

ADRIANO DE CARVALHO MENDES

**Experimentos tecnopolíticos urbanos: a
socioespacialidade do Projeto Piloto de reconhecimento
facial no Rio de Janeiro**

Dissertação apresentada ao Curso de Mestrado do
Programa de Pós-Graduação em Planejamento
Urbano e Regional da Universidade Federal do Rio
de Janeiro – UFRJ, como parte dos requisitos
necessários à obtenção do grau de Mestre em
Planejamento Urbano e Regional.

Orientadora: Prof. Dra. Lalita Kraus

Co-orientador: Prof. Dr. Rodrigo José Firmino

Rio de Janeiro
2025

CIP - Catalogação na Publicação

M538e Mendes, Adriano de Carvalho
Experimentos tecnopolíticos urbanos: a
socioespacialidade do Projeto Piloto de
reconhecimento facial no Rio de Janeiro / Adriano
de Carvalho Mendes. -- Rio de Janeiro, 2025.
97 f.

Orientadora: Lalita Kraus.
Coorientadora: Rodrigo Jose Firmino.
Dissertação (mestrado) - Universidade Federal do
Rio de Janeiro, Instituto de Pesquisa e
Planejamento Urbano e Regional, Programa de Pós
Graduação em Planejamento Urbano e Regional, 2025.

1. Reconhecimento Facial. 2. Segurança Pública.
3. Rio de Janeiro. 4. Racismo Algorítmico. 5.
Política Pública . I. Kraus, Lalita, orient. II.
Firmino, Rodrigo Jose, coorient. III. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos
pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

ADRIANO DE CARVALHO MENDES

**Experimentos tecnopolíticos urbanos: a
socioespacialidade do Projeto Piloto de reconhecimento
facial no Rio de Janeiro**

Dissertação apresentada ao Curso de Mestrado
do Programa de Pós-Graduação em
Planejamento Urbano e Regional da
Universidade Federal do Rio de Janeiro – UFRJ,
como parte dos requisitos necessários à
obtenção do grau de Mestre em Planejamento
Urbano e Regional.

Aprovado em:

Documento assinado digitalmente
gov.br LALITA KRAUS
Data: 21/01/2025 12:36:42-0300
Verifique em <https://validar.iti.gov.br>

BANCA EXAMINADORA

Prof. Dr^a. Lalita Kraus

Instituto de Pesquisa e Planejamento Urbano e Regional - UFRJ



Prof. Dr. Rodrigo José Firmino

Gestão Urbana - PUC/PR

Documento assinado digitalmente
gov.br ORLANDO ALVES DOS SANTOS JUNIOR
Data: 21/01/2025 19:30:16-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. Orlando Alves Santos Junior

Instituto de Pesquisa e Planejamento Urbano e Regional - UFRJ

DocuSigned by:

CE4B70B77F00494...

Dr^a. Iris de Macedo Rosa

Instituto Fogo Cruzado

“O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001”.

“This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001”.

DEDICATÓRIA

Dedico este trabalho de conclusão de mestrado a todas as pessoas negras que, diariamente, enfrentam as consequências do racismo estrutural em nossa sociedade. No campo da segurança pública, é incontestável que indivíduos negros são desproporcionalmente afetados por práticas que os marginalizam e os tornam alvos das políticas de repressão. A análise crítica aqui realizada evidencia que as ferramentas de segurança, em vez de promoverem a justiça, muitas vezes reforçam as estruturas opressivas que perpetuam o encarceramento da juventude negra e a criminalização de corpos negros.

Este trabalho também é dedicado ao movimento que luta pelo banimento das tecnologias de reconhecimento facial no contexto da segurança pública brasileira, representado pela campanha "Tire Meu Rosto da Sua Mira". As evidências de seu uso abusivo e opaco são alarmantes, e sua implementação não apenas compromete direitos fundamentais, como a privacidade e a proteção de dados pessoais, mas também ameaça direitos basilares como a liberdade de expressão, o direito ao encontro e os princípios de igualdade e não discriminação. A utilização dessas tecnologias é um reflexo claro do racismo institucionalizado e da vigilância excessiva que incidem sobre populações historicamente marginalizadas. Por isso, é imperativo que continuemos a lutar contra práticas que violam os direitos humanos e que impactam de forma tão profunda a dignidade e a liberdade de milhares de pessoas.

RESUMO

O reconhecimento facial é uma técnica biométrica que se propõe a identificar ou negar o controle de circulação de pessoas tidas como criminosas por meio da identificação. O uso desta tecnologia, para fins de segurança pública envolve obrigações éticas e regulatórias, mas que apresentam probabilidade de apresentar problemas tanto do ponto de vista jurídico, ético e social quanto para o uso em políticas públicas. Diante disso, a tecnologia de reconhecimento facial é apresentada em nível nacional como um avanço tecnológico capaz de resolver a insegurança e a violência urbana, levando à sua adoção por parte do poder público para o controle do espaço público. Nesse contexto, impulsionado pelos megaeventos que passaram pelo Brasil, mas sobretudo no Rio de Janeiro, observamos a implementação de projetos pilotos de segurança pública, abrindo portas para elevados investimentos tecnológicos e militarizados, incluindo sistema de videomonitoramento e reconhecimento facial, com a perspectiva de passar uma imagem de controle da violência. Porém, não se trata apenas de adquirir e implementar a tecnologia, observamos que trata-se de um sistema capaz de causar impactos diretos na vida social e urbana. Por isso, este trabalho está concentrado em compreender como o sistema de reconhecimento facial tem proporcionado efeitos socioespaciais, usando a partir da experiência de implementação do Projeto Piloto instalado em 2019 pelo Governo do Estado do Rio de Janeiro.

Palavras chaves: reconhecimento facial, espaço, território, política pública, segurança pública.

ABSTRACT

Facial recognition is a biometric technique capable of identifying or denying control of criminal conduct through identification. The use of this technology for public security purposes involves ethical and regulatory obligations, but is likely to present problematic legal, ethical and social aspects regarding its use in public policies. Given this, technology is presented nationally as a technological advance capable of resolving insecurity and urban violence, leading to its adoption by public authorities to control public space. In this context, driven by the mega-events that took place in Brazil, but especially in Rio de Janeiro, we observed the implementation of public security pilot projects, opening doors for high technological and militarized investments, including video monitoring and facial recognition systems, with the prospect of passing an image of control of violence. However, it is not just about acquiring and implementing technology, we observe that it is a system capable of causing direct impacts on social and urban life. Therefore, this work is focused on understanding how the facial recognition system has had an effect on public space for those who are impacted, using the experience of victims of the implementation of the Pilot Project installed in 2019 by the Government of the State of Rio. de Janeiro, therefore, the methodology is divided into four stages, including: bibliographical review, mapping of victims through the system, interviews and case analysis.

Keywords: facial recognition, space, territory, public policy, public security.

LISTA DE ILUSTRAÇÕES

Figura 1 - Mapa de observação em Copacabana e Ipanema	29
Figura 2 - Mapa de observação na região do Maracanã	29
Figura 3 - Mapa com delimitação do projeto piloto em Copacabana	49
Figura 4 - Mapa com delimitação do projeto piloto no Maracanã	50
Figura 5 - Sala de monitoramento do Centro Integrado de Comando e Controle	59
Figura 6 - Print da rede social “X”	63
Figura 7 - Promessas de campanha	64
Figura 8 - Tire o meu rosto da sua mira	69
Figura 9 - Campanha pelo banimento do reconhecimento facial	70
Figura 10 - Falhas do projeto piloto	76

LISTA DE ABREVIATURAS E SIGLAS

ADPF - Arguição de Descumprimento de Preceito Fundamental

CESEC - Centro de Estudos de Segurança e Cidadania

CCTV – Closed-Circuit Television

CICC – Centro Integrado de Comando e Controle

COR – Centro de Operações do Rio

DNA – Ácido Desoxirribonucleico

DP – Delegacia de Polícia

ESMESC – Secretaria Extraordinária de Segurança para Grandes Eventos do Ministério da Justiça

FIFA – Fédération Internationale de Football Association

IA – Inteligência Artificial

PCA – Análise de Componentes Principais

RF – Reconhecimento Facial

RJ – Rio de Janeiro

SEPM – Secretaria de Estado de Polícia Militar

TIC – Tecnologia da Informação e Comunicação

TJSP – Tribunal de Justiça de São Paulo

SUMÁRIO

1 - INTRODUÇÃO	11
1.1. PROBLEMA E PERGUNTA DE PESQUISA.....	18
1.2. OBJETIVOS.....	26
1.3. METODOLOGIA	26
1.3.1 LIMITES DA PESQUISA	31
1.4 ESTRUTURA	32
CAPÍTULO 2 - RECONHECIMENTO FACIAL E MILITARIZAÇÃO DO ESPAÇO PÚBLICO	34
2.1. DADOS, VIGILÂNCIA E CONTROLE SOCIAL.....	37
2.2 RECONHECIMENTO FACIAL NO ESPAÇO PÚBLICO	45
2.2.1. A MILITARIZAÇÃO E ESPAÇO PÚBLICO	47
CAPÍTULO 3 - TECNOPOLÍTICA DA SECURITIZAÇÃO E MILITARIZAÇÃO: O CASO DO PROJETO PILOTO	52
3.1. O projeto piloto e sua distribuição “estratégica”	52
3.2. Tecnologia á serviço da militarização	60
3.3. Discurso oficial e vigilância ampliada.....	68
3.4. Segregação sociotécnica	78
CONCLUSÃO 4	87
REFERÊNCIAS	93

1 - INTRODUÇÃO

Reconhecimento facial é uma técnica de identificação biométrica, na qual um software mapeia as linhas faciais e, através de algoritmos, compará-los a uma imagem digital resultando no reconhecimento da sua identidade ou negando (ABBAS DA SILVA; FRANQUEIRA; HARTMANN, 2021). O recurso é utilizado também como ferramenta que auxilia as políticas de videomonitoramento da segurança pública, como mecanismo de prevenção da criminalidade, pois substitui outras ferramentas de segurança (chaves, códigos numéricos e biometria com impressão digital) que diferentemente do reconhecimento facial, não traz uma maior veracidade (MASTRO; CORTIZ; DEIRÓ, 2022). O reconhecimento facial também é uma tecnologia, assim, apresentada como dispositivo eficiente para o controle de condutas criminosas por meio da identificação de pessoas através de câmeras de videomonitoramento instaladas na cidade.

Cada sistema é diferente, porém, o que há de comum quando o assunto é segurança pública, são os princípios básicos de funcionamento. A câmera registra a imagem do rosto das pessoas e as suas características, como por exemplo, nariz, boca, tamanho do crânio e entre outros aspectos biológicos, ou seja, tornam o rosto humano um dado biométrico calculável, sensível e potencialmente associado a desvio de padrão pré-estabelecido. Após a identificação, o sistema identifica os rostos que são capturados em tempo real e conseqüentemente comparados com imagens digitais contidas em banco de dados (RAMOS, 2022). Esse processo levanta questões éticas e regulatórias que exigem que o sistema seja abordado com cuidado. Por exemplo, ao ser utilizado em tomada de decisões públicas, é importante reconhecer que o reconhecimento facial apresenta probabilidade de erros, tratando-se de uma tecnologia que não tem capacidade de assimilar toda a complexidade do mundo real (O'NEIL, 2016).

A adoção de soluções tecnológicas, como o sistema de reconhecimento facial acoplado ao videomonitoramento na segurança pública, se insere num contexto mais amplo de popularização do uso de tecnologia na gestão de políticas públicas. Trata-se aqui a tecnologia como uma extensão da capacidade humana, com técnica acumulada, contudo, vivenciamos a multiplicação de tecnologias e suas implicações

no meio ambiente, no espaço físico (que também provém de processos tecnológicos), ao próprio corpo biológico. (FIRMINO; DUARTE, 2012). Diante disso, observamos um cenário de grandes mudanças que estão de certo modo ligadas a transformação, por exemplo, computadores cada vez mais poderosos permitem que surjam novas ferramentas de apoio cada vez mais sofisticadas principalmente no âmbito da informação e comunicação. Falamos de uma tecnologia que se insere em uma nova era que Weiser (1991) chama de computação ubíqua, onde vivemos em uma realidade na qual as máquinas e sistemas ligados a uma rede, se comunicam entre si e agem e tomam decisões por seres humanos. Isso não quer dizer que as tecnologias não necessitam de suas atribuições sociais, das intenções mercadológicas, socioeconômicas, políticas, culturais e entre outras dentro da sua conexão, de seus significados. (FIRMINO; DUARTE, 2012), mas que também passam a ser dados como inerentes ao seu espaço.

Da maneira que surgem novas ferramentas tecnológicas (celulares, tablets, laptops...) há uma busca incessante por dispositivos tecnológicos sempre mais eficientes para solucionarem questões presentes (ROSA; SZAPIRO, 2015). Hoje, com a existência da internet e as recentes tecnologias da informação e comunicação (TICs), possibilita estender o corpo, amplificar o ambiente, ampliar o espaço, além de aumentar a nossa capacidade comunicativa e interativa. (FIRMINO; DUARTE, 2012) Elas são a representação clara de manifestações de características híbridas ambíguas de espaço e tecnologia no mundo urbano. Contudo, preciso lembrar que a nossa história tecnológica, não se inicia com os produtos mais sofisticados, mas sim junto com os primeiros humanos ao descobrir possíveis modificações na natureza que permitam melhorar suas condições de vida e em grupo (fogo, bicicleta, avião) (VERASZTO, 2004).

Ao se apropriarem dessas tecnologias, vamos observar uma mudança com a adoção das tecnologias de informação e comunicação no âmbito da administração pública, com o objetivo de modernizar sua operação e tenham maior capacidade de gerar informações precisas e coerentes para tomadas de decisão (MAXIMO, 2004), um exemplo são os serviços eletrônicos pelos governos, mesmo que de maneira tímida, o recebimento, tratamento e armazenamento de informações, principalmente pela velocidade e flexibilização da informação (CASTELLS, 1999) e a transformação do ambiente onde a sociedade interagem é mais rápida.. uso de tecnologias não se

restringe apenas ao relacionamento entre o cidadão e o governo, mas também na tomada de decisão, em especial em setores onde a política pública tem um contato físico com a população, como por exemplo, o uso de TIC's no contexto urbano, como as câmeras com sistema de reconhecimento facial, onde evidencia um processo de apropriação das tecnologias na gestão urbana. (FIRMINO; FREY, 2009) e que é tema deste trabalho. A transformação da espacialidade contemporânea acaba por estabelecer novas relações de territorialidade. (FIRMINO; DUARTE, 2012), mesmo nos momentos em que falham. Do mesmo modo, o aproveitamento das infraestruturas sofisticadas associadas às TICs (como satélites, radares, geradores de ondas e, principalmente, os fluxos produzidos por estruturas (micro-ondas sinais, eletromagnéticos, etc), são normalmente silenciosas e invisíveis para a maioria da sociedade. Com isso, há uma tendência de acreditar que a tecnologia como produto de decisão estritamente técnica quando na verdade ela não é, e com isso, ignoramos elementos fundamentais que se constituem na relação tecnologia-sociedade, inclusive percebendo-as como neutras (SIMÃO; FIRMINO, 2019). É o caso da presença massiva de dispositivos de vigilância no cotidiano dos grandes centros urbanos, relacionada principalmente a questão da segurança, na qual a urgência de resolver a desordem, a busca por tecnologias de vigilância se torna algo grande (ROSA; SZAPIRO, 2015), como é o caso do sistema de reconhecimento facial acoplado às câmeras como uma forma engenhosa de combater a violência na sociedade (BARBOSA; LEHFELD, 2016). Nesse sentido, vamos observar que há um interesse político e econômico que vem crescendo de forma exponencial voltado para a implementação de modelos urbanos inteligentes, cuja realização é muitas vezes motivada pela necessidade de atrair investimento nas cidades e corresponder a uma agenda de sustentabilidade urbana (KRAUS, 2022). A agenda inteligente é um dos principais discursos legitimadores do amplo uso e implementação da tecnologia no contexto urbano (LUQUE-AYALA et al, 2014), fundamentando-se no princípio da gestão eficaz e na defesa do sistema de reconhecimento facial como solução neutra, livre de falhas.

Nesse contexto, a cidade contemporânea traz consigo novos elementos que necessitam ser considerados na reprodução do espaço urbano sejam tecnologias cada vez mais invisíveis e uma “ampliação” do espaço urbano para além das suas fronteiras a partir do uso de TICs (DUARTE; FIRMINO, 2009). É dentro desse

contexto que a tecnologia de reconhecimento facial é apresentada como um avanço tecnológico e solução para aliviar a insegurança e violência urbana, transformando centros urbanos em cidades não apenas inteligentes, como também mais seguras e sustentáveis. É importante destacar que o discurso urbano-tecnológico é utilizado como uma ferramenta que mobiliza consenso quando apresenta-se como um modelo ideal de sucesso com a capacidade de impactar positivamente as políticas e o planejamento urbano (GONÇALVES; PAIVA, 2012).

É a partir deste paradigma que observamos uma insistência por parte das corporações em investir cada vez mais em soluções tecnologias de ponta e de desenvolvimento de infraestrutura, em contraponto, temos o poder público mergulhando na agenda urbano-tecnológica para movimentar a economia e tornar a cidade mais competitiva (MOROZOV E BRIA, 2019). Ainda que a pauta urbano-tecnológica seja aquecida, muitas vezes, pelo setor privado e agências internacionais, vemos que a busca pela inovação também em grande parte se mostrou prioridade do poder público. A adoção de tecnologias no setor público é apresentada como caminho para maximizar a eficiência dos serviços públicos (novas habilidades de gestão ou processual, novos conhecimentos e/ou habilidades) e promover contextos urbanos inteligentes (HALVORSEN ET AL. 2005; LUQUE-AYALA et al, 2014).

Em vista disso, observamos a implementação de projetos pilotos que oferecem soluções tecnológicas que atingem a oferta de bens, serviços e equipamentos urbanos (OLIVEIRA, et al, 2022). Consideramos relevante a apresentação inicial de tais projetos com caráter de teste, facilitando e justificando a sua implementação num contexto urbano que funcionaria como laboratório da tecnologia e como um espaço de experimentações que tem por objetivo a melhoria da qualidade de vida¹. Contudo, é importante destacar o uso da nomenclatura “projeto piloto” para as primeiras experiências com o uso do sistema de reconhecimento facial no Rio, que acaba por permitir que seus operadores justifiquem erros. Apesar disso, vários desses projetos assumem características definitivas, envolvendo inclusive investimento consistentes para a implementação de uma grande quantidade de câmeras e a cobertura de grandes áreas urbanas, como no caso do pregão eletrônico

¹ GATES. 2011, p. 76

aberto pela Prefeitura de São Paulo para o projeto Smart Sampa² e outros projetos nos municípios de Vitória, João Pessoa, São José dos Campos (SP), Guarujá (SP) (SILVA, 2021).

Para contextualizar, no Rio de Janeiro a implementação do uso de reconhecimento facial, em conjunto com o sistema de videomonitoramento, está vinculada à agenda dos megaeventos. Desde a Conferência Eco 92 da ONU no Rio de Janeiro, a agenda política carioca vem sendo definida pelos megaeventos (LEITE, 2017). Ter a cidade do Rio de Janeiro como sede para tantos eventos em tão pouco tempo, produziu no contexto urbano e político uma imagem da cidade que fosse a expressão de um projeto nacional. No imaginário dos planejadores dos megaeventos, o reconhecimento facial representa uma oportunidade para promover uma forma de “solucionismo” (MOROZOV, 2013), que é proposta inclusive para controlar as crescentes manifestações políticas iniciadas em 2013 (ZIMBALIST, 2015).

Os megaeventos, ao colocarem o Brasil no centro dos holofotes internacionais, levantaram novas demandas de enfrentamento da questão da segurança pública para repassar uma imagem de controle da violência. Isso justificaria investimentos para barrar ameaças terroristas e combater o crime local. Só para a realização da Copa de 2014 foram investidos aproximadamente R\$1.9 bilhões em segurança pública, um recurso utilizado principalmente para a realização de operações, captação de agentes, armamento, treinamento e tecnologia. (CAMPOS, 2014). Foram escalados mais de 116,6 mil agentes das forças de segurança³. Essas intervenções marcam o território não apenas durante os megaeventos, como também nos dias atuais, à medida que a tecnologia de controle e securitização é considerada legado dos megaeventos, como no caso do Centro Integrado de Comando e Controle (CICC).

Mediante todas essas transformações, pode-se observar um movimento de despolitização da cidade, que significa o aceleração da transformação do espaço

² Smart Sampa: pregão eletrônico para contratação de 20 mil câmeras de monitoramento é agendado para 23 de maio. Prefeitura. Disponível em: <<https://www.capital.sp.gov.br/noticia/smart-sampa-pregao-eletronico-para-contratacao-de-20-mil-cameras-de-monitoramento-e-agendado-para-23-de-maio>>. Acesso em: 8 nov. 2023.

³ Governo brasileiro divulga balanço das ações durante a Copa do Mundo 2014. Disponível em: <<https://www.justica.gov.br/news/governo-brasileiros-divulga-balanco-das-acoes-durante-a-copa-do-mundo-2014>>. Acesso em: 26 abr. 2023

público em privado, ou seja, trata-se então sobre o enfraquecimento da ação coletiva do espaço público. Junto com a negligência do Estado e do setor imobiliário, o processo de privatização do espaço, neste período, alinha apenas os interesses das grandes empresas e da organização privada, como a FIFA e o Comitê Olímpico Internacional, e que nega a necessidade de uma discussão mais profunda e política em relação à democracia urbana. Dentre os assuntos abordados até aqui, pode-se perceber que os processos não acontecem de maneira isolada. Em quase todos os aspectos, os megaeventos operam dentro de um panorama de segurança pública precário, desigual e violento, além de criar novos mecanismos institucionais de caráter “excepcional”.

