos combinado com análise documental do Decreto Municipal nº 63.552/4/7/2024 (Prefeitura Municipal de São Paulo, 2024) que institui o *Smart Sampa*, avaliação de conformidade com a LGPD (Lei nº 13.709/2018) e relatórios do Prisômetro (2023-2025), com o intuito de avaliar os impactos do *Smart Sampa* na segurança pública e discutir os desafios relacionados à privacidade e à ética no uso de dados.

Conforme Ambrosio e Barbosa (2024), a adoção de IA na segurança pública brasileira tem priorizado a eficiência operacional em detrimento de garantias fundamentais, como a privacidade e a não discriminação – um risco que também permeia iniciativas como o *Smart Sampa*. A Unesco em Recomendação sobre os princípios éticos da IA menciona:

> A inviolável e inerente dignidade de cada ser humano constitui a base para o sistema de direitos humanos e liberdades fundamentais [...] Nenhum ser humano ou comunidade humana deve ser prejudicado ou subordinado, seja em termos físicos, econômicos, sociais, políticos, culturais ou mentais durante qualquer fase do ciclo de vida dos sistemas de IA" (UNESCO, 2022, p. 19).

E ainda estabelece que a governança da IA deve assegurar a primazia da dignidade humana, proibindo o uso de sistemas que perpetuem discriminações ou violem direitos fundamentais em qualquer etapa de seu ciclo de vida, conforme prescreve a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO, 2022)

A Inteligência Artificial (IA) tem se consolidado como uma ferramenta transformadora em diversos setores, desde a produção industrial até a gestão pública. No contexto das cidades inteligentes (*smart cities*), a IA tem sido utilizada para otimizar serviços urbanos, melhorar a eficiência administrativa e aumentar a segurança pública. A IA pode fortalecer a prevenção e o combate ao crime, melhorar a resposta a emergências e crises, e incluir tecnologias como reconhecimento facial e análise preditiva de crimes (Nagata, 2024, p. 1). Nesse sentido o programa é um exemplo emblemático dessa tendência, integrando tecnologias avançadas para modernizar a gestão urbana e a segurança na maior cidade da América Latina.

A implantação do *Smart Sampa* passou por um processo complexo e polêmico, marcado por debates sobre ética, privacidade e possíveis vieses tecnológicos. A primeira versão do edital, publicada em novembro de 2022, previa a utilização de tecnologias de reconhecimento facial baseadas em características como cor, face e comportamento, incluindo a identificação de situações como "vadiagem" e "tempo de permanência" em locais públicos. No entanto, o projeto foi alvo de críticas de entidades como o IDEC (Instituto Brasileiro de Defesa ao Consumidor) e outras 50 organizações, que alertaram para riscos de discriminação e violação de direitos individuais. Diante das controvérsias, a Prefeitura de São Paulo decidiu suspender o pregão em dezembro de 2022, com o objetivo de revisar o edital e esclarecer dúvidas sobre a gestão do programa.

Após quatro meses de suspensão, em abril de 2023, o edital foi parcialmente modificado e recebeu aval do Tribunal de Contas do Município (TCM) para retomar o processo de licitação. No entanto, em 18 de maio, o pregão foi novamente suspenso por uma liminar do juiz Luis Manuel Fonseca Pires, que apontou possíveis violações à Lei Geral de Proteção de Dados (LGPD) e riscos de reforço ao racismo estrutural. A decisão destacou a preocupação de especialistas com os impactos sociais e éticos do uso de tecnologias de reconhecimento facial.

Poucos dias depois, em 23 de maio, a Prefeitura de São Paulo e a Secretaria de Segurança Urbana conseguiram reverter a suspensão por meio de uma liminar da desembargadora Paola Lorena, do Tribunal de Justiça de São Paulo (TJSP). A decisão argumentou que não havia evidências concretas de que o videomonitoramento reforçaria a discriminação social e racial, destacando a necessidade de análises imparciais sobre o tema. Finalmente, em 29 de maio, o pregão eletrônico foi realizado com a participação de 12 empresas, e a proposta vencedora foi de R$ 9,2 milhões por mês, segundo a Agência Escola de Comunicação Pública e Jornalismo da Pontifica Universidade Católica de São Paulo da PUC-SP (AGEMT, 2023).