Assim, com a chegada dos megaeventos no Brasil, percebe-se uma onda de tecnologização e militarização das cidades com o intuito de garantir segurança durante a sua realização (GAFFNEY, 2016). O investimento tecnológico se insere, assim, como componente no processo de transformação do espaço urbano carioca. Tendo isso como ponto de partida, pretendemos com a presente pesquisa investigar o projeto piloto que, em 2019, deu início a implementação do sistema de reconhecimento facial na cidade do Rio de Janeiro e que operou na primeira fase durante o carnaval⁴.

Normalmente, esses projetos pilotos colocam a tecnologia de reconhecimento facial como item solucionador indispensável, indiscutível e inquestionável dos problemas urbanos de segurança. Trata-se de uma interpretação determinista de tecnologia que pode mascarar interesses ocultos corporativos e do setor público. O sentido conferido ao reconhecimento facial é um fator determinante na construção de um consenso em torno de modelos urbanos tecnológicos que podem mascarar, não apenas interesses nem sempre tão explícitos, como também eventuais contradições e efeitos controversos.

Nesse sentido, devemos reconhecer e observar a resposta social às determinações tecnológicas, particularmente ressaltando os efeitos e custos sociais à medida em que consideramos não só o caráter técnico como também político da

⁴ Cf: Copacabana terá sistema de reconhecimento facial durante o Carnaval. Disponível em: <<https://veja.abril.com.br/brasil/copacabana-tera-sistema-de-reconhecimento-facial-durante-o-carnaval/>>. Acesso em: 1 fev. 2022.

tecnologia. Isso nos permite contextualizar o processo de implementação tecnológica, evitando uma abordagem que considere tais soluções como universais e neutras e ignore qualquer especificidade do contexto (KRAUS, 2022). Nesse sentido, reconhecemos a importância de tratar do reconhecimento facial no Rio de Janeiro considerando seu contexto socioespacial desigual e a atuação violenta do Estado em seus territórios periféricos.

Qualquer dispositivo tecnológico não deve ser avaliado apenas pela contribuição a algum tipo de eficiência ou melhoria na prestação de um serviço, como também pelos modos como incorpora formas de poder e como ordena a sociedade. Tecnologias, como o reconhecimento facial, não só podem otimizar processos, como podem mudar a forma como vivemos em sociedade. Portanto, não se trata apenas de adquirir e implementar as novidades mais sofisticadas quando estamos nos referindo a sistema que tem impacto direto na vida social. Por isso, conforme o poder público utiliza um número cada vez maior de soluções tecnológicas, devemos questionar o real impacto que o uso de tecnologia no setor público têm comparado ao antes e depois da implementação.

Sabemos que a maioria das cidades brasileiras têm problemas sociais que resultam em altos índices de violência e que é dentro desse contexto que observamos o aumento do uso de câmeras de reconhecimento facial no Brasil, inclusive em espaços públicos. A implementação de tais sistemas é acompanhada por um discurso que os apresenta como sistemas de monitoramento capazes de observar a movimentação das pessoas e identificar crimes, porém, também observamos o quanto a instalação desses equipamentos tem levantado uma série de debates quanto a sua aplicação envolvendo aspectos jurídicos, técnicos e sociais.

Em relação ao aspecto jurídico, além da coleta e manipulação de dados pessoais, o maior problema é que sistemas como o RF (Reconhecimento facial) têm como risco potencial uma falsa legitimação de um sistema jurídico e carcerário assimétrico, punitivista e completamente enviesado com relação às populações negras e periféricas. Em termos técnicos é preciso garantir a precisão da operacionalização da tecnologia para que se evite os “falsos positivos” (LAVADO, 2022). Além disso, são inúmeros os estudos que apontam os riscos da instauração de uma sociedade vigiada e cada vez mais controlada (BRUNO et al, 2018).

Portanto, o aumento da tecnologia de reconhecimento facial em espaços públicos tem contribuído para o avanço do setor privado na gestão sobre o espaço público. Isso quer dizer que à medida que se implementa o monitoramento de espaços públicos, por trás há uma empresa privada que gere esse espaço que deveria ser livre de qualquer tipo de controle privado. Existem maneiras de se entender o espaço, contudo, espaços mais controláveis resultam num rearranjo de fronteiras (FIRMINO, 2017), que em outras palavras, é abrir precedente para questionar se o uso de sistemas de reconhecimento facial são novas estratégias de controle, acessos e circulação.

Considerando esse contexto e reflexões iniciais, essa pesquisa pretende compreender, entre outros aspectos, a relação existente entre a tecnologia de reconhecimento facial e o espaço público, investigando como essa ferramenta de vigilância impacta a dinâmica social, o acesso e uso dos espaços urbanos, bem como as implicações para direitos fundamentais, especialmente no que se refere à privacidade, liberdade de circulação e possíveis discriminações relacionadas a raça e classe social quando o sistema de reconhecimento facial atua. A seguir será apresentada a organização e estrutura da pesquisa, apontando o problema de pesquisa, os objetivos e a metodologia adotada.

1.1. PROBLEMA E PERGUNTA DE PESQUISA

A implementação do sistema de reconhecimento facial nas cidades brasileiras tem se dado de forma exponencial. Desde 2011 pode-se observar que a utilização da tecnologia pelo setor público tem se dado no campo da educação, transporte, controle de fronteiras e segurança pública. (IGARAPÉ, 2022). No Brasil, pode-se afirmar que o reconhecimento facial está presente em todos os estados, incluindo pelo menos 195 projetos no campo da segurança pública. Além disso, o estudo lançado pela pesquisa Panóptico do Centro de Estudos de Segurança e Cidadania (2019) aponta que entre 2019 e 2022 foram identificados 509 casos de pessoas presas e atingidas pelo sistema. Observa-se essa tendência também em outras cidades da América Latina, como Buenos Aires, Córdoba, Mendoza, Lima e Coahuila (RODRIGUEZ, 2019).

No campo da segurança pública as iniciativas avançaram respaldadas por regulamentações, como por exemplo a Portaria no 793, de 24 de outubro de 2019,

que previu financiamentos específicos via Fundo Nacional de Segurança Pública para a implementação do uso de reconhecimento facial para ações voltadas ao enfrentamento da criminalidade. Este é um marco jurídico emblemático que impulsiona a política de segurança tecnológica vigente, inclusive o surgimento do Termo de Cooperação Técnica que deu origem ao projeto piloto no Rio de Janeiro. Nesse caso, assim como em outros, observamos implementações pontuais e fragmentadas territorialmente que correm o risco de incentivar o uso da tecnologia sem o devido debate e consideração dos riscos de violação de direitos, inclusive da privacidade, de vigilância e outros possíveis efeitos controversos. Essa questão deve ser contextualizada em âmbitos já marcados por violência, abusos e falta de direitos, como no caso da cidade do Rio de Janeiro.

Entre 1982 a 1995 houve um aumento exponencial do uso de câmeras, tornando-se uma ferramenta e estratégia para enfrentar a insegurança pública e, mais recentemente, para combater o terrorismo (LEITE; BONAMIGO; MELGAÇO, 2017). O estado do Rio, mas principalmente a cidade, sempre foi um lugar estratégico para experimentações políticas, dentro das quais podemos incluir também experimentações no campo da segurança pública. Durante os anos 90, o Rio passou por vários episódios violentos, o que fez com que a cidade fosse demarcada por uma divisão entre o morro e o asfalto (LEITE 2001). Se por um lado viver em favelas significa conviver com tiroteios em espaços públicos a qualquer hora, mortes, torturas, tráfico de drogas, prisões arbitrárias, invasões de habitação (LEITE, 2017) o asfalto é tudo aquilo que se distancia deste espaço. É nesse contexto de experimentações que queremos situar o uso do sistema reconhecimento facial, hipotetizando que se trate de mais um sistema de marginalização e perseguição social.

Devemos contextualizar a implementação dessa tecnologia numa realidade de exacerbada violência social que se expressa em elevados indicadores epidemiológicos e criminais que podem ser comparados com países que estão em situação de guerra (MATTOS ROCHA & MOTTA, 2020). De acordo com o relatório divulgado pelo Fogo Cruzado, no primeiro ano da pandemia da covid-19, 2098 pessoas foram baleadas, com média de 3 tiroteios por dia e 5 baleados a cada 24 horas, mesmo com a ADPF (Arguição de Descumprimento de Preceito Fundamental) das Favelas 635 (que estabelece a proibição de operações policiais em favelas durante a epidemia. É importante ressaltar que parte desses confrontos resultam em

mortes em ações policiais. No primeiro semestre do mesmo ano, após uma operação policial, foram mortas 28 pessoas, configurando a operação policial mais letal do Rio de Janeiro, ficando conhecida como Chacina do Jacarezinho com inúmeras violações de direitos humanos. Ao todo, em 2020, foram 2791 tiroteios e 37 chacinas que deixaram 595 mortos e 543 feridos, incluindo crianças e adolescentes⁵.

As balas perdidas são as consequências mais cruéis. De 2016 até novembro de 2022, 1000 pessoas foram vítimas desta letalidade na Região Metropolitana no Rio. Dentre esses anos, destaca-se o ano de 2018, quando 252 pessoas foram vítimas de balas perdidas, período de Intervenção Federal⁶. Ou seja, quando o assunto é a cidade do Rio de Janeiro, pode-se notar que os conflitos armados extrapolam os crimes comuns. Além disso, é necessário destacar que a violência afeta a população de forma totalmente desigual em função de gênero, raça e regiões urbanas.

Nesta conjuntura surgem os estigmas sobre os morros e as favelas sendo indicados como principais responsáveis pela insegurança e a violência urbana. Estamos falando de um estigma que marca também as massas urbanas mais pobres e marginalizadas, transformando-as em perigosas e controláveis (VALLADARES, 2005). Tais estigmas sustentam a segregação material e simbólica desses territórios levando camadas médias e altas a demandarem por ordem pública. Não por acaso, a alocação da força policial nas entradas desses territórios e a maneira como a vigilância é conduzida nos limites dos trânsitos dos moradores pelos bairros, é um padrão de política de segurança pública no Rio de Janeiro (LEITE, 2001).

Quando o conflito social é apresentado como uma guerra, inclusive com o apoio da mídia, são legitimadas e autorizadas medidas excepcionais e estranhas à normalidade institucional e democrática. Nos parece que a cidade do Rio de Janeiro

⁵ Cf: Grande Rio tem média de 15 tiroteios por dia, diz Fogo Cruzado; quase 600 pessoas morreram este ano. Disponível em: <<https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/07/12/fogo-cruzado-tiroteios-semester.ghhtml>>. Acesso em: 30 jun. 2023.

⁶ Cf: Fogo Cruzado, em 6 anos, mil pessoas foram atingidas por balas perdidas, 229 morreram, “infelizmente esta longe de acabar”, diz mãe de Agatha Felix. Disponível em: <<https://g1.globo.com/rj/rio-de-janeiro/noticia/2023/01/11/fogo-cruzado-em-6-anos-mil-pessoas-foram-atingidas-por-balas-perdidas-229-morreram-infelizmente-esta-longe-de-acabar-diz-mae-de-agatha-felix.ghhtml>>

funciona como um verdadeiro laboratório de segurança pública, servindo de modelo de ocupação de territórios. Há aproximadamente 20 anos segue-se uma política de patrulhamento das favelas cariocas em carros blindados adaptados para uso militar (caveirão), helicópteros blindados, fuzis e outras tecnologias que só se usam em uma situação de guerra (MAGALHÃES, 2021). A cidade é teatro de uma praça de guerra mediante o uso de estratégias de combate e terror, ocupação territorial e apreensão do potencial inimigo empregando uma força militar máxima.

Isso resulta em altas taxas de homicídio de jovens (envolvidos ou não com o tráfico) que habitam nestes territórios e elevado índice de letalidade policial (LEITE, 2001). Só no ano de 2019 foi registrado o maior número de mortes por policiais na história do Rio de Janeiro (CANO, 2003), mostrando a persistência da repressão sobre a população negra e periférica apesar da comprovada ineficiência da política de segurança baseada no uso da força para o enfrentamento da criminalidade. Esse incremento no ano de 2019 tem a ver com a escolha deliberada do governador eleito, Wilson Witzel, pela política do confronto e do extermínio (MAGALHÃES, 2021).

Tais medidas excepcionais também contribuem para o surgimento de grupos paramilitares/milícias que crescem justificados pelo discurso de combate às drogas e ao crime organizado (MOTTA ROCHA; BAZONI DA MOTTA, 2020). As milícias, assim como os traficantes de drogas, fazem uso do controle territorial armado com um modelo de governança muito bem definido compondo a paisagem urbana. Sua estratégia de controle do território inclui: coagir o comércio local com taxas para exploração econômica; fornecer redes de canais de tv, água e luz; usar a violência (CANO; DUARTE, 2012). Segundo o Ministério Público Federal, entre 2010 e 2017, as milícias duplicaram sua área de atuação⁷, lembrando que os policiais que patrulham um determinado espaço muitas vezes compõem os grupos de milicianos (MAGALHÃES, 2021).

O ponto que queremos destacar é que qualquer intervenção na segurança pública deveria ser contextualizada e pensada a partir desta conjuntura marcada por

⁷Cf: Violência policial não diminuiu a ocorrência de crimes no RJ, aponta estudo do Ministério Público. G1. Disponível em: <<https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/09/29/violencia-policial-nao-diminui-ocorrencia-de-crimes-no-rj-aponta-estudo-do-ministerio-publico.ghtml>>. Acesso em: 13 abr. 2023.

conflitos sociais. Por isso, na análise desse contexto de guerra devemos situar o avanço autoritário e violento de novas tecnologias, como a implementação do sistema de reconhecimento facial com videomonitoramento, que pode aumentar a vigilância em massa, a identificação e o monitoramento de comportamentos (MONDEGO, 2019).

A conjunção destes pressupostos leva-nos a refletir sobre os impactos que geram sobre as normas socialmente estabelecidas na autorregulação da vida pública, o que pode desrespeitar a relação do Estado com os cidadãos e os valores culturais que se expressam nos espaços públicos. O reconhecimento facial, assim como o sistema de videomonitoramento, evoca uma espécie de onipresença de quem vigia, cria uma permanente exposição de quem está sendo observado, assim como legitima o controle baseado na força. Além disso, essa tecnologia possibilita a concretização de novas dinâmicas de controle do espaço público a partir, entre outros, de sua lógica algorítmica e do regime e uso dos dados.

O Brasil vem seguindo uma tendência mundial de implementação de câmeras de reconhecimento facial na segurança de forma desenfreada. Supostamente o setor público deveria preservar o interesse da sociedade, porém, pouco tem se atentado para os riscos e o impacto dessa tecnologia na violação de direitos, visto que não há hoje prestação de contas e de dados estatísticos consolidados, inclusive sobre o tratamento de dados pessoais. Existe o risco que as câmeras com sistema de reconhecimento facial agravam a situação de guerra e de disciplinamento dos mais pobres em uma cidade cada vez mais desigual e violenta (MATTOS ROCHA; BAZONI DA MOTTA, 2020). Diante do novo cenário de adoção progressiva e iminente de uma tecnologia que apresenta riscos, também seus pontos positivos ainda não foram debatidos e consolidados. Isso se dá num contexto opaco em relação aos resultados e à eficácia no reconhecimento.

Os erros do sistema, o risco de racismo algorítmico e a segurança no tratamento dos dados são questões centrais, inclusive para avaliar e compreender os efeitos no espaço público. Primeiro, a implementação do reconhecimento facial torna-se um desafio considerando também as elevadas taxas de erro do sistema. De acordo com o levantamento da Rede de Observatório de Segurança, 90,5% das pessoas presas pelo sistema eram negras. A nível nacional, o Estado que lidera é a Bahia com

51,7% das prisões e em segundo o Rio de Janeiro com 37,1%, seguido por Santa Catarina (7,3%) e Paraíba (3,3%)⁸. Um caso emblemático é o de uma mulher que foi detida por engano em Copacabana, depois das câmeras darem como positivo um quadro de foragida⁹. É questionável o fato de pessoas sem antecedentes criminais terem sua imagem no banco de dados de suspeitos pela política, sem contar que uma prisão neste caso pode muitas vezes passar por violações de direitos humanos.

Não é surpresa também que a base de dados que treina o sistema de reconhecimento facial é composta por imagens que não refletem a matriz étnico-racial da sociedade brasileira. Em 2018 foi identificado, por exemplo, que os softwares de reconhecimento facial cometem erros ao identificar mulheres negras em 34,7% das vezes, enquanto para homens brancos essa taxa de erro cai para 0,8% (BUOLAMWINI et al., 2018). O uso da tecnologia levanta, portanto, questionamentos quanto à reprodução de opressões e à manutenção do aumento da população carcerária, considerando que o Brasil possui a terceira população carcerária do mundo com 773 mil pessoas¹⁰

Em vista disso, Silva (2019) aplica o conceito de racismo algorítmico para caracterizar o breu por cima dos aspectos raciais da tecnologia digital, a partir da ideia de que os algoritmos não são neutros e, ao contrário, reproduzem opressões. Diferentes autores (LOHR, 2018; NAKAMURA, 2008) apresentam a perspectiva de que os erros da tecnologia não são apenas naturais, mas sim discriminatórios. Por isso, numa realidade em que a população negra vivencia diariamente um genocídio (NASCIMENTO, 1978), é primordial que haja uma análise sobre as possíveis implicações do reconhecimento facial no que tange às violações contra grupos discriminados (MELO; SERRA, 2022).

⁸Cf: 90% das pessoas presas por reconhecimento facial são negras, diz estudo – CESEC. Disponível em: <<https://cesecseguranca.com.br/reportagens/90-das-pessoas-presas-por-reconhecimento-facial-sao-negras-diz-estudo/>>. Acesso em: 12 jul. 2023.

⁹Cf: Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. Disponível em: <<https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>>. Acesso em: 12 jul. 2023.

¹⁰ 10Cf: Dados sobre a população carcerária do Brasil são atualizados. Serviços e Informações do Brasil. Disponível em: <<https://www.gov.br/pt-br/noticias/justica-e-seguranca/2020/02/dados-sobre-populacao-carceraria-do-brasil-sao-atualizados>>. Acesso em: 19 abr. 2023.

Outra questão que deve ser encarada é quem deve ter acesso aos dados sensíveis do cidadão. A segurança dos dados é de suma importância para preservar a privacidade, ainda mais em contextos em que existem abusos policiais e envolvimento com organizações criminosas que controlam os territórios periféricos. Além disso, pode ser questionado o processo de privatização na gestão do sistema. No Rio de Janeiro, por exemplo, a adoção das câmeras de reconhecimento foi realizada pelo Governo do Estado em parceria com as empresas Oi e a chinesa Huawei, sendo que a Oi já foi multada por venda de dados de clientes¹¹ e a Huawei está sendo banida em diversos países por conta da suspeita de auxiliar o governo chinês em espionagem dos cidadãos¹².

As questões acima citadas possuem relevância pública situando o reconhecimento facial como uma tecnologia que exige regulamentação (LEMOS, 2021). Apesar disso, o que vemos é um crescimento de um padrão de implementação na segurança pública através de testes, chamados de “projetos pilotos”, que prevê a implementação sem que direitos sejam necessariamente tutelados. Além disso, por serem territorialmente pontuais e fragmentados, impactam de forma seletiva o espaço público da cidade.

Podemos interpretar esse processo de expansão e implementação tecnológica como iniciativas que intensificam o controle territorial e o processo de militarização urbana. O reconhecimento facial se insere, assim, num processo de controle territorial e do espaço público para além das fronteiras da favela e das periferias. Trata-se de um modelo de política de segurança pública baseado na capacidade de ação, armamento e liberdade de atuação para garantir o controle militarizado do espaço público, um espaço que se torna cada vez mais controlado por sistemas algorítmicos que operam de forma opaca como caixas-pretas segundo uma lógica tecnicista de gerenciamento dos sujeitos criminosos (KRAUS et al, 2022).

¹¹Cf: Oi é multado em R \$3,5 milhões por vender informações de clientes. Disponível em: <<https://veja.abril.com.br/economia/oi-e-multada-em-r-35-milhoes-por-vender-informacoes-de-clientes/>>. Acesso em: 1 abr. 2023.

¹²Cf: A Huawei é acusada de roubar segredos comerciais para espionar o governo do Paquistão. Disponível em: <<https://g1.globo.com/economia/tecnologia/noticia/2021/08/16/huawei-e-acusada-de-roubar-segredos-comerciais-para-espionar-governo-do-paquistao.html>>. Acesso em: 1 abr. 2023.

O tema de segurança pública no estado do Rio de Janeiro é tão complexo que não pretendemos esgotá-lo no presente trabalho, porém, o que é interessante observar é como as sucessivas ondas de megaeventos esportivos e culturais trouxeram novas ferramentas para “solucionar” a questão da segurança pública, favorecendo a militarização das suas forças policiais, a politização de suas forças armadas, a perpetuação da violência como forma de controle sobre o território mediante uma nova sofisticação tecnológica.

Nesse contexto, espaços públicos geridos pelo setor privado e mediados por tecnologias com a promessa de neutralidade e objetividade maquínica vem compondo a paisagem urbana contemporânea. Contudo, estudiosos apontam que tais medidas podem tornar os espaços públicos carentes de urbanidades, ou seja, que se tornam corporativos, artificiais e esteticamente semelhantes, ou seja, sem vida (FIRMINO, 2017). O sistema que antes era usado para deixar os lugares mais seguros, protegidos e “limpos” mediante barreiras físicas, sensores, cercas eletrônicas e muros altos de concreto, agora é renovado pela ação das câmeras com sistema de reconhecimento facial. O ponto é que essas formas de vigilância e securitização normalmente definem não somente os limites legais, mas fortalecem as fronteiras territoriais e de exercício do poder (FIRMINO, 2017).

Também é importante considerar que se trata de um sistema que é cada vez mais utilizado e ampliado¹³, correndo o risco que os problemas acima apresentados se ampliem. O cidadão dessa cidade está submetido a um marcapasso tecnológico parcial que pode acentuar o disciplinamento e o controle limitando a vivência pública. Nesse contexto, surge a seguinte pergunta norteadora da pesquisa: quais os impactos socioespaciais do uso crescente da tecnologia de reconhecimento facial na segurança pública? Diante disso, escolhemos como objeto empírico de análise a implementação do projeto piloto de reconhecimento facial na segurança pública no Rio de Janeiro e a sua relação com os espaços videográficos monitorados e a sociedade.

¹³FERREIRA, Lola. Jacarezinho: RJ prevê câmeras para reconhecimento facial em ocupação.

Uol.com.br. Disponível em:

<<https://noticias.uol.com.br/cotidiano/ultimas-noticias/2022/01/19/reconhecimento-facial-jacarezinho.htm>>. Acesso em: 14 jul. 2023.

1.2. OBJETIVOS

O objetivo geral deste trabalho é realizar uma análise socioespacial do projeto piloto no Rio de Janeiro

Os objetivos específicos são:

1. Definir as características do sistema de reconhecimento facial evidenciando a sua relação com a tecnologização e militarização do espaço público no Rio de Janeiro;
2. Mapear as etapas da tecnologização da política de segurança pública no Rio de Janeiro;
3. Definir as características do Projeto Piloto do Rio de Janeiro (papel dos atores, distribuição geográfica, funcionamento do sistema) como da política de reconhecimento facial no Rio de Janeiro;
4. Realizar uma análise socioespacial do projeto piloto

1.3. METODOLOGIA

A metodologia adotada nesta pesquisa segue uma abordagem multidisciplinar, integrando métodos qualitativos e quantitativos para compreender a interseção entre o sistema de reconhecimento facial e as políticas de segurança pública no Rio de Janeiro. A pesquisa foi dividida em quatro etapas principais, cada uma abordando diferentes aspectos da análise, desde a construção do referencial teórico até a investigação empírica.

ETAPA 1: Levantamento Bibliográfico

O primeiro passo consistiu no levantamento bibliográfico abrangente para embasar teoricamente a pesquisa. Foram consultadas bases de dados acadêmicas, como Periódicos da Capes e Google Scholar, para selecionar estudos que abordassem os temas centrais: reconhecimento facial, políticas de segurança pública, espaço público e militarização urbana. As palavras-chave utilizadas incluíram: “facial recognition”, “public security policies”, “urban militarization”, e “public space”.

O objetivo dessa etapa foi estruturar o arcabouço teórico que servirá como fundamento para a análise crítica do sistema de reconhecimento facial. Além de artigos acadêmicos, também foram consultados relatórios de ONGs, estudos de casos internacionais, e documentos técnicos relacionados ao uso de tecnologias de vigilância.

Esse levantamento forneceu uma base sólida para compreender as dinâmicas históricas e sociais relacionadas à militarização dos espaços públicos no Brasil e em outros contextos globais. Também possibilitou identificar as lacunas nas pesquisas anteriores, permitindo direcionar o foco da investigação para as especificidades da implementação no Rio de Janeiro.

ETAPA 2: Levantamento de Estudos e Documentos sobre Tecnologia na Segurança Pública no Rio de Janeiro

A segunda etapa consistiu no levantamento de documentos oficiais e estudos relacionados à incorporação de tecnologias no âmbito da segurança pública do Rio de Janeiro. Foram analisados relatórios governamentais, contratos públicos, termos de cooperação técnica, e audiências públicas para compreender o contexto de implementação do projeto de reconhecimento facial. Esses documentos foram obtidos através de pedidos via Lei de Acesso à Informação (LAI) e consultas ao Portal da Transparência, além de registros públicos de debates legislativos e entrevistas com especialistas.

Essa etapa teve como objetivo mapear o processo de evolução tecnológica na segurança pública da cidade, detalhando as políticas e estratégias adotadas pelo governo para introduzir o sistema de vigilância por reconhecimento facial. Além disso, buscou-se identificar os atores envolvidos, como empresas contratadas, órgãos públicos responsáveis pela gestão do sistema e associações da sociedade civil que participaram do debate público.

ETAPA 3: Análise do Projeto Piloto de Reconhecimento Facial

A terceira etapa envolveu a análise detalhada do projeto piloto de reconhecimento facial implementado no Rio de Janeiro. Essa fase incluiu a coleta de dados e informações a partir de documentos oficiais, relatos da mídia, e entrevistas com atores chave, como representantes de ONGs, movimentos sociais, e acadêmicos

do campo da segurança pública. A análise buscou investigar o funcionamento técnico, a distribuição geográfica das câmeras e o papel dos atores envolvidos na gestão do projeto. Foram considerados dados sobre operações policiais, abordagens e prisões realizadas com base no uso da tecnologia.

Embora o projeto piloto no Aeroporto Santos Dumont tenha sido uma das primeiras implementações no Rio de Janeiro, foi observado que o ambiente controlado do aeroporto não reflete as dinâmicas sociais mais complexas presentes em espaços públicos de bairros periféricos e centrais da cidade. Por isso, a pesquisa se concentrou em áreas urbanas abertas, como Copacabana, Ipanema e Maracanã, locais onde o impacto do reconhecimento facial na vida cotidiana e nas dinâmicas de controle social são mais visíveis.

ETAPA 4: Análise Socioespacial

Na quarta etapa, foi realizada a análise socioespacial do projeto piloto, a partir de uma abordagem crítica fundamentada em uma estrutura multidimensional (Abello Colak, Lombard & Guarneros-Meza, 2023). A análise foi realizada a partir de quatro perspectivas analíticas:

- **Segregação e Fragmentação Urbanas:** Essa categoria investigou como a implementação do sistema de reconhecimento facial contribui para reforçar a segregação territorial, aprofundando as disparidades entre áreas formalizadas e periféricas. A militarização e a vigilância intensificam a desigualdade espacial, criando "zonas de segurança" em áreas de interesse econômico enquanto reforçam a marginalização de territórios populares.

- **Estigmatização Territorial:** Essa análise focou em como o reconhecimento facial pode perpetuar a criminalização de determinados territórios, especialmente favelas e áreas pobres, associando-as à insegurança. O sistema de vigilância, ao ser amplamente utilizado nesses locais, reforça preconceitos e discriminações já enraizadas, intensificando o estigma social contra seus moradores.

- **Inseguranças Sobrepostas e Especializadas:** Considerou-se como o reconhecimento facial intensifica a percepção de insegurança entre grupos vulneráveis, ao amplificar o controle populacional e criar um ambiente de vigilância constante. A presença do sistema em espaços públicos modifica a forma como as

peessoas vivenciam a cidade, criando dinâmicas de medo e autocensura, especialmente entre a população negra e periférica.

- **Lutas Territoriais:** Esta categoria investigou as disputas pelo controle do território entre o Estado e grupos sociais, especialmente em áreas onde o sistema de vigilância é mais intensivo. O reconhecimento facial levanta questões sobre privacidade, liberdades individuais e direitos humanos, particularmente em espaços onde há forte resistência da população local contra práticas repressivas e abusivas.

Nessa etapa, foram realizadas entrevistas com moradores e detidos/afetados pelo sistema - para compreender as percepções, sentimentos de segurança e eventuais impactos na vida cotidiana - e com especialistas em segurança pública. Além disso, realizamos observações durante os meses de Fevereiro a Setembro e fizemos um trabalho de observação nas áreas atingidas pelo projeto piloto. Escolhemos como pontos de observação (Figura 1 e 2):

- Leme, o bairro de residência de pessoas com grande poder aquisitivo, que se encontra na entrada das favelas do Chapéu-Mangueira e Babilônia.;

- A entorno da divisa entre Ipanema e Copacabana cuja as características são áreas residenciais residências e os arredores da subida da favela do Pavão-Pavãozinho e Cantagalo, próximo ao Posto 6;

- Os arredores do hotel Copacabana Palace e a orla da praia;

- Metro da Cardeal Arcoverde,

- Arredores do Metrô Siqueira Campos e da Ladeira dos Tabajaras e Morro dos Cabritos.

- Entorno do estádio do Maracanã e seus acessos, incluindo os dois sentidos da Avenida Maracanã, entre a Rua São Francisco Xavier e a Av. Rei Pelé;

- o Viaduto Oduvaldo Cozzi e seus acesso, incluindo as entradas e saídas das estações de metrô e trem de São Cristóvão;

- Avenida Professor Manoel de Abreu e os arredores da Universidade Estadual do Rio de Janeiro;

- Acesso da favela do Metrô do Maracanã, Metrô-Mangueira, Mangueira I e II, incluindo os condomínios do Minha Casa Minha Vida.

Figura 1 - Mapa de Observação em Copacabana e Ipanema



Figura 2 - Mapa de Observação na região do Maracanã



Os critérios de seleção dos locais nos mapas acima foram estabelecidos a partir de uma observação inicial dos bairros, com o objetivo de identificar os locais com maior concentração de câmeras de vigilância. Além disso, foram coletadas informações de canais de notícias e realizadas entrevistas com especialistas para compreender o fluxo de movimentação de pessoas e a diversidade de usos dos locais selecionados, que incluem áreas residenciais, comerciais, de serviços e de lazer. Também foi levado em consideração a variação de dias e horários para avaliar a relação desses espaços com a vigilância por câmeras, observando os diferentes usos que eram feitos de cada local.

1.3.1 LIMITES DA PESQUISA

Identificamos, ao longo da pesquisa, obstáculos no acesso a dados sobre o projeto piloto, incluindo informações sobre a dimensão técnica e de gestão. Infelizmente, a tentativa de entrevistar representantes governamentais envolvidos no Projeto Piloto não obteve o esperado. Conseguimos preencher parcialmente essa

lacuna entrevistando especialistas na área de segurança pública, incluindo pesquisadores, que conseguiram contatos com gestores em gestões anteriores.

Esses especialistas sinalizam a dificuldade de acesso a dados sobre o projeto, sugerindo que eles podem não estar sendo produzidos. Além de ser uma questão de relevância política, a ausência de dados impede o acompanhamento da política e constitui um limite para a realização da pesquisa. Além disso, tentamos realizar as entrevistas no CICC. No entanto, sempre nos deixavam esperando no saguão e a secretaria informava que pegariam nosso contato para comunicar a disponibilidade, mas isso nunca aconteceu. Por último, tentamos requerimentos de informação pelo gabinete da Deputada Estadual Dani Monteiro e pelo Portal da Transparência. Solicitamos informações sobre o número de prisões, abordagens e falsos positivos, além de detalhes sobre como o reconhecimento está sendo operacionalizado, para que pudéssemos avaliar a eficiência do programa. No entanto, não obtivemos respostas. A falta de compromisso com as informações nos leva a questionar a ética na implementação do sistema de reconhecimento facial, considerando princípios como transparência e equidade.

1.4 ESTRUTURA

A dissertação então se estrutura em 3 capítulos, além do capítulo da introdução. O capítulo 2 “Reconhecimento facial e a militarização do espaço público” aborda a base conceitual central da pesquisa, ou seja, a descrição das características do sistema de reconhecimento facial, o seu funcionamento e o que apresenta de novo em relação ao videomonitoramento. O foco da questão é trazer para o centro do debate os mecanismos que o sistema de reconhecimento facial e a sua implementação no espaço público vem endereçando em relação às questões técnicas, éticas, jurídicas e sociais, especialmente a partir do seu emprego na segurança pública. Abordarem essas questões segundo a perspectiva da militarização do espaço público. Partindo de uma contextualização em nível local e nacional analisando a sua articulação com a realização dos megaeventos esportivos no Rio de Janeiro.

No capítulo 3, “tecnopolíticas da securitização e militarização: o caso do projeto piloto”, apresento o projeto piloto como política de sistemas de

reconhecimento facial na segurança pública do Rio de Janeiro, cidade que vivencia inúmeros processos de reestruturação e recomposição do espaço público urbano e de reorganização das formas e sentidos do poder nas cidades a partir de políticas piloto. Inserida dentro de dinâmicas para tornar as cidades mais competitivas através de investimentos em projetos “inteligentes” que motivam processos de tecnologização da segurança pública no Rio de Janeiro. Abordaremos também a análise do projeto piloto e seu impacto socioespacial, explorando estudos sobre implementações semelhantes em outras localidades, teorias socioespaciais e questões éticas relacionadas ao uso da tecnologia de vigilância. O foco será nas implicações dessa tecnologia para a sociedade e o espaço urbano. Destacamos como os mais pobres acabam sendo inseridos em um contexto de criminalização e demonização, colocando o sistema de reconhecimento facial no centro do debate sobre modelos neoliberais que reforçam o encarceramento em massa, a vigilância e a desvalorização dos direitos. Isso evidencia uma desigualdade urbana baseada no controle e coloca em xeque a justiça social.

CAPÍTULO 2 - RECONHECIMENTO FACIAL E MILITARIZAÇÃO DO ESPAÇO PÚBLICO

Neste capítulo apresento o sistema de reconhecimento facial e as suas características e limites em relação a sua implementação, tentando destacar o que há de novo em relação ao videomonitoramento por câmeras e quais questões e problemáticas éticas, jurídicas e sociais são levantadas pelo uso do sistema para a “garantia” da segurança pública na cidade.

O reconhecimento facial é uma tecnologia biométrica, desenvolvida em 1964 pelo matemático e cientista da computação Woodrow Wilson Bledsoe, o pai do reconhecimento facial. E hoje, é um dos métodos de identificação mais utilizados pelos seres humanos, pois consegue identificar rapidamente qualquer pessoa. Embora reconhecer a face de alguém seja uma tarefa simples para nós, implementar esta tarefa em uma máquina - que pode não somente identificar, mas também perceber o estado emocional de uma pessoa apenas observando a sua impressão (EKMAN, 1993) - pode trazer inúmeros desafios.

No cenário de uma sociedade cada vez mais digitalizada (BISSI, 2018), o nicho tecnológico avança com a inteligência artificial sendo aplicada cada dia mais em nossas vidas, fazendo com que questões éticas a respeito ganhem ainda mais forças e importância. Nesse contexto, as soluções de reconhecimento facial atualmente em uso e descritas ao longo desse estudo empregam elementos de inteligência artificial (IA) que, ao serem treinados para diferenciar e reconhecer partes físicas, podem cumprir determinados objetivos, como por exemplo, identificar rostos e determinar diferenças e semelhanças a partir de enormes bancos de dados de referência (COSTA & KREMER, 2022). É importante evidenciar que todas as experiências se baseiam na identificação de pontos nodais tais como a distância entre os olhos, nariz, ossos laterais do corpo e comprimento do nariz (OKABE E CARRO, 2015; SIMONYAN & ZISSERMAN, 2014; COSTA 2021).

Não há um consenso na literatura sobre o conceito de inteligência artificial, mas Bissi (2018) o caracteriza em linhas gerais como uma reprodução da cognição humana em que aprendizado, memória e processo de tomada de decisão são determinados por softwares computacionais. Sendo assim, trata-se da possibilidade de uma máquina, por meio de algoritmos, aprender a executar tarefas e desenvolver

algum nível de capacidade cognitiva (SILVA & MAIRINK, 2019, p. 65). Assim, a definição de inteligência artificial pode incluir a habilidade de interpretar, aprender corretamente dados externos e alcançar objetivos propostos (KAPLAN & HAENLEIN 2019). Afinal, na sociedade contemporânea os dados estão em todos os lugares (CARVALHO, 2019), sendo cada vez mais coletados, armazenados e processados por inúmeros dispositivos tecnológicos. Dados esses que não seriam capazes de serem processados por seres humanos (STATISTA, [s.d.]), mas que alimentam sistemas de IA, como o reconhecimento facial.

O tal sistema, do ponto de vista técnico, a execução de tarefas de forma automatizada mediante algoritmos de aprendizagem envolve as seguintes etapas: encontrar um rosto na imagem, focar um rosto por vez, compreender os diferentes ângulos e iluminação sob os quais um mesmo rosto pode se apresentar; identificar características únicas no rosto humano que permitam distinguir entre rostos diversos; e, por fim, comparar as características distintivas de um rosto com os rostos constantes no banco de dados e encontrar o nome da pessoa a quem o rosto pertence (ESTEVES et al., 2021). Como exemplo, podemos citar o banco de dados dos estudantes com direito à gratuidade no transporte público.

Mesmo que o principal foco do presente trabalho seja a segurança pública, há uma variedade de aplicativos que operam esse sistema para uso pessoal, monitoramento e aumento de produtividade nas empresas, entre outros (COGNEX, 2013). Desde de 2011, o Instituto Igarapé (2019) monitorou a instalação do sistema de reconhecimento facial em diversas áreas. Um exemplo é o caso do transporte em São Paulo, cujo o metrô passou pela instalação das câmeras com reconhecimento facial em 2017 onde foi possível captar nos 2 primeiros anos mais de 300 mil bilhetes bloqueados por supostamente pertencer a outras pessoas (ESTEVES et al., 2021). Outro exemplo é a cidade de Seabra, que foi escolhida pelo governo da Bahia como uma das 78 cidades a receber sua festejada tecnologia de reconhecimento facial. São oito câmeras cobrindo parte do centro urbano do município (NASCIMENTO, 2023). E o mesmo processo se dá também nos estados do Nordeste, avançando para outros estados como Minas Gerais, Espírito Santo, Pará e o Distrito Federal (NUNES 2019).

O uso de reconhecimento facial para fins de segurança é levantado por muitos ativistas e pesquisadores como algo potencialmente perigoso e que levanta

preocupações sobre a coleta de dados e informações sobre o cidadão, muitas vezes legitimando o seu uso em locais públicos sem estabelecer os limites do seu impacto sobre a população e na participação democrática mais ampla (ZALNIERIUTE, 2021). Por isso, muitos estudiosos argumentam que a tecnologia pode resultar no efeito assustador para aqueles que fazem um discurso divergente. Zalnieriute trará em seu texto alguns exemplos emblemáticos espalhados por cidades no mundo todo evidenciando como o uso de sistemas de reconhecimento facial “durante os protestos de 2020 relacionados ao assassinato de George Floyd” e outros exemplos que contribuem para a sustentação de que de fato, a tecnologia tem sido uma ferramenta que tem impactado o uso dos espaços públicos pela sociedade e a sua organização em todo o mundo.

Ao mesmo tempo em que a popularização das técnicas biométrica é crescente, também a produção bibliográfica sobre o reconhecimento facial avança (OKABE E CARRO, 2015; INDRAWAN et al, 2013, YANG et al 2017), apresentando diferentes aplicabilidades e abordagens analíticas.

Para abordar esses estudos e as análises propostas, podemos pensar no reconhecimento facial como sistema sociotécnico, pois nos possibilita compreender o sistema não apenas como algo técnico para auxiliar os problemas de segurança pública, mas também como um sistema que opera e organiza a sociedade através das suas relações de poder político - público ou privado - e possuem efeitos sociais (prisões por erros, injustiça social, vigilância) (NASSER & EGLER, 2022). Assim, incorporar uma estrutura automatizada nestes contextos requer identificar os tipos de subjetividades que emergem dessas práticas, por exemplo, na construção de subjetividades pacíficas e criminosas dos espaços públicos patrulhados, e reconhecer a limitação do trabalho executado no território pelos oficiais de patrulha nos moldes tradicionais, cuja solução viável passa por remediar tais práticas através de tecnologias que propõem um nível de eficiência e de justiça que nem sempre são comprovados antes de serem colocados em prática.

E como uma rede sociotécnica (LATOUR, 2001) as câmeras com sistema de reconhecimento facial operam como dispositivos de controle e vigilância que só se efetiva com colaboração entre diferentes entidades e numa atuação cujo o algoritmo é capaz de interferir na ação humana evidenciando uma necessidade de atores

humanos e não humanos (LATOUR, 2006) produzindo três deslocamentos: primeiro, as câmeras passam a ser um novo agente produtor de determinados efeitos; segundo, este novo agente se encontra espalhado e ocupando espaços públicos como ruas, praças e, por último, a onipresença das câmeras substitui a presença da polícia (LATOUR, 2001), sendo o controle e a vigilância uma consequência desta ação sociotécnica (LEITE RIBEIRO PEDRO, SALETE BONAMIGO, MELGAÇO, 2017).

Existem diversas possibilidades narrativas e de discurso que retificam e fetichiza a tecnologia de vigilância e gestão como soluções para quase todos os aspectos da vida urbana contemporânea, depositando na eficiência de processos a marca da cidade neoliberal (FIRMINO, 2017), que carrega consigo efeitos controversos, como questões éticas, jurídicas e sociais que desdobra na vigilância, nos dados coletados, na imprecisão do sistema e na reprodução de injustiças sociais.

2.1. DADOS, VIGILÂNCIA E CONTROLE SOCIAL

Com as câmeras de vigilância (CCTV) e o reconhecimento facial, mesmo operando um sistema de vigilância centralizado nas mãos de empresas privadas e do Estado - estilo panóptico, o poder sobre o outro é alimentado pelas informações adquiridas e acumuladas sobre os indivíduos de forma quase imperceptível.

A extração de dados, constante e sem consentimento, gera o que o que Zuboff (2015) define como capitalismo de vigilância. A intenção desse trabalho não é explorar esse conceito, mas nos ajuda a compreender melhor o deslocamento que transforma qualquer pessoa em um sistema móvel de vigilância, revelando um caráter antidemocrático (BRUNO et al., 2018) que avança na medida que as receitas de uma super vigilância se tornam um mercado lucrativo que cresce contribuindo para aumentar os riscos e as mais recentes formas de securitização de espaços sejam eles privados ou públicos. Os artifícios de securitização são capazes de promover uma naturalização e banalização da linguagem física-material-arquitetônica da tecnologia na cidade, de maneira que banalizamos o uso de cercas elétricas, câmeras, guaritas - o que é fundamental para a compreensão das interações territoriais analisadas neste texto, onde as diferentes camadas superpostas de

território na cidade, estão delimitadas muitas vezes pela influência da propriedade privada que se sobrepõem ao domínio público (FIRMINO, 2017).

A questão é que tais novas tecnologias são a porta de entrada para novas oportunidades de monetização. A lógica de acumulação, atualmente institucionalizada, acaba por “produzir agenciamentos em hiperescala de dados objetivos e subjetivos sobre indivíduos e seus habitats no intuito de conhecer, controlar e modificar comportamentos para produzir novas variedades de mercantilização, monetização e controle” (ZUBOFF, 2018, p. 18). A questão é que esse processo se beneficia da captura de análise de dados do comportamento alheio, em prol da obtenção de lucro, o que favorece uns em detrimento de outros. Muitas das práticas associadas à capitalização desafiam normas sociais associadas à privacidade, sendo contestadas como violações de direitos e leis.