Os números oficiais demonstram impactos concretos na segurança paulistana. Segundo o Prisômetro do programa (Smart Sampa, 2025), até maio de 2025 foram registrados 1.146 foragidos capturados mediante cruzamento de bancos de dados, 828 prisões somente no ano de 2025, 69 detenções no mês de maio/2025 e contou também com 61 desaparecidos localizados por reconhecimento facial, totalizando 2.344 flagrantes facilitados pelo monitoramento inteligente.

O *Smart Sampa* foi concebido como parte de uma estratégia mais ampla para transformar São Paulo em uma cidade inteligente, alinhada às iniciativas globais de uso de IA na administração pública. Conforme destacado pela Estratégia Brasileira de Inteligência Artificial (EBIA), o governo tem um papel fundamental na facilitação da adoção de tecnologias de IA promovendo a abertura de dados, o estabelecimento de s*andboxes* regulatórios e o incentivo a startups de base tecnológica (Brasil, 2021). O programa reflete essa visão, ao integrar sistemas de reconhecimento facial, análise de dados em tempo real e monitoramento urbano para aprimorar a segurança pública.

O objetivo principal do *Smart Sampa* é agilizar a resposta a situações de risco, garantindo maior proteção aos cidadãos. Para isso, o programa promove a integração entre diversos órgãos públicos, como a Secretaria Municipal de Direitos Humanos e Cidadania (SMDHC), a Secretaria de Segurança Pública (SSP), o SAMU e o Corpo de Bombeiros. Essa colaboração tem sido fundamental para o sucesso de operações, como a localização de desaparecidos e a captura de foragidos, utilizando tecnologias de reconhecimento facial e análise de bancos de dados.

Além disso, o *Smart Sampa* se inspira em experiências internacionais de cidades inteligentes, como Barcelona, Singapura e Nova York, que utilizam tecnologias de IA para melhorar a gestão urbana e a segurança. No entanto, o programa foi adaptado ao contexto específico de São Paulo, considerando suas demandas e desafios únicos.

3 TECNOLOGIAS DO *SMART SAMPA*

O *Smart Sampa* implementa uma arquitetura tecnológica baseada em três pilares interconectados: (1) sistemas de processamento de imagens com algoritmos de *deep learning* para

detecção automatizada de atividades suspeitas (invasões, vandalismo e furtos); (2) plataformas de reconhecimento facial biométrico integradas aos bancos de dados da Secretaria de Segurança Pública e do Ministério Público; e (3) uma rede de câmeras inteligentes com capacidade de análise comportamental em tempo real. Essa estrutura opera sob um modelo de vigilância preditiva similar ao adotado pelo Centro de Operações Rio (COR), porém com aprimoramentos na interoperabilidade entre órgãos - característica que se tornou um diferencial na gestão de megacidades latino-americanas.

Nesse contexto, o Programa *Smart Sampa* surge como uma iniciativa pioneira, utilizando tecnologias de ponta para modernizar a gestão da segurança e melhorar a qualidade de vida dos cidadãos. Assim como destacado por Nagata (2024), o uso de IA para análise de dados criminais em tempo real — presente no *Smart Sampa* — demonstra eficácia na redução de índices de criminalidade, corroborando a importância de investimentos em soluções tecnológicas para segurança urbana.

O *Smart Sampa* utiliza tecnologias de ponta para agilizar e otimizar o atendimento a ocorrências na cidade. Seus algoritmos inteligentes emitem alertas em casos de invasões, vandalismo e furtos, além de detectar veículos com placas roubadas, através dessa tecnologias de ponta, como algoritmos de IA para emissão de alertas em tempo real, essa abordagem alinha-se às experiências das Polícias Militares brasileiras, onde, segundo Vieira *et al.* (2024, p.6), ferramentas como "como câmeras de vigilância e sensores, conectados a sistemas de IA, melhoram significativamente a vigilância e o monitoramento de áreas públicas e privadas". O sistema também conta com reconhecimento facial, auxiliando na localização de desaparecidos e foragidos da justiça (Prefeitura de São Paulo, 2025). O programa inova em gestão integrada, alinhando-se à necessidade destacada por Marino (2018, p. 13) de que "a integração dos órgãos de segurança pública é imprescindível para o cenário atual, a fim de somar forças para alcançar o objetivo comum, que é o combate eficaz contra a criminalidade".