Além do mais, na sociedade normalmente não existe uma percepção da vigilância e dos dados coletados “na medida que os espaços de vigilância aumentam, o privado encolhe” (GRAY, 2002). O desafio está em garantir que as soluções tecnológicas não se transformem em ameaças quando são apresentadas para a solução de problemas. Entretanto, os efeitos de uma vigilância generalizada estão para além dessas fronteiras, como por exemplo, os problemas decorrentes das possibilidades de erros de dados que está ligado à privacidade, tornando esse um dos casos que mais chama a atenção em termos de reconhecimento facial. Outra questão relevante é que, em muitos casos, esses sistemas são operados de maneira unilateral e fora dos mecanismos democráticos legítimos, desrespeitando a escolha do consumidor e a reciprocidade (BRUNO et al., 2018).

Lyon (2001) ressalta que a vigilância articula ideias ambíguas entre o cuidar e o controlar. Ou seja, vincular identidades ao anônimo na multidão amplifica a possibilidade de vigiar todos e dá poder de vigiar quem é o outro em nome da segurança. Hoje, com as câmeras e o sistema de reconhecimento facial, a ideia de cuidar e vigiar se misturam na relação de copresença. Enquanto Foucault (1979) já chamava a atenção para o surgimento do panóptico - entendido como uma arquitetura que permite que um único vigilante observe todos os prisioneiros a partir de uma torre central - nos dias de hoje não existe um ponto único de observação. Existem múltiplos pontos invisíveis ou imperceptíveis de vigilância (ZUBOFF, 2015).

A natureza da vigilância ostensiva vem sendo profundamente alterada pela introdução de sistemas de reconhecimento facial acoplados às câmeras de CCTV (NORRIS, 2003; FONTES & LUTGE, FIRMINO, 2017). Uma coisa é pensar câmeras de videomonitoramento que não atuam sozinhas e que só fazem sentido quando há funcionários responsáveis para monitorar as operações, outra é a modernização desse videomonitoramento com sistemas de reconhecimento facial que automatiza parcialmente esse processo, ao mesmo tempo em que aprimora os moldes de observação, interpretação e resposta. Não se trata de uma automatização completa porque, por exemplo, imagens são ainda interpretadas por operadores da tecnologia que podem ou não agir reproduzindo estereótipos, demonstrando a importância do olhar humano para validar sujeitos observados (OLIVA; PÁTARO, 2017). Ou seja, é fundamental compreender que as imagens são interpretadas por humanos que possuem uma forma enviesada de olhar tanto para aquilo que é exposto quanto para o oculto.

No caso do videomonitoramento, em sua maioria, o padrão de comportamento de um operador inclui controlar a câmera e analisar a imagem observada em tempo real. Nesse caso, o sentido imagético só existe graças àquele que registra, observa e interpreta. Somado a isso, o próprio registro do vídeo é uma interpretação visual e que, independente de ser considerado um testemunho, é passível de uma interpretação carregada de visões culturais (OLIVA; PÁTARO, 2017). A modernização do videomonitoramento com sistema de reconhecimento facial automatiza o processo, sofisticando os moldes de observação, interpretação e resposta.

Com o reconhecimento facial, a captura da imagem do rosto torna-se um aspecto central automatizado por algoritmos, que, ao serem alimentados por banco de dados e por um crescente cruzamento de informações, revelam a possibilidade de uma operação multifuncional em relação às imagens coletadas. Isso aumenta exponencialmente o seu efeito panóptico (NORRIS, 2003). Isso acontece num contexto em que é descartado o tempo necessário de um olhar humano sobre esse processo de identificação e aperfeiçoando a precisão. Além do mais, mesmo que as imagens sejam defeituosas, parciais e enviesadas, o uso do sistema permanece sendo visto como uma tecnologia promissora, que se materializa na manutenção e

defesa de seu desenvolvimento de modo que se tornem ainda mais automatizados e sofisticados.

Para o funcionamento do sistema reconhecemos que os dados constituem o elemento central para o desencadeamento de mecanismos de vigilância. A falta de consentimento sobre o tratamento de dados biométricos levanta questões de natureza ética, inclusive quando a tecnologia é utilizada na prestação do serviço público, já que o reconhecimento facial traça perfis de indivíduos ao circular no espaço público (RODRIGUES & COSTA, 2019). Banco de dados são, assim, construídos a partir da captura de imagens alegando a justificativa de busca de criminosos, sendo que todos os rostos são gravados (SMITH, 2020). Trata-se de um mecanismo que disciplina as pessoas em movimento, mediante a ação invisível de tecnologias e algoritmos (Ibid).

Além disso, faz-se necessário questionar se existe transparência na coleta de dados, como os dados são gerenciados e de que forma é garantida a proteção, considerando inclusive a onda crescente de parcerias público-privadas que levanta questões sobre os limites no acesso e uso dos mesmos. Observamos, paralelamente ao avanço na implementação do sistema de reconhecimento facial, a dificuldade em formular estratégias que sejam capazes de regular o seu uso, incluindo dos dados. O processo legislativo não acompanha o ritmo dos avanços tecnológicos, levando a uma realidade em que as pessoas são cada vez mais submetidas à vigilância e ao controle político e legal a partir dos dados (RODOTÀ, 2008).

Além das questões inerentes à vigilância, estudos demonstram como essa tecnologia faz parte de nossas vidas, evidenciando suas formas de funcionamento e efeitos do seu uso (KUROIWA & CARRO, 2015 ESTEVES, 2021; CARDOSO, 2018). Esteves (2021), por exemplo, propõe uma análise sobre o uso do sistema de reconhecimento facial, destacando a maneira como funciona a partir da inteligência artificial que, além de efetivar a instauração de sistemas de vigilância, possibilita mecanismos de controle éticos, jurídicos e sociais, como por exemplo, a notória preocupação, entre cientistas sociais e juristas, que o emprego do reconhecimento facial reforce a seletividade penal brasileira, considerando seus vieses quanto à raça, etnia e gênero.

Tecnologias e algoritmos podem se somar a relações sociais opressivas, partindo do princípio de que a tecnologia não é neutra e que carrega consigo a intenção de quem codifica/decodifica. Por isso, é necessário que a sua implementação seja monitorada, desvendando os valores embutidos nesses sistemas (NOBLE, 2018). Dito isto, é importante estar atento para que o dispositivo não opere à serviço da lógica criminalista do Estado, segundo a qual negros e negras são perseguidos e culpados. Novos desafios surgem num contexto em que, segundo Dados do Instituto Criminalistas-TJSP, magistrados condenam proporcionalmente mais negros do que brancos, sendo que só na cidade de São Paulo 71% dos negros julgados foram condenados por todas as acusações feitas (BARCELOS, 2019). Um outro exemplo está no Rio de Janeiro, com quase 80% dos casos de homicídio associado a ações policiais são negros, segundo os dados da Rede de Observatório da Segurança (2021). O dispositivo de reconhecimento facial pode produzir para aqueles que possuem pele escura erros ainda maiores devido à qualidade do banco de dados fornecida ao sistema (NANAVATI; THIEME, NANAVATI, 2002). Desta maneira, a disseminação digital como exercício do poder emitido pelas tecnologias de vigilância, pode produzir sobre os corpos negros uma “verdade” sobre a sua identidade, gerando ainda mais uma violência produzida onde brancos são a norma. (GORDON, 1980).

Outra questão problemática está no fato da tecnologia operar a partir da visão daqueles que a vê como promissora, definindo parâmetros que influenciam a performance, do reconhecimento facial em ambientes não controlados (ESTEVES, 2021). O “ambiente não controlado”¹⁴ refere-se à captura de imagens em contextos espontâneos da vida cotidiana (ruas, praças e outros espaços de grande circulação de pessoas). Nesses espaços da vida cotidiana, os sistemas de inteligência de vigilância e controle não definem explicitamente quem são pessoas boas ou ruins, mas definem e limitam o direito delas de acessá-los (NORRIS, 2003).

O estudo realizado por Kuroiwa e Carro (2015) apresenta, a partir de métodos técnicos, os resultados do uso de sistemas de reconhecimento facial em um projeto cuja realidade de testes é bem definida, com um público específico, banco de dados enxuto em ambiente facilmente controlado cujos resultados dependem -

¹⁴ tradução livre do termo unconstrained environments (MOU, 2020)

diferentemente dos sistemas em ambientes “não controlados” - do ambiente a ser controlado. Porém, mesmo o ambiente de operação do sistema sendo controlado, por exemplo para controlar o acesso de alunos nas escolas ou identificar os alunos em aulas online, o sistema encontra falsos positivos, dependendo da qualidade das imagens do banco de dados, a variação de ângulos, iluminação do local vigiado, qualidade das imagens colocando a taxa de confiança abaixo do esperado.

Existem outros estudos que corroboram a ideia de que a tecnologia apresenta limites em termos de precisão do sistema. Diniz (2013) ressalta como o sistema opera em ambientes virtuais a partir de dois métodos: a análise de componentes principais (PCA) - onde o algoritmo é programado para extrair informações mais relevantes e únicas sobre a identidade de alguém - e o Eigenfaces (autofaces) - que busca diretamente um conjunto de características capaz de diferenciar uma face de outras. Ambas as abordagens mostram resultados imprecisos devido às condições de captura do reconhecimento facial em relação ao banco de dados e à qualidade das imagens, o que evidencia limites quanto a sua operacionalização e a necessidade de aperfeiçoamento.

O uso da tecnologia se fundamenta na ideia que corpo de uma pessoa ou os perfis comportamentais da mesma podem ser usados para identificá-la de maneira única e exclusiva através de biometria, gerando e analisando dados fisiológicos ou comportamentais (BISSI, 2018). Por um lado, a biometria fisiológica corresponde ao DNA de cada corpo humano, cuja individualidade dificulta qualquer tentativa de burlar o sistema e de perda de informações no tempo. Por outro lado, a biometria comportamental pode ser alterada de acordo com as variações de estado emocional de cada indivíduo, levando em consideração as mudanças que ocorrem com o tempo, por exemplo, na voz, a coordenação dos dedos, detalhes estéticos, dependendo inclusive da condição psicológica ou mesmo do ambiente (SRIVASTAVA, 2013). Assim, apesar da precisão da tecnologia ser o pilar central para o funcionamento correto do sistema, é fundamental reconhecer a individualidade da identificação do corpo humano, em especial os atributos da face, que têm sido utilizados para identificar e diferenciar pessoas nos dias atuais. Isso significa dizer que mensurar as características dos indivíduos não é uma tarefa fácil, somando a isso os limites de cada dispositivo biométrico.

Uma das ações necessárias para aprimorar a precisão seria a ampliação da base de banco de dados, que implica na expansão ou sofisticação de sistemas de captura e armazenamento de dados, principalmente no que tange à segurança pública. Isso levanta outros questionamentos pois significa expandir formas de vigilância e legitimar eventuais abusos, já que podem ser usadas de maneira discriminatória, reforçando o racismo, a marginalização e criminalização de grupos minoritários (ANTONIO, 2022; BARROS, 2020; MENDES; MATTIUZZO, 2019).

Outra questão relevante é que, além da questão da imprecisão e da vigilância, o uso do reconhecimento facial funciona como um sistema controlador que detecta rostos em lugares públicos (OKABE E CARRO, 2015). Isso compromete a garantia da privacidade na sociedade e sustenta um sistema de injustiças no campo ético e moral (LUDEMIR, 2021), considerando que o sistema é construído a partir das coordenadas e interesses de quem as programou (SILVA & MARINK (2019). O rosto se torna um verificador da veracidade e acaba por dar a abertura a um mecanismo de controle social que tira proveito do poder e da capacidade de segurança para estratégias preventivas de intervenção (NEGISHI, 2013). A avaliação de um suspeito em potencial faz parte de uma comparação ao valor do rosto de alguém, colocando o rosto num contexto de intensificação dos modos de vigilância. Ao capturar inúmeros rostos, a programação permite instantaneamente reconhecer as impressões dos rostos encontrados, indicando uma complexa biopolítica do rosto (SMITH, 2020) que permite que as pessoas sejam identificadas sem possibilidade de questionamento.

Além de estar caminhando na contramão dos princípios básicos de transparência de dados sobre a segurança pública e criminalidade, a localização dessas câmeras no espaço público geralmente são posicionadas muito acima do campo de captura do algoritmo no ambiente de vigilância. e a captura só será possível numa direção a distância, diante disso, fatores como a iluminação, desfoque das imagens a partir das mudanças de movimento somados a um banco de dados que não é composto por imagens capturadas de maneira real e sim imagens capturadas por uma câmera na frente das pessoas (KIM et al., 2018), torna ainda mais complexo o desempenho da tecnologia.

Diante do que já foi exposto, enquanto esse tipo de governança tem contribuído para fortalecer vulnerabilidades faciais - uma vez que o ser monitorado e

controlado compromete um conjunto de direitos, incluindo o de acessar e ocupar espaços de forma anônima -, surgem também artifícios faciais com o intuito de burlar de alguma forma a identificação facial para insurgir aos processos biopolíticos de poder. Por tanto, o rosto se torna uma máscara complexa com diversos significados simbólicos e sociais (SMITH, 2020).

Longe de ser uma análise exaustiva dos mecanismos de controle éticos, jurídicos e sociais desencadeados pela implementação do sistema de reconhecimento facial, as questões abordadas levantam importantes elementos para se pensar instrumentos regulatórios. Assim, como apontado por Esteves (2021), a base normativa não baliza como o sistema deveria ser operado, o nível de transparência, a maneira de lidar com apreensões enganosas e a possibilidade de instaurar auditorias independentes. Além disso, empresas privadas desenvolvem a tecnologia sem parâmetros regulatórios, o que demonstra uma negligência sobre as consequências penais. Considerando o avanço inexorável do sistema, exigir uma resposta dos órgãos de controle é o mínimo, principalmente levando em consideração o nível de novidade e complexidade da Inteligência Artificial.

Existem desafios impostos pelo processamento algorítmico de grandes quantidades de dados, pois isso dificulta a superação de vieses e da falta de transparência sobre os processos de funcionamento das redes neurais. Perpetua-se, assim, a discrepância entre a ampliação no uso do sistema e sua imprecisão, considerando por exemplo que foi alcançado o 90% de erros nas apreensões realizadas no primeiro teste do projeto piloto no Rio de Janeiro.

Diversas pesquisas continuam apontando tais fragilidades (ESTEVES et al., 2021). Além disso, de todos os sistemas biométricos, esse é o que tem as mais altas taxas de falsos positivos - quando a máquina erroneamente identifica a face buscada como sendo aquela de uma pessoa registrada na base de dados - e falsos negativos - quando a face buscada é de uma pessoa registrada na base de dados, mas a máquina não identifica isso. Isso levanta questões para o controle social da tecnologia por parte da sociedade civil e do poder público.

Diante disso, observa-se que onde o Estado está pouco presente e mesmo que estabeleça um lapso de evolução social exige precedentes legais para a sua operacionalização (BRUNO et al., 2018), porém, basta saber se é possível corrigir os

problemas antes que as plenas consequências do projeto de reconhecimento facial se concretizem, pois a implementação do sistema de reconhecimento facial nos espaços de circulação pública tem sido vigiada com reflexões sobre a confiabilidade da tecnologia e ao seu modelo de desenvolvimento (FONTES; LUTGE, 2022). Os aspectos controversos a partir da perspectiva ética, jurídica e social impactam a vida na cidade, tornando o espaço público uma moeda de troca na cidade neoliberal.

2.2 RECONHECIMENTO FACIAL NO ESPAÇO PÚBLICO

O debate em torno das implicações éticas, jurídicas e sociais do sistema de reconhecimento facial revela efeitos na transformação do espaço público, apontando os riscos do determinismo tecnológico (FIRMINO, 2017). Novas formas tecnológicas de controle e vigilância possibilitam e otimizam novas formas de repressão nos espaços urbanos. Por isso, daqui em diante pretende-se chamar a atenção para um outro fenômeno: a militarização do espaço público e do aparato de segurança pública através do sistema de reconhecimento facial.

O espaço se constitui pela maneira como ele é socialmente definido e não por definições espaciais de propriedade (LEFEBVRE, 1991). Desta maneira, o espaço público pode ser considerado palco da vida social urbana e importante lugar para a vida pública e a sociabilidade urbana. O espaço se estabelece numa projeção da humanidade, como sentido de existência e processo de apropriação e compreensão da historicidade do espaço. Este é palanque das principais intervenções políticas, sociais e culturais (FONTES; LUTGE, 2022), constituindo-se como espaço de reunião e associação, expressão e reivindicação. É, inclusive, no espaço público que se manifestam movimentos insurgentes que contestam a política hegemônica, apresentam elevada (vitrine da vida pública) e capacidade mobilizadora. Aqui o conflito e a coesão social entram em negociação, deixando marcas em termos de memória coletiva e luta política emancipatória. A organização espacial é, assim, resultado de dinâmicas de interação e comunicação por compartilhar um mesmo espaço (GOMES, 2018).

Com o uso do sistema de reconhecimento facial na segurança pública, o sentido político de espaço público pode ser rompido. Um primeiro aspecto a ser destacado é a garantia do anonimato como direito que acaba sendo prejudicada pela

ação constante de vigilância. Além disso, as políticas de vigilância pública impactam a interação social urbana do dia a dia, como por exemplo, o uso exagerados de câmeras com sistema de reconhecimento facial, ao substituir as lentes humanas, podem causar uma diminuição da noção de responsabilidade e humanidade no espaço público como ajudar outras pessoas em situações que podem levar o risco de vida em locais onde as câmeras já estão instaladas (GRAY, 2002).

O reconhecimento facial, ao ser apropriado por uma rede de atores hegemônicos, transforma as maneiras como o espaço público e a vida pública são vividos por diferentes classes e grupos sociais (FIRMINO, 2017). Os espaços públicos vem passando por um efeito de neoliberalização que tem como efeito o crescimento dos espaços privados em detrimento dos públicos (ABRAHÃO, 2008), onde o direito privado, estabelecido mediante contratos privados, através desta tecnologia consegue de alguma maneira controlar, limitar e reduzir a maneira como as pessoas em sociedade se comportam.

Desta forma, observamos formas de apropriação do espaço urbano por meio do controle. Dividimos as formas de controle em materiais - pelo uso, por exemplo, de muros, cercas, arames farpados - e imateriais - pelo uso de sistemas integrados, bancos de dados, CCTV com reconhecimento facial, cercas eletrônicas, sensores - que acabam por expandir e reforçar os limites territoriais de exercício do poder (FIRMINO, 2017). Os muros e as grades que separam a convivência na vida pública representam enclaves fortificados (CALDEIRAS, 2001) que são atualizados pelas tecnologias da informação e comunicação. As formas imateriais definem novas formas de segurança e de sistema de controle nos territórios sociopolíticos da cidade, são muitas vezes imperceptíveis e invisíveis, constituindo segundo Firmino (2017), uma segunda camada territorial que é construída de forma digital. Nesse contexto, os espaços mais controlados definem novas formas de ocupação e segregação do território em várias partes intraurbanas.

Com o reconhecimento facial a r(e)produção de classificação social do espaço se torna mais complexa (FIRMINO, 2017), principalmente pela ação algorítmica. A ação algorítmica possibilita o acesso a muitos dados da população e a capacidade de tomar decisões mais rápidas, inclusive no campo da segurança pública. Os espaços passam a ser controláveis e usados como moeda de troca,

principalmente em um contexto onde o Estado está pouco presente sobre a lógica neoliberal.

Apesar dos problemas relativos ao funcionamento do sistema e seus efeitos controversos, a legitimidade e confiança no sistema são determinantes para a sua aceitação ou rejeição. Isso se soma à consideração das atividades policiais enquanto inquestionáveis e legítimas, levando ao apoio de ações de segurança pública, mesmo quando são "problemáticas, inapropriadas ou totalmente erradas" (BRADFORD et al., 2020). A confiança num sistema de controle policial, do qual o reconhecimento facial faz parte, causa uma maior insegurança nos espaços públicos. Assim, a justificativa da geração de espaços "seguros" perpetua na verdade a possibilidade de riscos à cidadania no Brasil e de esvaziamento do espaço público (SOUZA, 2018). Isso se soma a formas estabelecidas de gestão da vida e de controle social pela ação violenta do Estado quando adota "medidas cada vez mais de confronto, colocando policiais e a população num cenário de exposição" (RIBEIRO; SINHORETTO; BUENO, 2015). Assim, no contexto da realidade brasileira, em que o policiamento é militar, o uso do sistema de reconhecimento facial pode contribuir para a lógica militarizada de controle social, de vida e morte, de medo e estigma.

2.2.1. A MILITARIZAÇÃO E ESPAÇO PÚBLICO

Observamos uma lógica militarizada da segurança pública ao longo da história do país. A Constituição define a preservação da "incolumidade das pessoas e do patrimônio" como finalidade da segurança pública e os policiais militares como forças auxiliares. Desde então já observamos intervenções que remodelam constantemente o espaço público pelo controle e a vigilância (MENDES, 2017). Há dois caminhos para se pensar a segurança pública no Brasil: centrada no combate a guerra ou como prestação de um serviço público, por meio de políticas públicas (BARTIRA; CARDOSO, 2020). A primeira interpretação é um modelo remanescente do regime militar e que ainda hoje predomina na atuação do Estado (Ibid).

O Brasil, desde que se tornou República, teve as forças de segurança pública militarizadas como ferramenta legítima para proteger o Estado e sua hegemonia. A militarização possui sentido amplo e é definida como um segmento que emprega "modelos, métodos, conceitos, doutrinas, procedimentos e pessoal militar em

atividade de natureza policial, dando assim uma feição militar às questões de segurança pública” (CERQUEIRA, 1998, p. 140). Evidentemente, reforça-se a ideia de que os efeitos observados no espaço urbano são diferentes dos ambientes de guerra, contudo, independente do ambiente, a violência com equipamentos cada vez mais tecnológicos partem dos mesmos princípios (GRAHAM, 2017). Em uma democracia não há necessidade de manter a organização com caráter militar, mas o Brasil insiste em manter um modelo de polícia atrelado à defesa do Estado, não colocando o cidadão no centro. Dessa forma, a constituinte preservou o modelo da ditadura militar, colocando-se em contradição com o Estado Democrático de Direito (VALENTE, 1969).

Por outro lado, a Constituição sinaliza a segurança como um direito social, ampliando a proteção garantida para as classes médias e altas também para os grupos sociais reprimidos como negros, habitantes de favelas e entre outros (BARTIRA; CARDOSO, 2020). Apesar de ser um direito fundamental individual, a segurança é um dever do Estado e será gerida a partir da necessidade de preservação da ordem pública. Segundo o que está previsto na lei, em relação aos agentes da lei, os policiais são integrantes de um poder de polícia que os coloca à disposição para prevenir sempre, reprimir quando necessário. Segundo Dias (2003) a Segurança Pública completa a Segurança Pessoal, ou seja, as pessoas num primeiro momento previne e a polícia reprime. É importante evidenciar que todos sem exceção estão submetidos a uma ordem estatal.

Nesse contexto, o que vemos cada vez mais são instrumentos governamentais de intervenção no meio urbano em nome da segurança pública. No Rio de Janeiro as intervenções de segurança pública representam um exemplo de militarização, normalmente justificada para o combate ao crime organizado e ao tráfico de drogas (SOUZA, 2018). A militarização ganha força na medida que a sociedade se torna predominantemente urbana (GRAHAM, 2017). Observamos a tendência a investir em intervenções pontuais ao invés de programas/políticas públicas civis de segurança. Além disso, a cidade, desde os anos 90, testemunhou cinco missões na qual foram utilizadas as Forças Armadas nas ruas em combate ao tráfico de drogas e no auxílio na segurança nos megaeventos, ou seja, momentos nos quais as Forças Armadas operaram no lugar da polícia (SOUZA, 2018). As intervenções militares na segurança têm, assim, um caráter de legalidade, mesmo

vestida da ilegalidade, levantando preocupações em termos de violência e crimes cometidos por militares em função de polícia (VALENTE, 1969).

Diante disso, a militarização da segurança pública rompe com os direitos à cidadania, principalmente sobre aqueles que são estigmatizados e que são colocados em estado de sítio. A policialização das forças armadas e a militarização da polícia operam práticas de controles (TEIXEIRA; LEONARDO, 2020), especialmente quando a necessidade de monitorar conta com aparatos de controle e proteção, diminuindo a qualidade de vida e restringindo a liberdade (GRAHAM, 2017). Nesse contexto, os mais pobres acabam sendo inseridos em um contexto de criminalização e demonização, especialmente a população negra que é comumente retratada como violenta, criminoso e não humana (MBEMBE, 2016; TEIXEIRA; LEONARDO, 2020). O Estado reforça, assim, parâmetros punitivistas e autoritários pelo seu braço armado, colocando em xeque uma desigualdade urbana baseada no controle (Ibid). Essa nova configuração, que entrelaça a segurança e a guerra, não opera mais sem decisões e ações mediadas tecnicamente, segundo um processo de gestão calculista da vida e da morte (FOUCAULT, 1999). Nesse contexto, a apresentação de soluções tecnológicas como ferramenta de combate ao medo e insegurança, somadas à ineficiência do Estado em promover a segurança do espaço público, são os principais motivos que levam à modernização da política de segurança através do reconhecimento facial (LEITE; BONAMIGO; MELGAÇO, 2017).

A combinação de câmeras e sistema de reconhecimento facial impõe um controle populacional manifestando o poder do Estado, principalmente centrado no controle biológico da vida, o que FOUCAULT (1999) apresenta como uma governamentalidade, cujo poder é atribuído a partir da dominação política. Nesta discussão, Foucault chama atenção não para um biopoder que não tem apenas o poder de matar, como também de controlar a vida. Desta maneira, as instituições estatais na cidade do Rio de Janeiro não apenas exercem um biopoder ao criar a divisão dos territórios entre zonas da vida e da morte - permitindo experiências distintas entre os moradores de uma mesma cidade, onde uns vivem na paz e outros em formato de guerra e exceção permanente (AGAMBEN, 2004; TEIXEIRA; LEONARDO, 2020) - como exercem também um controle na vida cotidiana. Essa realidade é considerado fundamental é a única maneira de lidar com esta realidade e chamando de guerra (GRAHAM, 2017)

O Centro Integrado de Comando e Controle (CICC) do Rio de Janeiro é um bom exemplo para pensarmos a metaforização da “guerra” de Graham (2017), ao instituir um enorme aparato de monitoramento urbano como parte dos investimentos infraestruturais para a realização dos megaeventos na cidade. O CICC compõe uma infraestrutura tecnológica com softwares, conexões e equipamentos físicos, concentrando modelos operacionais gerenciais militarizados, que abordam o espaço da cidade como um território de guerra a partir de um uso autoritário, hierárquico e intervencionista da tecnologia (CARDOSO, 2018). Essas tecnologias, a partir de grandes investimentos públicos e participação do setor privado, começam a compor a paisagem urbana (BAUMAN, 1999; 2003). Isso contribui para consolidar paradigmas urbanos sociais baseados no uso da violência, segundo os quais o papel das instituições, além de reprimir e controlar o crime, acaba por também determinar quem vai ser bem tratado ou não no espaço urbano (TEIXEIRA; LEONARDO, 2020). Os investimentos para os megaeventos deram forma a um novo modelo de segurança pública ainda mais sofisticado. O projeto piloto foi gerido nesse mesmo centro.

Institui-se uma tecnopolítica da guerra urbana. Segundo Cardoso (2018) tecnopolíticas podem ser encaradas como um conjunto de ferramentas que visam criar, reforçar ou reverter maneiras de dominar e explorar os modos de existir e de organização da sociedade. Muitas vezes esta guerra não é uma “guerra real” em andamento, mas sim uma “guerra sentida” (BECK, 2007), onde o inimigo é o “poder paralelo”, que é o tráfico de drogas que controla territórios da cidade, o que muitas vezes legitima a aplicação da expressão “guerra civil”. Isso reforça a ideia de que está sendo instituído um novo modelo de controle social baseado no encarceramento em massa, a vigilância e da desvalorização dos direitos (WACQUANT, 1999), e isso só é possível transferindo a ideia de que os altos custos das mortes são a nova forma de se garantir a segurança pública.

Portanto, é importante levar em consideração que as estratégias tomadas para a instalação das câmeras com reconhecimento facial são realizadas por uma hegemonia que concentra o poder de classificar e controlar grupos sociais e de determinar limitações no aproveitamento do espaço público. Isso acontece, por exemplo, quando o sistema de reconhecimento facial é instalado em locais onde a incidência de contraversão sobre determinados grupos passa por uma necessidade de monitoramento social (ABBAS DA SILVA; FRANQUEIRA; HARTMANN, 2021)

Devemos contextualizar o uso de reconhecimento facial, com seus impactos no espaço público e na vida pública, sob o argumento da preservação da ordem pública, especialmente em ocasião de determinados acontecimentos, como por exemplo os megaeventos. Assim, fazer desses eventos uma oportunidade para reunir uma grande quantidade de dados a partir da naturalização da tecnologia como meio para o progresso social, inclusive á a justificativa para a realização de testes.

CAPÍTULO 3 - TECNOPOLÍTICA DA SECURITIZAÇÃO E MILITARIZAÇÃO: O CASO DO PROJETO PILOTO

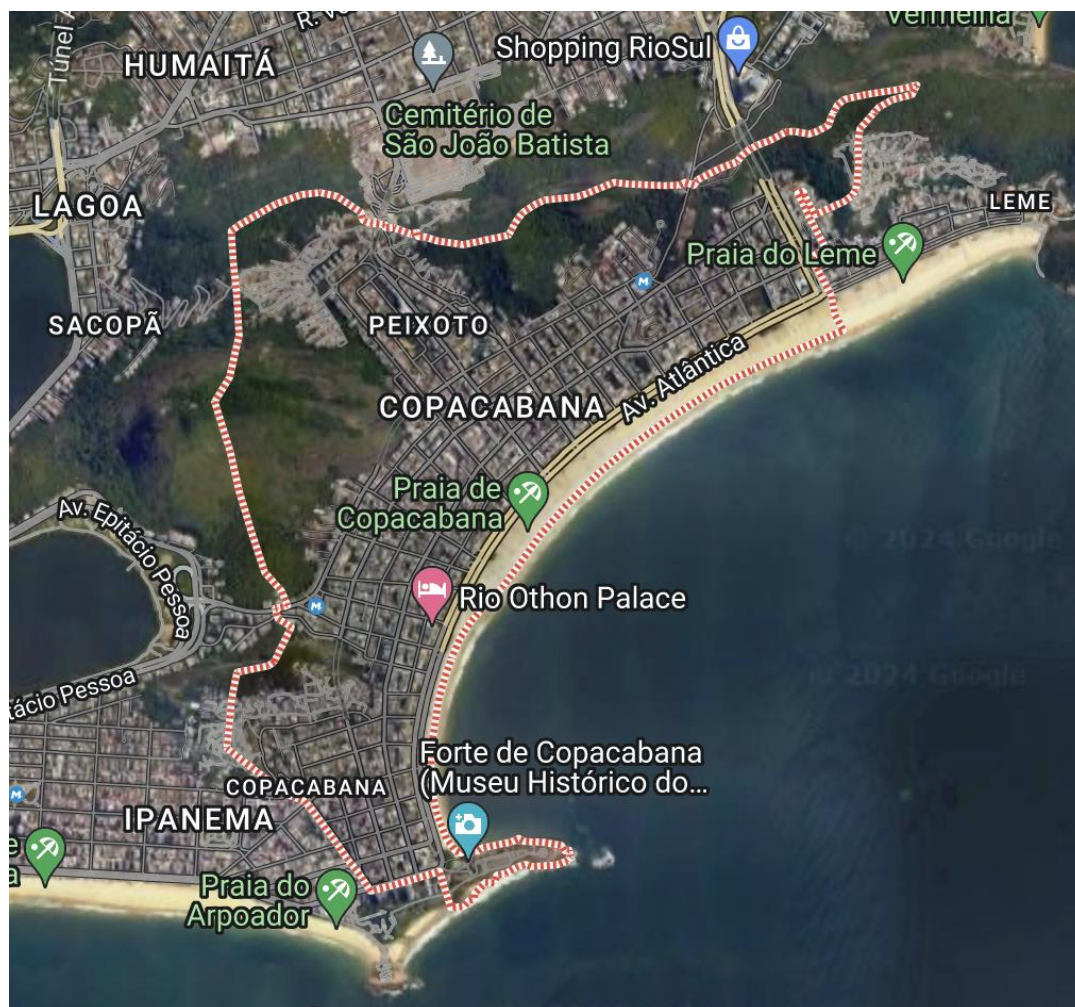
Neste capítulo, avançamos para a análise empírica que busca descrever e interpretar os impactos do uso do sistema de reconhecimento facial na segurança pública do Rio de Janeiro, com foco nas implicações socioespaciais. Com base no estudo de caso do programa piloto, implementado em 2019, esta etapa da pesquisa examina como a tecnologia de vigilância transforma não apenas a gestão da segurança, mas também a percepção do espaço urbano e a vivência cotidiana das populações afetadas. O debate acerca do reconhecimento facial envolve questões éticas, jurídicas e sociais, que vão além da polarização entre segurança e privacidade. Aqui, concentramos a análise em como determinadas populações e territórios são construídos como potenciais ameaças, examinando os efeitos disso na estruturação do espaço público, na mobilidade urbana e nas interações sociais.

3.1. O projeto piloto e sua distribuição “estratégica”

Em 2019, o Governo do Estado do Rio de Janeiro, por meio da Secretaria de Estado de Polícia Militar (SEPM), implementou o Projeto Piloto de videomonitoramento por reconhecimento facial. Esta iniciativa marcou a primeira experiência de uso dessa tecnologia na segurança pública da cidade. Foram inicialmente instaladas 34 câmeras no bairro de Copacabana, 12 das quais equipadas com sistemas de reconhecimento facial e reconhecimento de placas de veículos (BRUNO, 2019) (Mapa 1). Neste primeiro momento, foram usadas câmeras de trânsito já existentes e outras em "lugares estratégicos" de Copacabana. De acordo com a Agência Brasil, o porta-voz da secretaria informou que a seleção dos locais para a instalação das câmeras contou com a participação dos comandos do batalhão e das unidades de polícia pacificadora atuantes em Copacabana. Após o teste inicial durante o Carnaval daquele ano, o governo de Witzel anunciou a expansão do projeto piloto, com a instalação de câmeras de reconhecimento facial no estádio do Maracanã e no Aeroporto Santos Dumont, abrangendo áreas estratégicas próximas ao estádio Maracanã, incluindo avenidas de alta circulação, como a Radial Oeste e a Avenida Maracanã (Maciel, 2019) (Mapa 2). O projeto foi, portanto, expandido com a previsão de instalar 140 câmeras. No entanto, o relatório do Panóptico (2020) revela que, na realidade, foram instaladas apenas 95. Desta maneira, o Governo do Estado

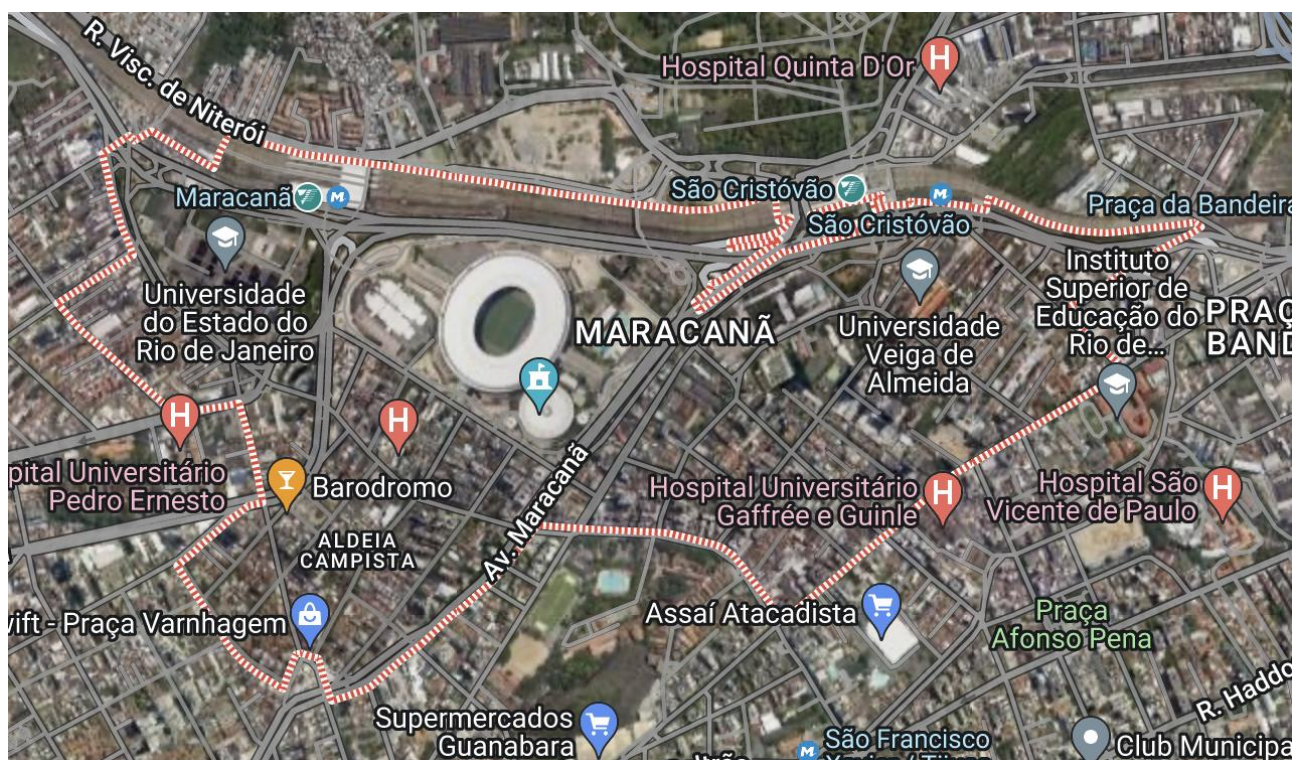
fortalecer o sistema de identificação de pessoas procuradas pela polícia ou veículos em situação irregular¹⁵ (FERNANDES, 2020). A cidade adquire, assim, um novo tipo de patrulhamento.

Figura 3 - Mapa com Delimitação do projeto piloto em Copacabana



¹⁵AGÊNCIA BRASIL. Câmeras de reconhecimento facial começam a funcionar em Copacabana. Época Negócios, 27 fev. 2019. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2019/02/cameras-de-reconhecimento-facial-comecam-funcionar-em-copacabana.html>. Acesso em: 25 jun.

Figura 4 - Mapa com delimitação do projeto piloto no Maracanã



A escolha da localização das câmeras pode refletir os aspectos políticos que impulsionam o projeto. No entanto, ao solicitarmos ao Centro Integrado de Comando e Controle (CICC) o mapa com a localização exata das câmeras, a fim de compreender a incidência desses locais estratégicos, não obtivemos resposta, seja por meio do Portal da Transparência, seja por contato direto com gestores locais. No Termo de Cooperação Técnica (2019, p. 6), encontramos no parágrafo terceiro a menção de que a "listagem dos locais para instalação foi definida pela SEPM, de acordo com suas estratégias de segurança pública", sem, no entanto, especificar os pontos exatos. Essa falta de transparência dificulta a compreensão dos critérios usados para posicionar as câmeras e o reconhecimento facial, impedindo uma análise crítica da estratégia empregada.

Outra questão relevante é que a própria falta de dados claros e objetivos sobre a escolha dos bairros (Copacabana e Maracanã) pode ser considerada um dado em si. A ausência de explicações detalhadas sobre o critério utilizado para selecionar essas áreas levanta sérias dúvidas quanto à imparcialidade e transparência do processo. A falta de divulgação desses dados pode gerar desconfiança, especialmente porque a escolha de bairros com altos índices de fluxo

de pessoas e grande visibilidade política e midiática sugere que a segurança pública está sendo voltada mais para a criação de uma imagem de cidade segura.

A ideia de que a “falta de dados é um dado” está em consonância com estudos sobre gestão pública de segurança. Segundo o pesquisador e sociólogo André Lemos (2003), a gestão de dados em projetos de vigilância, frequentemente esconde, nas lacunas de informação, uma forma de controle social que não se destina a atender as necessidades de todos os cidadãos de maneira equitativa. Em relação ao projeto piloto, a omissão dos critérios de escolha e priorização de áreas como Copacabana, com grande apelo turístico, ou o Maracanã, com seus eventos de grande visibilidade, sugerem que os investimentos tecnológicos na segurança pública estão definidos por interesses políticos, econômicos e midiáticos. Nesse sentido, a falta de transparência não é apenas uma falha administrativa, mas uma falha ética.

Além disso, a partir das declarações do ex-governador Wilson Witzel acerca do projeto piloto, detectamos uma preocupação com a necessidade de fortalecer a segurança pública, capturando foragidos, especialmente em locais que houvesse grande circulação de pessoas que transitam pelo espaço, facilitando a própria detecção de individuais com mandados de prisão¹⁶. Contudo, em outros documentos, de natureza não governamental, observamos outros elementos que evidenciam a escolha estratégica do território de implementação do projeto piloto. Segundo o relatório “Um Rio de Câmeras Com Olhos Seletivos: uso do reconhecimento facial pela polícia fluminense” (2022), o bairro de Copacabana foi selecionado por ser um símbolo da cidade e um ponto de destaque internacional, portanto, uma vitrine ideal para o projeto piloto, com o intuito de projetar internacionalmente a imagem de uma cidade segura e atrativa.

Por isso, a relevância turística e econômica do bairro de Copacabana impulsiona investimentos e uma multiplicidade de medidas de segurança ostensivas. Esse contexto converte o bairro em um verdadeiro laboratório para práticas intensivas de controle social e monitoramento, onde as tecnologias de segurança não apenas são testadas, mas também implementadas de forma sistemática e em grande escala.

¹⁶VEJA. Witzel anunciou reconhecimento facial no Maracanã e Santos Dumont. Disponível em: <<https://veja.abril.com.br/politica/witzel-anuncia-reconhecimento-facial-no-maracana-e-santos-dumont/>>. Acesso em: 7 nov. 2024.

O conceito de "laboratório" aqui se refere à utilização seletiva de territórios, como Copacabana, para testar tecnologias de segurança avançadas, como o reconhecimento facial. A escolha desse bairro, devido à sua alta visibilidade e importância turística, transforma-o em um campo experimental, onde práticas são testadas antes de uma possível expansão para outras áreas da cidade, exemplificando o caso de um projeto piloto. Este tipo de tecnologia permite um monitoramento quase em tempo real dos cidadãos, transformando a cidade em um espaço onde o controle e a vigilância são ampliados para uma cobertura quase total de suas dinâmicas sociais e comportamentais. Isso se torna funcional para garantir a segurança dos turistas e também durante a realização dos grandes eventos que cada vez mais estão acontecendo na praia de Copacabana.

Desde a instalação do projeto piloto de reconhecimento facial, Copacabana se consolidou como o epicentro de eventos de massa, como o Réveillon e mega shows, que atraem milhões de turistas e investimentos, intensificando a projeção política e o posicionamento da cidade como vitrine global. Além do histórico evento do Réveillon, observamos a realização de novos grandes eventos, como o show da Madonna em 2024 e da Lady Gaga em 2025. Trata-se de eventos que precisam de uma infraestrutura e estratégia de segurança altamente militarizada e tecnológica¹⁷.