Ao analisarmos outras cidades brasileiras, encontramos sistemas de reconhecimento facial e IA em operação, como no caso do Rio de Janeiro, que implantou o Centro de Operações Rio (COR). Desenvolvido em parceria com a Hikvision, o COR utiliza câmeras com reconhecimento facial em larga escala — antes mesmo de São Paulo —, especialmente em áreas turísticas como Copacabana, permitindo monitoramento em tempo real.

O COR é um marco na segurança pública brasileira. Inaugurado em 2010 como parte dos preparativos para os Jogos Olímpicos, consolidou-se como o primeiro centro integrado de monitoramento urbano da América Latina, com capacidade para antecipar crises e otimizar respostas a emergências (Centro de Operações Rio, 2024). Sua estrutura inclui 3.800 câmeras monitorando a cidade; 500 profissionais atuando em turnos 24h; 2.000 ocorrências registradas mensalmente e 80 grandes eventos mapeados por mês.

Além do reconhecimento facial, o COR processa dados de sensores ambientais, órgãos públicos e colaboração cidadã. Embora não integrado diretamente ao COR, cabe destacar o papel complementar da Plataforma Córtex, sistema federal gerido pelo Ministério da Justiça e Segurança Pública (MJSP), que permite o monitoramento em tempo real de pessoas e veículos, já implementado com um termo de cooperação com o programa *Smart Sampa* desde janeiro de 2025 (São Paulo, 2025). Conforme o MJSP, trata-se de ferramenta de uso exclusivo por agentes públicos, cuja adesão por órgãos de segurança é regulamentada pela Portaria nº 218/2021 (Brasil, 2021). Essa distinção entre sistemas locais e federais evidencia os diferentes níveis de atuação na segurança pública, onde iniciativas como o COR operam em paralelo a ferramentas estratégicas nacionais.

4 ANÁLISE DO DECRETO MUNICIPAL Nº 63.552/2024 E A INSTITUCIONALIZAÇÃO DO PROGRAMA *SMART SAMPA*

O Decreto Municipal nº 63.552, de 4 de julho de 2024, formaliza a criação do Programa *Smart Sampa*, que visa integrar tecnologias avançadas à segurança pública e gestão urbana. O documento estabelece 12 diretrizes principais (Art. 2º), com destaque para:

- Integração tecnológica: Plataforma multiagência para unificação de dados de órgãos públicos (incisos I e III);
- Videomonitoramento inteligente: Rede de câmeras em locais estratégicos, com interoperabilidade entre segurança pública e serviços de emergência (inciso II);
- Proteção de dados: Conformidade com a LGPD, incluindo anonimização de informações não vinculadas a investigações (inciso XII e Art. 12);
- Parcerias público-privadas (PPPs): Cooperação com setor privado e academia para inovação tecnológica (inciso VI).

Apesar da proposta inovadora de governança digital integrada, o programa enfrenta desafios críticos como riscos de vigilância massiva, pois, a escala do monitoramento, embora amparada pelo discurso de transparência (Art. 11), pode colidir com direitos fundamentais, especialmente pela ausência de mecanismos claros para mitigação de vieses algorítmicos — que, conforme Ambrosio e Barbosa (2024), reflete a fragilidade da autorregulação estatal em sistemas de IA no Brasil.

Outro fator importante é a dependência de infraestrutura, haja vista que a efetividade do programa está condicionada a investimentos contínuos em tecnologia e capacitação técnica (Art. 10), o que demanda sustentabilidade orçamentária.

Para fiscalização, o decreto institui estruturas inéditas, composto por um Conselho de Gestão e Transparência (Art. 6º), com representantes de secretarias municipais, responsável por aprovar bases de dados e emitir relatórios anuais (Art. 7º), também prevê a Ouvidoria do Programa (Art. 8º), canal

para demandas da sociedade civil, com prazos de resposta definidos (30 dias).

Em termos de transparência, o documento avança ao prever relatórios públicos e códigos de conduta (inciso VII, Art. 7º), reforçando *accountability,* e integração com o Sistema único de Segurança Pública-SUSP (Art. 9º), alinhando-se à Lei Federal nº 13.675/2018.

Contudo, a centralização decisória na Secretaria de Segurança Urbana (Art. 4º), sem participação direta da sociedade civil, representa uma contradição frente ao Art. 11, que enfatiza proteção de dados e ética. Essa dissonância pode comprometer a legitimidade do programa, especialmente em temas sensíveis como anonimização de imagens (Art. 12) e a exigência de compromisso ético por parte de servidores (Art. 13).

Segundo Crumpler (2020), os sistemas de reconhecimento facial atingiram níveis de precisão próximos a 99,9% em condições controladas, mas sua eficácia diminui significativamente em ambientes não cooperativos, como espaços públicos. O autor complementa:

> Em abril de 2020, o melhor algoritmo de identificação facial tinha uma taxa de erro de apenas 0,08%, em comparação com 4,1% do algoritmo líder em 2014, de acordo com testes do Instituto Nacional de Padrões e Tecnologia (NIST). [...] No entanto, esse grau de precisão só é possível em condições ideais. Em implementações no mundo real, as taxas de precisão tendem a ser muito menores. Por exemplo, o FRVT descobriu que a taxa de erro para um algoritmo líder subiu de 0,1% ao comparar com fotos de identificação policial de alta qualidade para 9,3% ao comparar com fotos de indivíduos capturadas 'na natureza'. (Crumpler, 2020)

A falta de clareza no decreto quanto a mecanismos concretos para mitigação de vieses algorítmicos ou discriminação em sistemas de reconhecimento facial é preocupante. Como demonstrado no estudo seminal de Buolamwini e Gebru (2018), uma análise interseccional revelou disparidades significativas ocultadas por métricas agregadas: enquanto homens de pele clara apresentavam 0% de erro na classificação de gênero, mulheres de pele escura atingiram taxas de erro de até 34,7% em sistemas comerciais.

Esses resultados evidenciam a existência de vieses estruturais intrínsecos aos algoritmos, que transcendem questões meramente relacionadas à qualidade dos dados (Buolamwini; Gebru, 2018, p. 10-11). Este cenário ecoa quando Pinheiro (2024) alerta que a busca por eficiência na segurança pública via IA não pode ignorar os riscos de vigilância excessiva, que ameaçam liberdades civis e complementa que "sistemas de IA podem reforçar preconceitos e desigualdades, como já observado em outras partes do mundo" (Pinheiro, 2024, p. 59).

4.1 ANÁLISE DO ALINHAMENTO DO DECRETO Nº 63.552/2024 (SMART SAMPA) COM A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD – LEI FEDERAL Nº 13.709/2018)

O Decreto Municipal nº 63.552/2024, que institui o Programa *Smart Sampa*, demonstra

preocupação formal com a Lei Geral de Proteção de Dados, mas sua conformidade efetiva depende da implementação prática. Ao analisarmos os fundamentos legais e finalidade (Art. 6º, LGPD). O decreto explicita a finalidade do tratamento de dados (segurança pública e gestão urbana) e vincula seu uso a limitações técnicas e legais (Art. 1º e Art. 11).

O programa se apoia no interesse público (Art. 7º, IV, LGPD) e no cumprimento de obrigação legal (Art. 7º, II, LGPD), já que a segurança pública é dever do Estado (CF, Art. 144).

No que tange a proteção de dados pessoais (Art. 5º, LGPD), o Art. 12 determina que dados não relacionados a investigações devem ser anonimizados, conforme exigido pela LGPD (Art. 12). Mais à frente no Art. 14 exige que os sistemas adotem medidas técnicas (ex.: criptografia) para garantir confidencialidade e integridade, alinhado ao Art. 46 da LGPD.

Na LGPD em seu Art. 6º no qual trata da transparência e governança, podemos notar que no decreto em seus Art. 6º e 7ª cria o Conselho de Gestão e Transparência o qual será responsável por aprovar políticas de uso de dados e publicar relatórios, atendendo ao princípio da prestação de contas (Art. 6º, X, LGPD) como também a ouvidoria (Art. 8º), canal para cidadãos exercerem direitos previstos na LGPD (Art. 18), como acesso e retificação de dados. Sobre o assunto de limitação de acesso (Art. 18, LGPD), logo no Art. 17 do decreto restringe o acesso a imagens e dados apenas a agentes autorizados, evitando violações à privacidade.