Grandes eventos muitas vezes se tornam justificativos para o aumento de patrulhamento ostensivo e a implementação de tecnologias de vigilância de alta capacidade, como câmeras de monitoramento e reconhecimento facial. Recentemente, leis como a 2743/23 e regulamentações têm exigido o uso dessas tecnologias em estádios, supostamente para aumentar a segurança dos frequentadores¹⁸. Isso reflete uma tentativa de controlar o espaço não apenas em termos de segurança, mas também de gestão pública da ordem pública. Assim como em Copacabana, a paisagem securitária em torno do Maracanã é moldada por um

¹⁷WITH, C. Madonna draws record-breaking crowd of 1.6 million for biggest concert of her career: "Who knows if she'll ever come back". Disponível em: <<https://celebrity.nine.com.au/latest/madonna-news-singer-performs-biggest-ever-concert-rio-de-janeiro-copacabana-beach-record-breaking/2e1778ae-b7e5-47f5-a1d3-8a3b97e2cbb6>>. Acesso em: 19 out. 2024.

¹⁸da CNN. Reconhecimento facial será obrigatório nos estádios a partir de 2025. Disponível em: <<https://www.cnnbrasil.com.br/esportes/futebol/reconhecimento-facial-sera-obrigatorio-nos-estadios-a-partir-de-2025/>>. Acesso em: 18 dez. 2024.

entendimento de risco que privilegia a proteção de direitos públicos e ignora os desafios sociais mais profundos que o cercam.

No caso do Maracanã, a implementação do projeto piloto de reconhecimento facial não se justifica apenas pela realização de grandes eventos, mas também pelo papel histórico e simbólico do estádio como ícone esportivo. Além de ser também um espaço que merece uma análise profunda quando se trata de segurança militarização e as diversas concepções de risco e criminalidade. Como palco de grandes eventos, desde jogos de futebol a shows e manifestações culturais, o estádio e seu entorno atraem uma vasta gama de frequentadores, que vão de torcedores locais a internacionais, moradores e trabalhadores informais.

Essa pluralidade de usos e ocupações transforma uma área em um microcosmo de tensões sociais, políticas e securitárias. A intensificação da violência no futebol, ao longo dos anos, resultou na militarização desses eventos, que deixaram de ser "espontâneos" e passaram a envolver um forte aparato de segurança, muitas vezes incluindo armas de fogo (Lopes & Perina, 2018). Os confrontos entre torcidas não se limitam aos dias de jogo, influenciando as operações de segurança no entorno do estádio (Tsoukala, 2014). Essa violência e seus impactos na área circundante ameaçam a "imagem" do evento esportivo e a percepção pública.

Embora o discurso oficial sugira que o sistema pode contribuir para enfrentar os desafios da violência, ele, na verdade, reflete uma tendência crescente de tratar os estádios e seus arredores como espaços de vigilância massiva, sem abordar as questões estruturais que originam a violência. Mais uma vez, a tecnologia surge como uma resposta superficial para problemas complexos, sem que haja um verdadeiro esforço para compreender a natureza dos conflitos ou promover um ambiente que vá além da simples detecção de suspeitos. Além disso, o argumento de que o reconhecimento facial poderia promover uma gestão mais equitativa do espaço esconde o fato de que essas tecnologias, na prática, reforçam desigualdades e estigmatizam grupos já marginalizados. As torcidas organizadas, frequentemente associadas ao vandalismo, se tornam alvos preferenciais dessas tecnologias, enquanto outras formas de violência, muitas vezes perpetradas por setores mais privilegiados, são ignoradas. O planejamento urbano, em vez de ser orientado pela inclusão e pela segurança de todos, acaba consolidando a fragmentação e o controle

hierárquico do espaço público, relegando a verdadeira segurança a um plano simbólico.

Em entrevista, a Deputada Estadual Dani Monteiro e presidenta da Comissão de Direitos Humanos da ALERJ, que acompanhou de perto a implementação do projeto, explicou: "A escolha do Maracanã para o projeto piloto não é uma surpresa. Estamos falando de uma área que reflete as desigualdades territoriais do Rio de Janeiro. De um lado, temos um bairro que recebe grandes investimentos para eventos esportivos, do outro, moradores que enfrentam inseguranças diárias e que pouco têm acesso a áreas periféricas ou facilitam práticas de vigilância seletiva." (23 de maio 2024). A frase da Deputada Dani Monteiro destaca a disparidade entre duas realidades que coexistem no Rio de Janeiro, especialmente em relação ao projeto piloto de reconhecimento facial no Maracanã. "Um lado" refere-se à área do Maracanã, que é um espaço privilegiado, recebendo grandes investimentos para eventos esportivos, como finais de campeonatos e shows. Essa área representa uma vitrine para o turismo e para a promoção de uma imagem de segurança e sucesso da cidade. "O outro lado" diz respeito aos moradores que vivem nas comunidades próximas, que enfrentam inseguranças diárias, como violência e marginalização, e que têm pouco acesso a oportunidades e serviços de qualidade. Essa população é frequentemente sujeita a práticas de vigilância seletiva, onde a segurança é intensificada apenas em áreas com maior visibilidade e riqueza, enquanto as necessidades e os direitos dos moradores são negligenciados.

Embora o projeto piloto seja promovido sob o argumento de aumentar a segurança, levanta preocupações sérias, especialmente em relação à proteção de crianças, adolescentes e grupos minorizados. O relatório "Esporte, Dados e Direitos: O uso de reconhecimento facial nos estádios brasileiros", produzido pelo Panóptico, traz à tona os riscos de violações de direitos fundamentais, sobretudo no que diz respeito à privacidade e ao uso indevido de dados biométricos. O cenário é ainda mais preocupante quando se considera a coleta de dados de crianças, um grupo especialmente vulnerável e protegido por legislações específicas, como o Estatuto da Criança e do Adolescente (ECA).

A prática de cadastrar crianças de colo e jovens menores de 16 anos para o uso de reconhecimento facial em estádios, não só contraria a Lei Geral do Esporte,

que estabelece o controle biométrico a partir dos 16 anos, mas também esbarra em importantes preceitos da Lei Geral de Proteção de Dados (LGPD). Esses dispositivos legais foram criados justamente para garantir que a coleta e o processamento de dados sensíveis sejam feitos com base no consentimento e na proteção adequada, especialmente para menores de idade, que estão sujeitos a um nível de vulnerabilidade acentuado. A segurança não pode ser usada como justificativa para a criação de um ambiente de vigilância permanente, especialmente quando os mais vulneráveis são os mais afetados. É necessário um posicionamento firme contra essas práticas, que priorize a proteção de dados e o respeito aos direitos humanos, especialmente no que se refere às crianças e adolescentes.

Em relação ao projeto piloto, essa divisão significa que a implementação da tecnologia de vigilância no Maracanã pode ser vista como uma maneira de reforçar a segurança em um espaço que já é privilegiado, enquanto ignora as condições de vida e os direitos dos moradores das áreas periféricas. A escolha do Maracanã para o projeto simboliza uma priorização do controle e da segurança em espaços que atraem turistas, em vez de abordar as questões de desigualdade e insegurança que afetam diretamente a população local. Portanto, o projeto pode ser criticado por perpetuar um ciclo de exclusão e controle, em vez de promover uma segurança que abranja todos os cidadãos de maneira equitativa.

A militarização revela uma resposta estatal que prioriza o controle ostensivo e repressivo para monitorar e proteger o estádio, um símbolo não apenas do futebol, mas também da identidade cultural, midiática e econômica da cidade. A escolha do Maracanã como local para o projeto se justifica pela sua diversidade de usos urbanos, comportando tanto eventos de grande escala quanto uma população flutuante significativa, com picos de concentração de moradores e visitantes. Isso evidencia a necessidade de novas ferramentas de monitoramento para regiões de alta mobilidade e destaque, reforçando o papel do estádio como um ponto estratégico na cidade. A seletividade territorial do projeto piloto reforça, portanto, uma securitização que vai além da resposta a ameaças concretas, representando uma reconfiguração do cotidiano em torno de práticas de vigilância, que naturalizam o controle social para finalidades econômicas e políticas (BIGO, 2002).

3.2. Tecnologia á serviço da militarização

A execução do projeto envolve uma rede operacional composta por diversos atores responsáveis por sua implementação e operação. O Termo de Compromisso rege a parceria entre as secretarias de Polícia Militar e Polícia Civil, o Departamento Estadual de Trânsito (Detran), a Prefeitura do Rio de Janeiro e a empresa Oi. De acordo com o termo, a Oi, em parceria com a Huawei e a empresa britânica Staff of Technology Solution, era responsável pelo fornecimento da tecnologia de reconhecimento facial nas câmeras de segurança. Embora a tecnologia seja fornecida por empresas privadas, o controle do banco de dados e a operação do sistema são responsabilidade do Estado (Lisboa, 2019). A Secretaria de Polícia Militar tinha a responsabilidade de conduzir a prova de conceito, isto é, avaliar a aplicação, aprovar a implementação e validar o funcionamento dessa tecnologia nas operações policiais (Henrique Coelho, 2019).

A SEPM enfatizou que a parceria com a Oi para o projeto piloto de reconhecimento facial não acarretaria custos financeiros ao Estado, dado que a empresa já fornece a rede de dados necessária para o tráfego de informações. Contudo, essa cooperação técnica é regida por contratos prévios e não contempla cláusulas específicas que detalham o uso do novo sistema de reconhecimento facial, criando um cenário marcado pela opacidade e pela falta de transparência sobre os termos e objetivos do acordo. Esse vazio regulatório é ainda mais problemático quando se considera que a Oi, além de ser beneficiada financeiramente pela parceria, pode estar capitalizando dados coletados para fins comerciais, ampliando suas oportunidades no mercado de dados pessoais. Tal ausência de clareza em relação ao uso dos dados públicos gera uma desconfiança crescente sobre a verdadeira natureza dessa parceria. A falta de especificação sobre como a Oi irá utilizar esses dados levanta a suspeita de que a empresa possa estar, na prática, usando o projeto como uma porta de entrada para a troca e a venda de informações pessoais, com interesses comerciais que não são necessariamente alinhados ao bem público. Em um contexto em que a coleta massiva de dados é cada vez mais comum, a possibilidade de esses dados serem compartilhados com outras empresas ou governos, sem um controle adequado, coloca em risco os direitos de privacidade dos cidadãos.

Além disso, é importante ressaltar o histórico da Oi, que em 2014 foi multada por violar a privacidade de seus clientes ao coletar e compartilhar dados sem o devido consentimento¹⁹. Esse episódio levanta sérias questões sobre a capacidade da empresa de gerenciar informações sensíveis de maneira ética e transparente, principalmente quando ela se torna um ator central em um projeto de vigilância em larga escala. O cenário é ainda mais alarmante ao considerarmos que o sistema de reconhecimento facial, promovido como uma solução para segurança pública, é na verdade parte de um mercado global de tecnologias de vigilância, que são oferecidas como soluções prontas, sem uma análise profunda sobre suas implicações sociais e éticas.

O projeto piloto se insere em uma dinâmica global de acumulação baseada em dados que é alimentada por sistemas privados e militares de vigilância. A falta de transparência em relação à coleta e uso massivo de dados, sem consentimento explícito dos cidadãos e sem a implementação de mecanismos adequados de supervisão e responsabilização, não é apenas uma prática abusiva; é uma afronta ao direito fundamental de circulação e manifestação.

Existe um forte ativismo por parte de organizações da sociedade civil e pesquisadores em defesa da proteção de dados pessoais e que mostram preocupação com projetos como o piloto. Organizações como o Instituto Brasileiro de Defesa do Consumidor (Idec) alertam para os riscos de vazamento ou má utilização dessas informações. Bárbara Simões, advogada e pesquisadora do programa de direitos digitais do Idec, destaca a necessidade de garantir a segurança dos dados pessoais coletados, uma vez que esses dados podem ser vendidos por empresas privadas ou manipulados de maneira inadequada, comprometendo a privacidade de milhões de cidadãos. Ela questiona o uso da tecnologia sem uma clara regulamentação e sem garantias de que as informações não serão usadas de forma prejudicial, ou seja, o debate sobre o uso dessa tecnologia deve ir além da eficiência no combate ao crime, questionando os limites do controle estatal e os efeitos de uma

¹⁹Oi é multada em R\$3,5 milhões por vender informações de clientes. VEJA. Disponível em: <<https://veja.abril.com.br/economia/oi-e-multada-em-r-35-milhoes-por-vender-informacoes-de-clientes>>. Acesso em: 28 jun. 2024.

vigilância cada vez mais abrangente na liberdade e nos direitos fundamentais da população²⁰

Também em entrevista, o ativista e pesquisador Pablo Nunes (24 de abril de 2024) ressalta que a opacidade que permeia sistemas, como o do projeto piloto, intensificam riscos de abusos e de violação dos direitos humanos. Isso reflete uma falha do poder público na salvaguarda de direitos básicos, como a privacidade e a liberdade. Isso é ainda mais preocupante quando pensamos que o projeto é gerido pela polícia militar. A rede operacional de atores conta também com a centralidade do Centro Integrado de Comando e Controle (CICC), gerido pela Polícia Militar, onde convergem todas as imagens transmitidas pelo projeto piloto, que se insere num sistema urbano-tecnológico operacional de monitoramento já existente.

Criado em 2014, pelo decreto número 44.698, de 2 de abril de 2014, o CICC fazia parte do Sistema Nacional Integrado de Comando e Controle (SICC), desempenhando um papel crucial no planejamento e operação da segurança pública durante a Copa do Mundo de 2014. Na época, conforme Cardoso (2018) afirma, houve grandes investimentos em sistemas tecnológicos e muitas empresas de tecnologia recebem fundos públicos da Secretaria Extraordinária de Segurança para Grandes Eventos (ESMES), entre as quais a Aceco TI S.A., Aeromot, Agora Telecomunicações, Unisys Brasil, Comtext Telecomunicações e Medidata Informática. O mercado globalizado associado aos megaeventos impulsionou investimentos tecnológicos na área de segurança pública, atendendo, em parte, a exigências contratuais para a realização desses eventos.

O CICC opera dentro de um modelo de cidade inteligente, englobando e integrando 18 agências²¹ dos setores de segurança pública e defesa civil. Segundo o Termo de Cooperação Técnica, o projeto piloto representa uma oportunidade de

²⁰ Câmeras de reconhecimento facial levam a 4 prisões no carnaval do Rio. Disponível em: <<https://agenciabrasil.ebc.com.br/geral/noticia/2019-03/cameras-de-reconhecimento-facial-levam-4-prisoas-no-carnaval-do-rio>>. Acesso em: 19 dez. 2024.

²¹ Polícia Militar do Estado do Rio de Janeiro (PMERJ), Polícia Civil do Estado do Rio de Janeiro (PCERJ), Corpo de Bombeiros Militar do Estado do Rio de Janeiro (CBMERJ), Guarda Municipal do Rio de Janeiro (GM-Rio), Secretaria de Estado de Segurança (SESEG), Defesa Civil Estadual, Defesa Civil Municipal, Centro de Operações Rio (COR), Departamento de Trânsito do Rio de Janeiro (DETRAN-RJ), Agência Nacional de Telecomunicações (ANATEL), Polícia Rodoviária Federal (PRF), Polícia Federal (PF), Exército Brasileiro, Marinha do Brasil, Força Aérea Brasileira (FAB), Agência Brasileira de Inteligência (ABIN), Secretaria Municipal de Transportes, Secretaria Estadual de Saúde.

fortalecimento da segurança pública, mediante a “integração com todas as unidades policiais no Estado do Rio de Janeiro, e podendo integrar a polícia militar, polícia civil, corpo de bombeiros, guarda municipal, SAMU, dentre outras unidades”. É o CICC, com seu aparato tecnológico, que garante a infraestrutura necessária para a realização da integração.

O acesso ao CICC é controlado por monitores biométricos, seguindo a doutrina militar de Comando e Controle (C2), com diferentes andares que correspondem a distintos níveis de comando e de urgência. O primeiro nível, o Centro Integrado de Defesa Social, gerência emergências por meio de canais como 190, 192 e 193. O segundo nível, o Centro Integrado de Operações, monitora eventos e crises como durante a pandemia de COVID-19. No último nível, o Conselho de Gestão de Crises lida com crises de alta complexidade, como no caso de intervenções federais.

Em entrevista, Bruno Cardoso (17 de abril. 2024), destaca que a colaboração entre agências é facilitada pela infraestrutura de Tecnologia da Informação e Comunicação (TIC), que possibilita integrar dados coletados por dispositivos tecnológicos distribuídos no espaço urbano, como as câmeras de vigilância.

Imagens e dados convergem numa grande tela que funciona como um grande ponto de observação da cidade (Figura 5). Os dados gerados pelo sistema de videomonitoramento do projeto piloto são integrados e cruzados em tempo real com bases de dados de diversas agências que fazem parte do Centro de Operações, como a Polícia Civil e o Detran. O videomonitoramento captura imagens e vídeos continuamente. Essas imagens são analisadas por sistemas de reconhecimento facial, que verificam automaticamente a presença de pessoas ou veículos com registros suspeitos nas bases de dados associadas.

Quando o sistema detecta uma correspondência, o alerta é gerado de forma automática. A partir desse momento, o sistema envia os dados do incidente para os operadores de segurança, que têm acesso a informações detalhadas sobre a situação em tempo real. O despacho de ações de intervenção policial, como a abordagem de indivíduos ou a apreensão de veículos, é agilizado pela troca instantânea de informações entre as diversas bases de dados e os sistemas de videomonitoramento e RF.

Segundo o Termo de Cooperação Técnica (2019, p. 3), o sistema de imagens do projeto piloto permite:

“A redução de custos operacionais e o tempo de despacho, proporcionando muito mais assertividade nas ocorrências, e, o que é mais importante, eventualmente, salvando vidas, o que melhora sensivelmente o serviço prestado ao cidadão, fazendo estes se sentirem mais seguros, e aumentando sobremaneira a capacidade de gerenciamento do Estado e do staff de segurança, dando um passo muito alto na transformação em um “Smart and Safe State”.

A tecnologia é apresentada, assim, como algo que possibilita uma maior assertividade, oferecendo um serviço ao cidadão e tornando o estado mais “inteligente” e “seguro”. Ao contrário, o que argumentamos com a presente pesquisa é que a tecnologia do projeto piloto aprimora a capacidade operacional, mitigando efeitos e não atingindo as causas dos problemas de segurança pública, e fortalece uma lógica militar de comando e controle.

Figura 5 - Sala de monitoramento do Centro Integrado de Comando e Controle



Fonte: google imagens

A tecnologia à serviço do projeto piloto aprimora, portanto, a capacidade operacional militar (Kraus et al., 2022). O projeto piloto envolve algumas inovações tecnológicas que garantem uma maior eficiência no atendimento e agilização de despachos de ocorrências. Entre elas, destaca-se o Android Emergency Location Service (ELS), que envia automaticamente a localização exata do dispositivo Android para os serviços de emergência durante uma chamada. Além disso, o projeto permite que qualquer chamada de voz seja transformada em uma chamada de emergência aprimorada, oferecendo serviços como localização GPS precisa, vídeo ao vivo e bate-papo bidirecional, sem a necessidade de um aplicativo adicional. Um add-on também pode ser instalado facilmente em sistemas de segurança privados, proporcionando dados de localização, vídeo ao vivo e bate-papo para agilizar a análise das ocorrências pelos socorristas.

Além disso, o projeto oferece ferramentas para análise detalhada de eventos e relatórios, permitindo que responsáveis pelo comando de segurança compreendam padrões e comportamentos das ocorrências, possibilitando uma gestão das emergências. O sistema de consulta também é acessado de forma restrita, com

cadastro em login e termos de responsabilidade para os funcionários do Estado do Rio de Janeiro, garantindo a segurança e a privacidade das informações. Essas inovações visam aumentar a eficiência no atendimento às emergências, embora seja essencial avaliar seus impactos na privacidade e no controle social.

O projeto piloto é promovido, segundo o Termo de Cooperação Técnica, em nome da “assertividade” e da redução dos pontos “frágeis” e pontos “cegos” na área de Segurança Pública”. As fragilidades são identificadas como aquelas que impedem um pronto atendimento. É promovida, assim, uma ideia de segurança restrita e limitada à capacidade de intervenção, deslocando o foco para o campo da eficiência e ignorando os problemas estruturais dos problemas de segurança pública.

Ao focar em medidas pontuais de intervenção, a proposta não busca uma transformação estrutural, mas sim a minimização dos efeitos da violência e da criminalidade. Essa abordagem acaba por reforçar a ideia de uma segurança limitada, centrada em respostas rápidas e tecnológicas, sem contemplar as profundas desigualdades sociais e a falta de políticas públicas integradas que poderiam atacar as raízes desses problemas. Portanto, enquanto a intervenção imediata pode oferecer uma sensação de controle, ela não resolve os desafios mais amplos e persistentes da segurança pública, como a violência sistêmica e as falhas nas políticas sociais. Isso reforça a visão apresentada por Evgeny Morozov (2013) de um solucionismo tecnológico que mitiga efeitos, sem atingir as causas estruturais dos problemas sociais.

Além da dimensão operacional, o sistema tecnológico do projeto piloto está diretamente a serviço da lógica militar de comando e controle, alinhando-se com a agenda militarizada da segurança urbana. Nesse sentido, é importante destacar que o CICC foi originalmente subordinado e financiado pela Secretaria Extraordinária de Segurança para Grandes Eventos (SESGE) do Ministério da Justiça, extinta em 2017 (Presidência da República, 2011). Após essa mudança, a gestão do centro deveria ser assumida pela Secretaria de Segurança Pública do Estado do Rio de Janeiro. No entanto, com a extinção desta secretaria no início do mandato do governador Wilson Witzel, em 2019, a administração do CICC passou para a responsabilidade da Polícia Militar do Estado do Rio de Janeiro.