Como já mencionado o decreto não aponta medidas concretas para mitigar discriminação racial ou de gênero em sistemas de IA, um desafio crítico em tecnologias de vigilância (ex.: falsos positivos em grupos marginalizados). E ainda prevê o compartilhamento de dados com terceiros (Art. 7º, VII) o qual seria a previsão de parcerias com entidades privadas (Art. 3º) exige cláusulas contratuais rígidas para evitar vazamentos ou uso indevido, conforme Art. 26 da LGPD. O texto não detalha esses mecanismos.

O documento carece de falta de detalhamento sobre Relatórios de Impacto (Art. 11, LGPD), embora o Art. 11, parágrafo único, cite a necessidade de Relatórios de Impacto à Proteção de Dados (RIPD), não há exigência de sua publicação ou critérios mínimos para avaliação. A ausência de detalhamento sobre Relatórios de Impacto na LGPD reflete um desafio. Como orienta Conselho Nacional de Proteção de Dados e da Privacidade - CNPD (2024) em documento sobre atuação do encarregado pelo tratamento de dados pessoais:

> Quanto à elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que consiste na documentação do controlador e contém a descrição dos processos de tratamento de dados pessoais, que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como salvaguardas e mecanismos de mitigação de risco. (CNPD, 2024 p. 29)

Ainda nessa esteira, Vieira *et al.* (2024, p.10) ressaltam que "a privacidade dos cidadãos deve ser sempre protegida, e a transparência nas operações de IA deve ser mantida para garantir a confiança

pública nas tecnologias utilizadas pelas forças policiais".

O decreto analisado não estabelece prazos para a exclusão de imagens e dados pessoais, um requisito essencial para garantir a efetividade do direito à eliminação previsto no Art. 15 da LGPD. Essa omissão pode levar a inconsistências na aplicação da norma, visto que a falta de um limite temporal pode retardar ou até mesmo inviabilizar o exercício desse direito pelos titulares.

Verifica-se que o *Smart Sampa* está formalmente alinhado à LGPD, mas sua aderência real dependerá de regulamentação complementar, pois a Secretaria de Segurança Urbana deve detalhar protocolos de anonimização, prazos de retenção e auditorias (Art. 4º). Como ressalta a Autoridade Nacional de Proteção de Dados-ANPD (2024, p. 26), "a ausência de etapas de pré-tratamento adequadas para anonimização em sistemas de IA aumenta os riscos de tratamento indevido de dados pessoais". De fiscalização independente, haja vista o Conselho de Gestão precisa incluir especialistas em proteção de dados para evitar abusos. E também de transparência, com divulgação de RIPDs e políticas de uso de algoritmo.

Recomenda-se incluir no programa avaliações periódicas de impacto em direitos fundamentais, como previsto no Art. 20 da LGPD e criar um canal específico para demandas relacionadas à proteção de dados, além da ouvidoria geral.

4.2 ANÁLISE CRÍTICA DOS IMPACTOS SOCIAIS E TECNOLÓGICOS DO *SMART SAMPA*

Os resultados operacionais do *Smart Sampa*, conforme demonstrado pelo Prisômetro (Prefeitura de São Paulo, 2025), evidenciam ganhos quantitativos inegáveis na segurança pública. Contudo, como alerta Zuboff (2021) em sua análise sobre capitalismo de vigilância, a eficiência tecnológica não pode ser o único parâmetro de avaliação.

A análise de resultados evidencia que os avanços do *Smart Sampa* em eficiência operacional (↓37% no tempo de busca de desaparecidos, ↑28% na solução de crimes) coexistem com externalidades negativas na esfera civil, conforme demonstra a seguinte relação:

Tabela 1 – Análise comparativa dos impactos do *Smart Sampa*

Eficiência Institucional	Custos Sociais
Integração de banco de dados	Commoditização de dados pessoais
Otimização de processos	Erosão da privacidade urbana
Resposta policial acelerada	Naturalização da vigilância

Fonte: Dados primários do Prisômetro (2025), análise e tabulação pela autora

A experiência internacional oferece valiosos para a evolução do *Smart Sampa*: O caso londrino é particularmente elucidativo. Conforme, um estudo independente conduzido pelo professor Pete

Fussey e pelo Dr. Daragh Murray em 2019, revelou graves falhas na precisão do sistema de reconhecimento facial utilizado pela polícia metropolitana de Londres (*Met Police*). A análise, que avaliou seis dos dez testes realizados pela polícia, constatou que, das 42 correspondências identificadas pela tecnologia, apenas oito (19%) estavam corretas — uma taxa de erro de 81%. Além disso, em quatro casos (9,5%), as pessoas não puderam ser localizadas porque foram "absorvidas pela multidão", tornando impossível confirmar a validade da identificação., corroborando as preocupações de Pinheiro (2024) sobre vieses algorítmicos no contexto brasileiro.

Baseado na análise dos dados e experiências comparadas, propõe-se um *framework* de governança multissetorial que inclui a criação de um comitê ético com participação equilibrada de diferentes setores: 40% de órgãos públicos, 30% da academia, 20% da sociedade civil e 10% do setor privado. Essa composição visa garantir que as decisões sobre o uso de tecnologias de reconhecimento facial considerem perspectivas técnicas, éticas e sociais, evitando vieses e promovendo maior legitimidade.

Complementarmente, são sugeridos protocolos de transparência ativa, que exigiriam a publicação trimestral de métricas detalhadas, incluindo taxas de acerto e erro por perfil demográfico (para monitorar possíveis discriminações), resultados de auditorias de algoritmos (com verificação independente) e relatórios de impacto social (avaliando efeitos sobre privacidade e liberdades individuais).

Para a fiscalização, propõe-se um modelo híbrido, combinando *oversight* governamental com monitoramento independente, alinhado às diretrizes da Organização para a Cooperação e Desenvolvimento Econômico - OCDE (2024) para Inteligência Artificial responsável, em especial ao Princípio 3 – "Transparência e Explicabilidade". A evolução dessa tecnologia enfrenta três trajetórias possíveis:

1. Cenário Otimista: Adoção integral das recomendações, com alocação de orçamento sustentável e equilíbrio entre ganhos de eficiência policial e proteção de direitos fundamentais.
2. Cenário de Estagnação: Manutenção do *status quo* levaria à erosão da confiança pública e ao aumento de litígios judiciais, sobrecarregando o sistema.
3. Cenário Crítico: Expansão não regulada resultaria em violações graves de privacidade, incidentes de discriminação algorítmica e eventual rejeição social, inviabilizando a continuidade dos projetos.

Essa estrutura busca mitigar riscos evidenciados por estudos como o de Fussey e Murray (2019), que alertaram para taxas de erro de 81% em sistemas policiais, reforçando a urgência de modelos de governança inclusivos e auditáveis. A implementação exigirá cooperação interinstitucional

e adaptação contínua às evidências empíricas.

5 CONSIDERAÇÕES FINAIS

O Programa *Smart Sampa* representa um avanço significativo na modernização da segurança pública, ao integrar tecnologias de Inteligência Artificial (IA), reconhecimento facial e análise de dados em tempo real. Os resultados preliminares demonstram sua eficácia operacional em três eixos principais: (1) localização de desaparecidos, (2) captura de foragidos e (3) identificação de crimes em flagrante. Esses êxitos reforçam o potencial da integração interinstitucional para respostas mais ágeis e eficientes na segurança urbana.

Contudo, a implementação do programa revela desafios críticos que demandam aprimoramentos. As questões éticas e de privacidade emergem como preocupações centrais, particularmente no que tange ao uso de dados pessoais e aos riscos de discriminação algorítmica. Como alerta Pinheiro (2024, p. 57), "o Brasil ainda não possui mecanismos eficazes para proteger os direitos individuais frente ao uso de tecnologias na segurança pública". Essa falta normativa torna imperativa a adoção de:

1. Regulamentações específicas para sistemas de IA na segurança pública;
2. Mecanismos confiáveis de transparência, incluindo auditorias independentes periódicas;
3. Participação efetiva da sociedade civil nas estruturas de governança do programa.

O Decreto Estadual nº 63.552/2024, embora alinhe o *Smart Sampa* à Lei Geral de Proteção de Dados (LGPD), apresenta deficiências em aspectos relevantes como os prazos claros para retenção de dados, os protocolos para mitigação de vieses algorítmicos e mecanismos de fiscalização independente.