O projeto piloto constitui mais um dispositivo militar que reforça a lógica de militarização urbana na cidade. A presença militar, o uso extensivo de videomonitoramento e reconhecimento facial e a operação do CICC consolidam a militarização como um elemento organizador da vida social (Cardoso, 2018). Além disso, relatos de pessoas apreendidas pelo sistema do projeto piloto indicam que as detenções ocorreram no meio de suas rotinas de trabalho, sem qualquer explicação prévia, sendo a verificação realizada apenas posteriormente, já na delegacia. Esse procedimento evidencia uma lógica de combate, na qual os alvos são identificados e atingidos. Além disso, a elevada margem de erro e o fato que atingem principalmente pessoas pobres e negras indica que o projeto piloto, com sua proposta de garantir assertividade e agilidade, é funcional à lógica militar de guerra urbana. Isso contribui com a configuração da cidade como um campo de batalha contra um "inimigo interno", onde os direitos dos cidadãos podem ser temporariamente suspensos, e a construção de territórios e corpos como objetos de medo legitima ações de controle e eliminação (Souza, 2015).

Essa tecnologia, portanto, serve a uma lógica de guerra que se estende além das favelas, visando "proteger" áreas de interesse econômico e turístico. Essa abordagem levanta questões socioespaciais cruciais sobre como promover uma sociedade segura e justa, questionando a efetividade e os impactos sociais de tais sistemas de vigilância e controle (Beck, 2007; Souza, 2018).

A lógica de comando e controle, operacionalizada do ponto de vista tecnológico pelo projeto piloto, reflete uma forma de governança urbana onde o controle territorial é exercido através de uma militarização invisível e que se manifesta principalmente quando acontecem apreensões. O projeto piloto contribui para transformar o espaço urbano em um campo de batalha, onde o Estado e suas forças de segurança, em parceria com o setor privado, monitoram, disciplinam e intervêm. Configura-se uma urbanização autoritária em que se consolida uma infraestrutura de segurança que segrega, inclusive a partir de quem detém o poder sobre as tecnologias, controlando o acesso aos direitos de privacidade, liberdade e mobilidade.

A segregação sociotécnica não se manifesta apenas no acesso desigual à tecnologia, mas também no seu uso como dispositivo de exclusão, controle e

criminalização de grupos vulneráveis, enquanto as estruturas de poder e comando continuam blindadas por uma lógica de militarização e repressão.

3.3. Discurso oficial e vigilância ampliada

A pesquisa indica que o projeto piloto faz parte das iniciativas da agenda pública de combate à criminalidade, influenciando de maneira significativa, e nem sempre positiva, a organização social e a reestruturação física e simbólica da cidade. Antes de explorar essas dimensões, consideramos importante destacar que, oficialmente, o projeto foi apresentado como bem-sucedido, evidenciando as diferentes interpretações sobre o que caracteriza um sucesso.

Nos primeiros meses de 2019, entre 1o e 6 de março, durante o Carnaval, o projeto piloto resultou no cumprimento de oito mandados de prisão em aberto, identificando cerca de 8 mil pessoas como foragidas, suspeitas ou desaparecidas, a partir da análise de aproximadamente 3 milhões de rostos capturados no período²² O ex-governador, Wilson Witzel, afirmou na época que a segurança pública era prioridade e comemorou o "sucesso" do projeto. A corporação avaliou que o projeto piloto "passou no primeiro test drive" que o sistema de leitura facial e de placas de veículo "demonstrou que funciona com alto grau de precisão"²³. Em sua rede social (Figura 6), ele aponta que a presença dessas tecnologias de vigilância representaria um "avanço significativo no combate à criminalidade".

Figura 6 - Print da rede social "X"

²²JULIÃO, Henrique. Reconhecimento facial no Carnaval do Rio identificou 8 mil pessoas de interesse. 09 maio de 2019. Disponível em: <<https://teletime.com.br/09/05/2019/reconhecimento-facial-no-carnaval-do-rio-identificou-8-mil-pessoas-de-interesse/>>. Acesso em: 27 jun. 2024.

²³Câmeras de reconhecimento facial levam a 4 prisões no carnaval do Rio. Disponível em: <<https://istoedinheiro.com.br/cameras-de-reconhecimento-facial-levam-a-4-prisoas-no-carnaval-do-rio/>>. Acesso em: 26 jun. 2024.



Fonte: rede social X

A fala do ex-governador reflete o interesse crescente das autoridades na adoção de tecnologias como ferramentas de segurança pública. Constroi-se um discurso que apresenta o projeto piloto e seu uso simbólico para promover uma sensação aparente de avanços na segurança. Mesmo diante de seus erros comprovados e de inúmeras campanhas públicas que pedem seu banimento, o reconhecimento facial tem sido apresentado como solução eficiente e neutra para o combate à criminalidade. Tal uso instrumentalizado reflete a visão de que essa tecnologia é um avanço simplista, ignorando a complexidade das interações sociais e os riscos de estigmatização territorial.

Desde as eleições de 2018, o sistema de reconhecimento facial já figurava como uma das principais promessas de campanha de Wilson Witzel. Ele afirmou que

lançaria o projeto-piloto nas ruas logo no primeiro mês de seu mandato. O anúncio foi feito durante uma entrevista à jornalista Míriam Leitão, na Globonews, onde Witzel antecipou que o projeto seria implementado por meio de uma parceria público-privada (PPP), garantindo que não haveria custos diretos para o Estado. A proposta de Witzel sinalizava uma aposta em soluções tecnológicas para a segurança pública, mas também levantava questões sobre o papel do setor privado no gerenciamento de dados sensíveis e na vigilância da população.

Figura 7 - Promessas de campanha



Fonte: G1

Diante disso, ao observar a implementação do projeto piloto de reconhecimento facial no Rio de Janeiro, nos deparamos com o projeto piloto se tornando um ponto central de intensas disputas discursivas entre diferentes grupos sociais que vivem, governam e atuam na cidade. Esses grupos – como governo, conselhos comunitários, comerciantes, Estado, moradores e população periférica – possuem visões contrastantes sobre a tecnologia, gerando um cenário de conflito em torno da apropriação e controle dos territórios.

De início pode-se observar uma clara opção por parte de gestores e governantes pelo vigilantismo estatal como forma de controle territorial. Além de Witzel, declarações de figuras como o Coronel Mauro Fliess, que esteve à frente do projeto piloto de reconhecimento facial durante o governo Witzel nos primeiros testes, ilustram essa visão. Segundo Fliess, a adoção em larga escala da tecnologia "vai

contribuir de maneira firme para a redução da criminalidade”²⁴. Ele projeta que, a médio prazo, o sistema será aplicado de forma permanente. Contudo, a adoção de tecnologia de vigilância, especialmente as que envolvem reconhecimento facial, não pode ser vista de forma tão simplista. Há questões complexas que envolvem desde os custos de instalação e manutenção dos equipamentos até as possíveis falhas técnicas que podem comprometer a eficácia do sistema. A falta transparência quanto ao destino e a utilização dos dados capturados também é uma preocupação central, considerando que informações sensíveis podem ser armazenadas e utilizadas sem o consentimento dos cidadãos.

É preciso destacar aqui a controvérsia em relação a redução da criminalidade, pois desde que o Cláudio Castro, que assumiu após o impeachment de Witzel, observamos uma intensificação da repressão violência e na manutenção das vulnerabilidades que afetam as favelas e periferias, isso é demonstrado nas 182 mortes em 40 chacinas, incluindo a tragédia no Jacarezinho e a chacina da Vila Cruzeiro, apontam para um padrão de violência sistêmica. Esses dados revelam não apenas a brutalidade das operações policiais, mas um padrão sistemático da violência que tem como alvos principais as favelas e periferias. A narrativa de “segurança pública”, frequentemente usada para justificar essas operações, mascara a realidade de uma guerra contra os pobres e racializados, que são vistos como ameaças a serem eliminadas em nome de uma suposta ordem. O ponto em evidenciar esses dados, está na apresentação do projeto “Cidade Integrada”²⁵ lançado pelo mesmo governador, que apresenta uma proposta de modernização e integração das favelas à cidade formal, o projeto pretende instalar câmeras de vigilância em áreas como o Jacarezinho, logo após uma das maiores chacinas da história recente do Rio de Janeiro. Longe de representar uma verdadeira inclusão ou integração, o uso dessas câmeras é visto como parte de uma política de vigilância seletiva e repressiva, que reforça a militarização e o tratamento das favelas como territórios de exceção.

²⁴ 24A PM vai ampliar os testes com as câmeras de reconhecimento facial no Rio. Disponível em: <<https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/03/22/pm-vai-ampliar-os-testes-com-as-cameras-de-reconhecimento-facial-no-rio.ghtml>>. Acesso em: 19 dez. 2024.

²⁵ Cidade Integrada: o que promete o Governo do RJ. Disponível em: <<https://g1.globo.com/rj/rio-de-janeiro/noticia/2022/01/23/cidade-integrada-o-que-promete-o-governo-do-rj.ghtml>>. Acesso em: 19 dez. 2024.

Nossa pesquisa identifica elementos que contradizem a interpretação tecnocrática apresentada pelos representantes da política de segurança pública do Estado, já que o projeto pode ser interpretado como um sistema que amplia a vigilância. Primeiro, o projeto piloto amplia um sistema de videomonitoramento já existente, implementado inicialmente em Copacabana e no Maracanã a partir dos anos 2000. De acordo com dados do SESEG (2020), desde então, e especialmente após a confirmação do Rio de Janeiro como sede de eventos internacionais, foram instaladas mais de 1.000 câmeras no Maracanã e 2.000 em Copacabana. O projeto piloto dá continuidade, efetivando a instalação de 125 câmeras, prevendo no mínimo 12 com reconhecimento facial em Copacabana. As câmeras do projeto piloto são capazes de capturar, em alta definição, os rostos de pessoas caminhando pelas ruas, mesmo em meio à multidão. Equipadas com lentes de alta potência, elas têm capacidade de aproximação de até 25 metros e conseguem registrar até 60 imagens por segundo²⁶. As câmeras de reconhecimento facial, ao identificar rostos e compará-los com imagens armazenadas em bancos de dados, automatizam a busca por pessoas foragidas ou procuradas, assim como por veículos roubados.

Como mencionado anteriormente, todas as imagens capturadas são transmitidas diretamente para o Centro Integrado de Comando e Controle (CICC), que conta com tecnologia de última geração. O CICC é equipado com um imponente videowall composto por 98 telas de LED de 55 polegadas, totalizando uma área de 17 metros de largura por 5 metros de altura. Através de um sistema de processamento distribuído, esse "paredão" exibe imagens de mais de 3 mil câmeras de monitoramento espalhadas por todo o estado, permitindo uma análise em tempo real e coordenada das informações capturadas²⁷. O centro, com suas telas, seus dispositivos e sistemas de videomonitoramento integrados, pode ser visto como uma forma de "Big Brother Urbano" (Lyon, 2003). O CICC centraliza as imagens, transformando a cidade em um grande espaço vigiado pelo olhar militar. O projeto piloto acrescenta complexidade, não somente ampliando o sistema de

²⁶Polícia do Rio começa a usar tecnologia de reconhecimento facial; novo sistema tem desafios. G1. Disponível em: <<https://g1.globo.com/jornal-nacional/noticia/2024/01/05/policia-do-rio-comeca-a-usar-tecnologia-de-reconhecimento-facial-novo-sistema-tem-desafios.ghtml>>. Acesso em: 26 jun. 2024.

²⁷REVISTA EMERGÊNCIA. Centro Integrado de Comando e Controle completa três anos - Revista Emergência. Disponível em: <<https://revistaemergencia.com.br/geral/centro-integrado-de-comando-e-controle-completa-tres-anos/>>. Acesso em: 19 dez. 2024.

videomonitoramento urbano, adicionando tecnologia avançada à presença física das forças de segurança, como também introduzindo o sistema de reconhecimento facial. O reconhecimento facial intensifica a vigilância do ponto de vista técnico ao adicionar uma camada sofisticada de monitoramento automatizado sobre o videomonitoramento tradicional. Enquanto câmeras convencionais capturam imagens em tempo real, o reconhecimento facial processa esses dados de forma ativa e em grande escala, identificando indivíduos em meio a multidões, cruzando as informações com bases de dados e gerando alertas em tempo real. Esse sistema aumenta a capacidade de vigilância ao identificar pessoas específicas sem a necessidade de supervisão constante de um operador humano, o que pode amplificar o controle estatal sobre os espaços urbanos.

O projeto piloto de reconhecimento facial acrescenta uma camada de sofisticação ao sistema de videomonitoramento que já existia na região. Antes da introdução do reconhecimento facial, o sistema de câmeras era usado basicamente para registrar e monitorar o movimento nas áreas públicas. Com o novo sistema, as câmeras podem agora não apenas filmar, mas também identificar pessoas em tempo real, proporcionando um controle mais preciso sobre quem circula pela região. O reconhecimento facial permite a identificação de pessoas em tempo real, sem que elas saibam que estão sendo observadas, ampliando o controle sobre o espaço público. Por exemplo, as câmeras capturam imagens de pessoas nas ruas e as comparam com bancos de dados de suspeitos ou infrações, permitindo uma identificação automática e constante. Esse controle mais preciso e “assertivo” potencializa uma estratégia de securitização militar, contribuindo para uma gestão da segurança pública que tem se voltado para a ampliação do controle sobre os corpos e os comportamentos no espaço público.

Esse novo sistema se conecta aos programas anteriores, como o Segurança Presente, que já contava com câmeras instaladas em pontos estratégicos para monitorar o que acontecia nas ruas. O reconhecimento facial torna esse monitoramento mais eficiente e invasivo, transformando a vigilância passiva em uma forma de monitoramento ativo.

O monitoramento e a vigilância do projeto piloto, além de sua componente técnica, possui determinantes sociais. O sistema para operar requer avaliação

humana e múltiplas verificações, desde a análise das imagens até a abordagem e conferência por parte da polícia (Cardoso, 2024). Primeiro, os operadores do CICC verificam os alertas gerados pelas câmeras, controlando se as informações transmitidas correspondem a imagens identificadas e a imagens existentes no banco de dados. Podem teoricamente verificar possíveis erros, como falhas na qualidade das imagens ou falsos positivos. Além disso, eles ficam na frente das telas monitorando as imagens produzidas em tempo real pelas câmaras e acionam a equipe quando são identificados comportamentos e situações suspeitas.

Em entrevista, o pesquisador Bruno Cardoso (17 de abril. 2024), aponta mais um elemento de vigilância ostensiva referente à transferência informal de imagens de câmeras de segurança para celulares pessoais de policiais. Esse uso desregulado agrava a vulnerabilidade de pessoas já estigmatizadas, e a disseminação dessas imagens em grupos informais e milicianos cria um ambiente de insegurança, onde a privacidade é constantemente violada e a perseguição violenta pode ser facilitada.

Além disso, o monitoramento pelo operador pode ser marcado pelo "tédio" inerente à vigilância, que leva a um olhar excessivo sobre atividades não relevantes para a segurança (Firmino e Trevisan, 2012), misturando elementos de controle, voyeurismo e espetáculo (Smith, 2004; Cardoso, 2010). Por um lado, conforme destacado por Bruno Cardoso em entrevista (17 de abril. 2024), a ação humana pode levar à suspeição injusta de civis comuns, com o risco de que preconceitos sociais influenciam de forma tendenciosa a análise das imagens, prejudicando especialmente minorias e pessoas em situação de vulnerabilidade. Por outro lado, pode incentivar uma prática de vigilância ostensiva e ampliada, que invade a privacidade em espaços privados como também público pelo poder de monitoramento que os operadores possuem.

Essa situação levanta importantes questões éticas e operacionais que deveriam ser devidamente tratadas nos treinamentos dos operadores. A entrevista realizada revela que a formação oferecida é extremamente breve, “não durando mais do que 15 minutos” e é ofertada pelos operadores já treinados. É um treinamento meramente técnico sobre as funcionalidades do sistema, mas “não existe um treinamento sobre o olhar da vigilância, que ensina como observar, o que observar e de que forma”. Além disso, frequentemente, os operadores são policiais aposentados

ou sob investigação. Isso revela que o funcionamento do sistema é tratado apenas como uma questão técnica, ignorando inclusive suas implicações sociais. Como resultado, o sistema tende a reproduzir uma estrutura opressora e preconceituosa, dependendo da forma como os operadores o utilizam e tomam decisões. Isso caracteriza uma nova complexidade na forma como a vigilância opera.

O caso do projeto piloto, portanto, reproduz uma lógica de uso e implementação da tecnologia com finalidades de vigilância e controle. Assim como apontado em entrevista pelo pesquisador Pablo Nunes (24 de abril de 2024), a tecnologia poderia contribuir para grandes avanços no combate ao crime e à violência urbana, mas está principalmente aplicada para operar uma vigilância e controle social.

Apesar das problemáticas éticas e sociais levantadas pelo projeto piloto, o discurso governamental persiste em sua manutenção e ampliação. Isso gera um clima de disputa política, que envolve também as organizações da sociedade civil, fazendo com que surja movimentos pelo banimento do reconhecimento facial, como a campanha “tire meu rosto da sua mira”²⁸, lançada por cerca de 60 organizações sociais, denuncia o uso abusivo e opaco dessa tecnologia (figura 8). A falta de transparência no seu funcionamento e a ausência de regulamentação clara para o seu uso em contextos públicos acendem um alerta para as violações de direitos que essas práticas podem representar. Um dos aspectos mais preocupantes é que o Brasil, terceiro país com maior população carcerária no mundo, apresenta um histórico de superencarceramento que afeta desproporcionalmente as populações negras e periféricas. Nesse contexto, o uso de reconhecimento facial tende a reforçar essas desigualdades, contribuindo para um ciclo de criminalização e encarceramento seletivo.

²⁸Sociedade civil faz campanha para banir reconhecimento facial na segurança pública #TireMeuRostoDaSuaMira. Disponível em: <https://tiremeurostodasuamira.org.br/cdr-sociedade-civil-faz-campanha-para-banir-reconhecimento-facial-na-seguranca-publica/?utm_source=chatgpt.com>. Acesso em: 19 dez. 2024.

Figura 8 - Tire o meu rosto da sua mira



Fonte: site oficial da campanha

A crítica mais contundente diz respeito ao viés racial embutido nesses sistemas. Estudos globais, inclusive os citados pela campanha, mostram que tecnologias de reconhecimento facial apresentam margens de erro significativamente maiores ao lidar com pessoas negras, trans e outros grupo minorizados. Esse fator agrava as práticas racistas no Brasil, onde o racismo estrutural já influencia a atuação de forças de segurança. A tecnologia, ao invés de ser uma ferramenta neutra de justiça, torna-se um amplificador de discriminações contribuindo para abordagens violentas, prisões injustas e até mesmo mortes e confrontos que poderiam ter sido evitados.

Essa campanha entre os movimentos sociais vêm mobilizando um movimento multipartidário que busca o seu banimento. A campanha #SaiDaMinhaCara²⁹, que conta com a adesão de mais de 50 parlamentares de diferentes espectros políticos (figura 9), sinaliza um crescente consenso sobre os riscos dessa tecnologia, que é vista como invasiva e discriminatória. Os projetos de lei em andamento são uma resposta à expansão acelerada do reconhecimento facial sob o pretexto de promover segurança pública. A iniciativa #SaiDaMinhaCara, que mobiliza organizações como a

²⁹ Parlamentares de todas as regiões do Brasil apresentaram projetos de lei pelo banimento do reconhecimento facial em espaços públicos. Disponível em: <<https://idec.org.br/release/parlamentares-de-todas-regioes-do-brasil-apresentam-projetos-de-lei-pelo-banimento-do>>. Acesso em: 19 dez. 2024.

Coding Rights, CESeC, IDEC e MediaLab-UFRJ, vai além de uma simples oposição ao reconhecimento facial. Ela é uma tentativa de interromper a lógica do policiamento digital, que não só é ineficaz, mas também profundamente injusta. O uso dessa tecnologia nas ruas das cidades brasileiras deve ser desafiado, pois ele não oferece segurança real, mas sim reforça um sistema de vigilância que oprime e marginaliza os mais vulneráveis. O caminho para a segurança pública deve ser outro: não baseado no controle massivo e na vigilância, mas em políticas públicas inclusivas e eficazes que realmente promovam a paz e a justiça para todos, sem discriminação.

Figura 9 - Campanha pelo banimento do reconhecimento facial

Parlamentares de todas as regiões do Brasil apresentam projetos de lei pelo banimento do reconhecimento facial em espaços públicos



Coding Rights · [Follow](#)

Published in Coding Rights · 7 min read · Jun 21, 2022

Fonte : Coding Right

Embora diversas iniciativas pelo mundo, incluindo no Brasil, defendam maior regulamentação ou até mesmo o banimento dessa tecnologia, a perspectiva predominante aponta para a continuidade e aprofundamento do vigilantismo como estratégia de segurança pública. Essa direção destaca o reconhecimento facial como uma ferramenta amplamente defendida em programas governamentais, apesar das crescentes preocupações.

A despeito das preocupações, há um interesse crescente das autoridades em ampliar o uso do reconhecimento facial, como observado no caso do projeto piloto, que até mesmo serviu como plataforma de propaganda eleitoral. Isso reflete a

perspectiva de que o sistema de reconhecimento facial é uma solução simplificada e neutra para problemas complexos como a criminalidade, o que contribuiu para eleger candidatos como Wilson Witzel e 17 outros prefeitos em 26 municípios (MELLO, 2021).

A vigilância por reconhecimento facial desta maneira acaba por desafiar a noção de espaços públicos abertos e inclusivos, expondo grupos vulneráveis a novos constrangimentos. A partir daqui, é imperativo questionar a discriminação e a privação de direitos adquiridos, revertendo os significados de espaço como aberto e inclusivo, e expondo grupos vulneráveis a novos constrangimentos no direito à cidade.

3.4. Segregação sociotécnica

A expansão indiscriminada de projetos de vigilância tecnológica, sem uma análise crítica de seus impactos sociais e técnicos, revela uma tecnologia que está sendo usada para reforçar a segregação social e territorial, na qual antigos espaços de encontro, convivência e cidadania, transforma-se em um território de controle e monitoramento seletivo, onde determinados corpos — sobretudo os de jovens negros e moradores de periferias — são constantemente vigiados e criminalizados.