Nesse contexto, o relatório da Autoridade Nacional de Proteção de Dados (ANPD) (2024, p. 32) enfatiza a necessidade de implementar "mecanismos de prestação de contas em sistemas de IA generativa", recomendação que deveria ser incorporada ao programa. O Paraná vem desenvolvendo modelos inovadores de proteção a vítimas de violência doméstica que podem inspirar aprimoramentos no *Smart Sampa*. Após testes pontuais com reconhecimento facial em viaturas (Freitas, 2023 Apud Vieira *et al.,* 2024), o estado implementou em 2025 o "Programa Mulher Segura" com monitoramento eletrônico simultâneo, sistema pioneiro que combina: tornozeleiras com *geofencing* para agressores; dispositivos móveis com botão de pânico para vítimas; integração em tempo real com o aplicativo 190 PR (Paraná, 2025).

Dados preliminares indicam redução de 24% nos feminicídios nos municípios pilotos, embora especialistas alertem para desafios como a cobertura em áreas rurais e a dependência de decisões judiciais individuais (Paraná, 2025). Essa experiência sugere que o *Smart Sampa* poderia incorporar módulos específicos para violência de gênero, ponto já sinalizado dentro do programa da cidade de São Paulo a ser expandido.

Em síntese, o *Smart Sampa* configura-se como ferramenta promissora para a segurança pública contemporânea. Contudo, seu sucesso sustentável exigirá equilíbrio cuidadoso entre inovação tecnológica e garantias fundamentais, marco regulatório específico para IA na segurança pública e um modelo de governança participativo e transparente.

Como demonstrado, o programa tem potencial para transformar práticas de segurança pública, mas sua consolidação como política pública democrática dependerá da superação dos desafios éticos e jurídicos aqui apontados.

REFERÊNCIAS

AMBROSIO, Gleiner Pedroso Ferreira; BARBOSA, André Luis Jardini. **O paradigma da implantação da inteligência artificial na segurança pública brasileira: regulação versus eficiência. Revista de Estudos Jurídicos da UNESP**, Franca, v. 28, n. 48, p. 73-92, 2024. Disponível em: https://ojs.franca.unesp.br/index.php/estudosjuridicosunesp/article/download/4398/3595/17002. Acesso em: 15 fev. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia de atuação do encarregado perante a ANPD.** Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/copy_of_guia_da_atuacao_do_encarregado_anpd.pdf. Acesso em: 18 abr. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Radar tecnológico nº 3: inteligência artificial generativa.** Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar_tecnologico_ia_generativa_anpd.pdf. Acesso em: 18 abr. 2025.

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Portal Gov.br, [s.d.]. Disponível em: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd#:~:text=A%20Lei%20Geral%20de%20Prote%C3%A7%C3%A3o,da%20personalidade%20de%20cada%20indiv%C3%ADduo. Acesso em: 11 jan. 2025.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Estratégia Brasileira de Inteligência Artificial: documento de referência**. Brasília: **MCTI, 2021**. 97 p. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-documento_referencia_4-979_2021.pdf. Acesso em: 08 mar. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. **Plataforma de Monitoramento Córtex**. Brasília, DF: MJSP. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/operacoes-integradas/destaques/plataforma-de-monitoramento-cortex. Acesso em: 25 jun. 2025.

BRASIL. **Portaria nº 218, de 29 de setembro de 2021.** Estabelece diretrizes para adesão à Plataforma Córtex. Diário Oficial da União: seção 1, Brasília, DF, ed. 186, p. 10, 30 set. 2021. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/operacoes-integradas/cortex/publicacoes/portaria-no-218-de-29-de-setembro-de-2021. Acesso em: 25 jun. 2025.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: **CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY (FAT*), 1., 2018, New York. Proceedings... [S.l.]: PMLR, 2018. p. 1-15**. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 29 jun. 2025.

CENTRO DE OPERAÇÕES RIO. **História**. Disponível em: https://cor.rio/historia/. Acesso em: 15 mar. 2025.

CRUMPLER, William. **How Accurate Are Facial Recognition Systems—And Why Does It Matter?** Center for Strategic and International Studies *(CSIS)*, 14 abr. 2020. Disponível em: https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it. Acesso em: 23 jun. 2025.

FUSSEY, P.; MURRAY, D. **Met Police's facial recognition tech has 81% error rate, independent report says**. *Sky News*, 2019. Disponível em: https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941. Acesso em: 16 fev. 2025.

GOVERNO DO PARANÁ. **Como será monitoração simultânea de mulheres vítimas de violência e agressores.** Agência Estadual de Notícias (AEN), Curitiba, [2024?]. Disponível em: https://www.parana.pr.gov.br/aen/Noticia/Como-sera-monitoracao-simultanea-de-mulheres-vitimas-de-violencia-e-agressores. Acesso em: 27 jun. 2025.

NAGATA, Sabrina Vettorazzi. **Utilização da inteligência artificial na segurança pública e sua contribuição na Polícia Militar**. Brazilian Journal of Development, Curitiba, v. 10, n. 6, p. 01-18, 2024. DOI: 10.34117/bjdv10n6-066. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/70815/49817. Acesso em: 08 mar. 2025.

OECD. **Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449)**. Paris: OECD, 2019 [atualizado 2024]. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Acesso em: 14 mar. 2025.

ORWELL, George. **1984**. Tradução de Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

PINHEIRO, Flávio Maria Leite. **O papel da tecnologia e da inteligência artificial na segurança pública: desafios e convergências com os direitos fundamentais individuais e**

sociais. Ministério Público do Estado do Rio de Janeiro (MPRJ). Disponível em: https://www.mprj.mp.br/documents/20184/7377608/flavio_maria_leite_pinheiro.pdf. Acesso em: 10 abr. 2025.

PREFEITURA DE SÃO PAULO. **Câmeras do Smart Sampa começam a ler placas para identificar veículos roubados.** Prefeitura de São Paulo, 10 jan. 2025. Disponível em: https://prefeitura.sp.gov.br/w/c%C3%A2meras-do-smart-sampa-come%C3%A7am-a-ler-placas-para-identificar-ve%C3%ADculos-roubados-%C2%A0%C2%A0. Acesso em: [insira a data de acesso no formato: 29 jun. 2025.

PREFEITURA DE SÃO PAULO. **Painel Prisômetro**. Smart Sampa, Prefeitura de São Paulo. Disponível em: https://smartsampa.prefeitura.sp.gov.br/#prisometro. Acesso em 02 fev. 2025.

PREFEITURA DE SÃO PAULO. **Smart Sampa: Tecnologia e inovação na segurança urbana.** Secretaria de Segurança Urbana, 2025. Disponível em: https://capital.sp.gov.br/web/seguranca_urbana/w/smart-sampa-2. Acesso em: 06 abr. 2025.

PREFEITURA DE SÃO PAULO. **Decreto nº 63.552, de 4 de julho de 2024**. Cria o Programa Smart Sampa. Diário Oficial da Cidade de São Paulo, 2024. Disponível em: https://legislacao.prefeitura.sp.gov.br/leis/decreto-63552-de-4-de-julho-de-2024. Acesso em: 08 mar. 2025..

PUC-SP. **Smart Sampa: o polêmico projeto de IA para SP**. *AGEMT - Agência Escola de Comunicação Pública e Jornalismo da PUC-SP*, 2023. Disponível em: https://agemt.pucsp.br/noticias/smart-sampa-o-polemico-projeto-de-ia-para-sp. Acesso em: 5 fev. 2025.

UNESCO. **Relatório mundial sobre ética da inteligência artificial.** Paris: UNESCO, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137_por. Acesso em: 25 jun. 2025.

VIEIRA, Flávia da Silva et al. **Aplicabilidade da Inteligência Artificial nas Polícias Militares Brasileiras: vantagens, desvantagens e/ou limitações.** In: CONGRESSO INTERNACIONAL DE CONHECIMENTO E INOVAÇÃO (CIKI), 2023, Florianópolis. Anais eletrônicos... Florianópolis: UFSC, 2023. Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/1631/925. Acesso em: 10 mar. 2025. 2024.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. Tradução: George Schlesinger. 1. ed. Rio de Janeiro: Intrínseca, 2021. 688 p. E-ISBN 978-65-5560-145-9. Disponível em: https://nae.com.pt/wp-content/uploads/A-Era-do-Capitalismo-de-Vigilancia-Shoshana-Zuboff.pdf. Acesso em: 16 mar. 2025.

ZUCHERATO, Gustavo. **Case Study: Um ano de City Câmera – a evolução, tecnologias e resultados do programa**. *Revista Digital Security*, 1 abr. 2018. Disponível em: https://revistadigitalsecurity.com.br/case-study-um-ano-de-city-camera-a-evolucao-tecnologias-e-resultados-do-programa/. Acesso em: 03 jul. 2025.