A vigilância ostensiva em bairros como Copacabana, seguida de sua implementação no Maracanã, ambos espaços de alta visibilidade e interesse econômico, demonstra uma clara priorização de áreas turísticas em detrimento de regiões periféricas, onde populações marginalizadas continuam expostas à violência e à arbitrariedade das operações policiais.

Desde a prova de conceito realizada pela Secretaria de Polícia Militar em 2019, a tecnologia foi apresentada como um avanço no combate ao crime. Com câmeras de alta definição capazes de captar rostos a até 25 metros de distância e transmitindo imagens para o Centro Integrado de Comando e Controle (CICC), o sistema foi promovido como uma solução inovadora. No entanto, o uso dessas câmeras de vigilância vai além do simples monitoramento urbano, assumindo um papel na manutenção de um estado de controle militarizado, onde os cidadãos, em especial os mais vulneráveis, são submetidos a uma constante vigilância. A vigilância não é neutra; ela opera dentro de uma estrutura de poder que prioriza o controle sobre a segurança, beneficiando alguns enquanto marginaliza e exclui outros.

Os efeitos do controle são evidentes no caso da apreensão indevida de uma das entrevistadas na realização do segundo teste do Projeto Piloto. Ela foi subitamente levada à delegacia enquanto trabalhava, após ser confundida com uma fugitiva que, mais tarde, descobriu-se estar presa desde 2015. O sistema utilizou uma correspondência com 70% de probabilidade, evidenciando falhas tanto na própria tecnologia quanto na sua integração com bases de dados atualizadas, como as do Conselho Nacional de Justiça. Após o acontecimento, a vítima de erro relata usar moleton para se esconder das câmeras mesmo sem dever nada à justiça.

Por operarem de forma silenciosa e "invisível", as instalações do projeto piloto impossibilitaram que a entrevistada soubesse o momento exato em que estava sendo identificada, bem como o motivo real. O sistema, portanto, opera de forma mais sutil, tornando difícil sua percepção e questionamento. Entrevistas realizadas no local revelam um desconhecimento generalizado sobre a existência dos sistemas de reconhecimento facial, expondo a falta de transparência no processo de implantação dessa tecnologia. Esse cenário é agravado pelo ceticismo de comerciantes locais nas entrevistas, que questionam tanto a eficácia quanto as reais intenções por trás do sistema.

Enquanto o reconhecimento facial é mais intensamente aplicado em áreas comerciais e turísticas, as periferias permanecem desassistidas em termos de segurança pública, enquanto continuam sujeitas a uma vigilância seletiva e abusiva. O projeto piloto consolida uma tecnologia que opera como um instrumento de controle social que gera uma sensação de constante vigilância e insegurança psicológica para as populações socialmente mais fragilizadas, como no caso citado acima. Embora promovida como uma ferramenta para garantir a segurança, a vigilância em massa demonstra que o papel do Estado está centrado em controlar, identificar e punir seus cidadãos, principalmente em espaços públicos e eventos culturais, que deveriam ser locais de liberdade e expressão. Se não houver uma regulação clara e eficaz, continuaremos a caminhar para uma sociedade onde o monitoramento massivo se tornará parte do cotidiano, colocando em risco nossas liberdades fundamentais.

A seletividade territorial do projeto piloto reforça a ideia de que certos espaços urbanos precisam ser menos perigosos e, portanto, precisam ser protegidos de ameaças "externas". Ao atingir populações mais vulneráveis, o projeto piloto opera

como outros sistemas e estratégias que frequentemente dificultam o acesso de moradores de favelas e subúrbios a regiões da zona sul do Rio de Janeiro. Durante o verão, por exemplo, operações de segurança são intensificadas, criando barreiras adicionais para quem tenta acessar espaços como Copacabana, cujo histórico de exclusão se agrava com os sistemas de videomonitoramento e reconhecimento facial.

Essa dinâmica constroi novas formas de pertencimento e exclusão no uso do espaço público. A presença de moradores de favelas e periferias, longe de ser vista como parte de uma convivência democrática e plural, é encarada sob a lente da vigilância e contenção. O projeto piloto, apesar de alegar a proteção de bairros turísticos, não gera uma verdadeira sensação de segurança, mas sim promove uma vigilância seletiva e ineficaz, que criminaliza determinados grupos sociais. Com isso, o projeto piloto não apenas se compromete com o aumento da segurança, mas também contribui para a construção de um "outro" social, reforçando a exclusão e estigmatização dessas populações, tratadas como alvos permanentes de suspeita e controle. Esse processo, em última instância, perpetua a segregação urbana e limita o direito à cidade, dificultando o acesso pleno e igualitário aos espaços públicos.

Tal abordagem aprofunda a segregação e reforça preconceitos, ao mesmo tempo que prioriza a proteção de uma imagem de segurança voltada ao turismo e ao consumo, deixando em segundo plano a criação de uma segurança pública mais inclusiva. Assim, o uso de ferramentas tecnológicas como o reconhecimento facial não só cerceia liberdades individuais, mas intensifica a segregação social. A ideia de que a tecnologia é mais um meio de controle do que de proteção indica que as populações vulneráveis não são vistas como cidadãs plenas, mas como alvos de monitoramento.

Assim, além da sensação de vigilância, essa constante presença de câmeras e dispositivos de segurança contribui para a estigmatização das populações vulneráveis, mas também amplifica as desigualdades sociais. Dados da Rede de Observatórios da Segurança (2019) indicam que 90% das pessoas presas por reconhecimento facial eram negras, sendo o Rio de Janeiro responsável por 37% desses casos. Uma moradora de Copacabana entrevistada revelou seu temor de ser presa por causa dos erros do sistema: "Sempre que estou com amigas brancas, acham que eu sou a empregada. Tenho medo de ser presa por esse sistema só por

ser negra”. Isso revela um sistema tecnológico que, por trás de uma legitimidade técnica, perpetua o racismo estrutural.

Esse dado é cruel frente a política pública de segurança, pois expõe como as tecnologias de segurança vem reproduzindo as dinâmicas de um racismo estrutural já presente nas práticas políticas tradicionais, abrindo portas para questionar qual o papel da tecnologia no fortalecimento de um controle social diferenciado, na qual a cor da pele e o local de residência continuam a determinar quem é considerado suspeito. A partir deste dado, é possível questionar como o racismo é incorporado nas novas tecnologias e confrontar a narrativa de que a ferramenta, como o reconhecimento facial, são “objetivas” e livres de viés.

Aqui a disputa é clara: de um lado, o governo que busca projetar a imagem de um estado que traz ordem e segurança às comunidades, usando a tecnologia como símbolo progressivo. Por outro lado, uma análise crítica revela que essas políticas e tecnologias perpetuam violências de longa data, transformando o direito à cidade em um privilégio para poucos e reforçando uma lógica de exclusão racializada.

Podemos questionar a legitimidade e a neutralidade técnica do projeto piloto também com base nos dados sobre as apreensões no entorno do Maracanã. De acordo com o Relatório Panóptico (2020), houve um número alarmante de falsos positivos, destacando que, dos 11 detidos na área, apenas quatro possuíam mandados de prisão. Esse índice de 63% de erro expõe como o sistema, em vez de promover segurança, reforça práticas discriminatórias, muitas vezes atingindo a população negra, já que a tecnologia frequentemente falha em reconhecer corretamente rostos negros e de outras minorias. A experiência do projeto piloto corrobora com outras pesquisas, como aquela da London Police Facial Recognition Failures (2020)³⁰, que comprovam que sistemas de reconhecimento facial frequentemente cometem erros, principalmente em relação a pessoas de pele mais escura, além de não haver evidências sólidas de que essas ferramentas contribuem para a diminuição de crimes violentos em áreas onde foram implementadas.

Além disso, os dados evidenciam a fragilidade dos sistemas de vigilância, que não apenas reforçam desigualdades, mas também contribuem para a chamada

³⁰ CLIFTON, H. Meadowhall facial recognition scheme troubles watchdog. 28 Jan. 2020.

"insegurança sobreposta" em contextos informais de livre circulação, como sugerem Colak, Lombard e Guarneros-Meza (2023). Um exemplo claro disso é o caso de Josiete Pereira do Carmo (figura 10), presa em Copacabana após ser erroneamente identificada pelo sistema de reconhecimento facial como foragida. Josiete havia sido alvo de um mandado de prisão preventiva de 2012, que, embora já não estivesse mais em vigor, permanecia incorretamente nos registros.

Figura 10 - Falhas do projeto piloto

Rio

Mulher identificada por reconhecimento facial em Copacabana é solta após erro em sistema ser constatado

Registro de ocorrência contra ela, feito em delegacia para onde foi levada, será cancelado

Por **Felipe Grinberg** e **Vera Araújo** — Rio de Janeiro

04/01/2024 11h54 · Atualizado há 11 meses



Fonte: O Globo

Esse caso expõe a ineficácia e a falta de confiabilidade dos bancos de dados utilizados nesses sistemas de vigilância. Apesar de estar cumprindo sua pena, Josiete foi presa devido a um mandado que não havia sido devidamente retirado dos registros. Esse erro ilustra como muitos mandados continuam constando nos sistemas, mesmo após terem perdido sua validade legal. A desatualização dessas informações, como no caso do sistema de foragidos utilizado pela Polícia Militar e Civil, revela a precariedade de sua operação.

Outro elemento preocupante quando se pensa a neutralidade do sistema é a compreensão de que o sistema de videomonitoramento, inclusive de reconhecimento facial, é determinado pela ação humana, por interesses políticos e econômicos. Conforme entrevista realizada com o pesquisador Bruno Cardoso (17 de abril. 2024), existe uma pressão para que o projeto piloto gere resultados concretos, assim "a pressão para produzir flagrantes reforçava a própria narrativa de segurança que eles

queriam vender". Para tanto, os operadores do CICC, que usam o sistema e monitoram as imagens, direcionam as câmeras à procura do flagrante para justificar os investimentos públicos com o sistema. Além disso, as empresas privadas que fornecem a tecnologia para o projeto piloto, como a Oi e a Huawei, operam com uma lógica de mercado e coleta de dados que exige a produção de flagrantes. Observamos, portanto, interesses políticos e econômicos em fazer assim que o sistema opere e gere algum tipo de resultado.

Nesse processo, os operadores do CICC focam na coleta de evidências, direcionando sua atenção a determinados perfis sociais. A identificação do "suspeito" e do "anômalo", mesmo quando não há evidências concretas de envolvimento com atividades ilícitas, é guiada por estruturas sociais pré-existentes.

A associação entre determinados grupos sociais e o risco de criminalização guia o olhar e o monitoramento automático. Quando o olhar procura pessoas negras, "faveladas" e "periféricas", reproduz estigmas raciais e territoriais, reforçando preconceitos e medidas de controle que intensificam a segregação social. A tecnologia, assim, pode ser tendenciosamente utilizada, atingindo os mais vulneráveis e reforçando uma divisão social que marginaliza aqueles já estigmatizados, como os "meninos de rua". Segundo a entrevista com o pesquisador Tarcízio Silva (19 mai. 2024), os erros do sistema de reconhecimento facial, somados à forma como os operadores utilizam a tecnologia, demonstram que o projeto piloto não apenas falha em reduzir a exclusão social, mas também reforça a aceitação da violência estatal. Ao invés de promover segurança e justiça social, ele intensifica o controle sobre corpos racializados e marginalizados, sobretudo pessoas negras e pobres. A vigilância, ao se concentrar nesses grupos, reforça as estruturas sociais e de poder que os marginalizam, criando uma dinâmica de criminalização baseada em estereótipos.

No entanto, esse enfoque sobre a identificação e punição criminal mascara a verdadeira função do projeto: o controle socioespacial e a exclusão de certos grupos da vida urbana. A vigilância, aqui, é menos sobre segurança pública e mais sobre quem tem o direito de circular e apropriar-se do espaço urbano. O uso de câmeras, como aponta Lannes-Fernandes (2012), opera tanto como barreira física quanto simbólica, delimitando quem pode ou não participar da vida urbana. Como observado

em campo, a instalação de câmeras se dá em pontos estratégicos, como entradas de bairros e áreas de grande movimentação, reforça uma vigilância ostensiva e cria uma sensação de controle.

As "barreiras simbólicas" dessa vigilância, mesmo que intangíveis, geram uma exclusão social velada, ao delimitar "áreas seguras" e "áreas de risco". Este tipo de controle seletivo estabelece fronteiras invisíveis que limitam a participação de certos grupos no espaço urbano, contribuindo para sentimentos de rejeição, desconforto e desvalorização de suas presenças.

Essas barreiras não são neutras, mas refletem a perpetuação de desigualdades estruturais. O projeto piloto mencionado utiliza mecanismos coercitivos para reforçar essas divisões, fazendo uso de força física, ameaças e pressão psicológica. Assim, o controle socioespacial se materializa na distinção social com base em classe, raça e local de residência. Esse processo de exclusão, longe de ser ocasional, é parte de uma lógica de segregação que molda o espaço urbano ao gosto das elites, restringindo a pluralidade e reforçando hierarquias sociais que marginalizam e excluem.

Por fim, tanto os moradores quanto os comerciantes destacam a falácia de usar a tecnologia como uma solução rápida para problemas estruturais, como a violência policial, a desigualdade social e a marginalização de certas áreas da cidade. A crítica a esse tipo de política de segurança é a de que ela desvia a atenção das causas profundas da insegurança e do crime, oferecendo uma resposta superficial que, em vez de resolver, intensifica as tensões existentes. Para esses grupos, a verdadeira solução passa por uma abordagem mais humana e integrada de segurança pública, que envolva a comunidade, promova a justiça social e invista em políticas públicas que reduzam as desigualdades e o medo.

O discurso de "segurança" e "modernização" muitas vezes oculta o impacto devastador dessas ações sobre as vidas nas favelas e nas periferias, perpetuando um ciclo de violência e marginalização. Essas práticas precisam ser analisadas em sua complexidade, levando em consideração o papel do Estado na manutenção e ampliação dessas desigualdades, bem como os interesses políticos e econômicos que alimentam a continuidade dessa violência sistêmica.

A própria Polícia Militar do Rio de Janeiro admite que o sistema precisa ser avaliado quanto à sua viabilidade econômica e técnica. Embora o coronel tenha afirmado que, após os testes, haverá um processo licitatório para a contratação da empresa responsável, ainda não há clareza sobre os custos totais de implementação em larga escala. O cerne da questão revela uma disputa narrativa entre, por um lado, o discurso de "segurança" que justifica a ampliação do aparato de vigilância e repressão como um bem comum e, por outro, o impacto real dessas políticas, que perpetuam o racismo estrutural e aumentam a vulnerabilidade das populações mais marginalizadas. A dependência de empresas privadas para gerir uma ferramenta de tamanha sensibilidade, como o reconhecimento facial, levanta questionamentos sobre o papel do Estado em garantir que os direitos dos cidadãos sejam preservados. A Oi, que participou dos testes, não terá garantido seu papel no futuro, mas o processo em si já sinaliza a crescente privatização da segurança pública.

Organizações como o Instituto Brasileiro de Defesa do Consumidor (Idec) alertam para os riscos de vazamento ou má utilização dessas informações. Bárbara Simões, advogada e pesquisadora do programa de direitos digitais do Idec, destaca a necessidade de garantir a segurança dos dados pessoais coletados, uma vez que esses dados podem ser vendidos por empresas privadas ou manipulados de maneira inadequada, comprometendo a privacidade de milhões de cidadãos. Ela questiona o uso da tecnologia sem uma clara regulamentação e sem garantias de que as informações não serão usadas de forma prejudicial, ou seja, o debate sobre o uso dessa tecnologia deve ir além da eficiência no combate ao crime, questionando os limites do controle estatal e os efeitos de uma vigilância cada vez mais abrangente na liberdade e nos direitos fundamentais da população.

A tecnologia foi testada de maneira exaustiva durante eventos de grande porte, o que, segundo o porta-voz da Polícia Militar Fliess, permitiu uma avaliação robusta de seu funcionamento sob pressão e que agora, a intenção é aplicar os testes em situações do cotidiano, para assegurar sua eficácia, além de eventos esporádicos. No entanto, a ampliação do uso de reconhecimento facial durante eventos patrocinados pelo governo, como o recente show da Madonna ou o futuro show de Lady Gaga, assim como o Réveillon e o G20, reflete uma normalização do monitoramento constante e o avanço de um regime de vigilância perversa.

O uso crescente de reconhecimento facial no Rio de Janeiro, justificado como uma medida para aumentar a segurança pública, escancara uma perigosa tendência de ampliação da vigilância estatal sem a devida transparência ou avaliação crítica. A falta de clareza sobre os custos e a viabilidade técnica desse sistema, somada à crescente dependência de empresas privadas para sua gestão, aponta para uma privatização disfarçada da segurança pública, colocando em risco a proteção dos direitos dos cidadãos. Além disso, ao normalizar o monitoramento constante em eventos de grande porte e agora no cotidiano, como demonstra a aplicação durante shows e celebrações, o Estado avança na criação de um regime de vigilância pervasiva que impacta diretamente a liberdade individual, sobretudo das populações mais vulneráveis.

Esse cenário exige uma reflexão crítica sobre os reais objetivos por trás da implementação dessa tecnologia. A promessa de segurança muitas vezes serve como uma cortina de fumaça para a expansão de um aparato de controle que perpetua o racismo estrutural e aprofunda desigualdades sociais. Sem uma regulamentação robusta e mecanismos que garantam a transparência e o uso responsável dos dados, o reconhecimento facial se transforma em mais uma ferramenta de repressão, exacerbando o controle estatal sobre a população sob o pretexto de segurança. O debate, portanto, deve ir além da questão técnica e questionar a quem realmente serve essa vigilância ampliada e quais as suas implicações para as liberdades fundamentais.

CONCLUSÃO 4

A introdução do reconhecimento facial em espaços públicos, particularmente em cidades brasileiras como o Rio de Janeiro, como é o caso do Projeto Piloto, levantou uma série de debates críticos sobre suas implicações em termos de vigilância, controle social e militarização. O que inicialmente foi apresentado como uma inovação tecnológica para o combate à criminalidade rapidamente se transformou em um instrumento poderoso de controle sobre a população, especialmente nos territórios mais vulneráveis. O reconhecimento facial, ao se aliar à militarização do espaço público, impõe novos desafios para o direito à cidade e para a democracia. A tecnologia, que deveria servir à segurança pública, acaba por reforçar as desigualdades sociais e espaciais que estruturam as cidades brasileiras.

O uso de reconhecimento facial em larga escala não apenas amplia o alcance da vigilância, mas também redefine as dinâmicas sociais e espaciais nas cidades. À medida que câmeras de videomonitoramento se proliferam a cada fase do projeto piloto em áreas de grande circulação e locais considerados estratégicos, os indivíduos se tornam sujeitos a uma vigilância constante, um fenômeno que impacta diretamente seu comportamento. O espaço público, que deveria ser um ambiente livre para o encontro e a convivência, transforma-se gradualmente em um território de controle, onde as pessoas não mais se sentem plenamente à vontade para circular ou interagir.

Essa onipresença tecnológica altera a percepção do espaço, fazendo com que muitos se sintam observados e monitorados o tempo todo, o que pode gerar um ambiente de tensão e desconforto. A sensação de vigilância constante contribui para uma mudança no comportamento das pessoas, que passam a agir de forma mais cautelosa ou a evitar certos espaços. Além disso, a implementação do reconhecimento facial carrega consigo um viés racial que torna essa tecnologia particularmente prejudicial para grupos historicamente marginalizados, como jovens negros e moradores de favelas, que frequentemente se tornam os alvos preferenciais da vigilância seletiva.

Ao invés de promover a segurança, o projeto piloto de reconhecimento facial, em larga escala, pode intensificar as desigualdades existentes, criando ainda mais um ciclo de criminalização de grupos já vulneráveis. A utilização indiscriminada dessa tecnologia nos espaços públicos, ao invés de proteger, impõe um tipo de segurança que exclui e ameaça os direitos fundamentais de liberdade e privacidade desses indivíduos. Assim, o que deveria ser uma medida de proteção torna-se, na prática, uma forma de controle social e estigmatização, aprofundando a segregação e a desconfiança entre a população e o Estado.

A coleta massiva de dados biométricos, especialmente por meio do reconhecimento facial, levanta sérias questões relacionadas à privacidade e aos direitos individuais dos cidadãos. Essa tecnologia permite que imagens faciais e informações pessoais sejam capturadas de maneira automática, muitas vezes sem o consentimento explícito ou o conhecimento dos indivíduos, configurando uma violação de direitos fundamentais, como o direito à privacidade e à liberdade. O fato de que essas informações possam ser coletadas em locais públicos, sem qualquer

aviso claro, transforma a noção de privacidade em algo cada vez mais intangível. Além disso, a forma como esses dados são armazenados, processados e compartilhados permanece envolta em um manto de opacidade, criando uma atmosfera de desconfiança generalizada. A falta de transparência nas práticas de coleta e tratamento dos dados biométricos gera incertezas sobre quem realmente tem acesso a essas informações e de que maneira elas são usadas.

Essas questões raramente são adequadamente abordadas pelas autoridades responsáveis pela implementação dos sistemas de reconhecimento facial, o que aumenta os riscos de abusos e violações dos direitos humanos. A falta de regulamentação clara e de um debate público robusto sobre os limites éticos e legais da coleta de dados biométricos alimenta a sensação de impunidade e de vulnerabilidade das pessoas frente a uma vigilância cada vez mais invasiva. Sem uma governança responsável, esses dados podem ser utilizados de maneira indiscriminada, seja para fins comerciais, políticos ou de controle social, criando um ambiente propício para discriminação, manipulação ou repressão, especialmente de grupos marginalizados.

A introdução dessa tecnologia exige uma reflexão crítica sobre o equilíbrio entre segurança e privacidade, e a urgência de estabelecer regulamentações que garantam a proteção dos direitos individuais e a transparência na gestão desses dados. Sem uma regulação adequada, a coleta massiva de dados biométricos corre o risco de transformar a privacidade em um conceito obsoleto, colocando em risco a liberdade e os direitos civis dos cidadãos em nome de uma segurança que, muitas vezes, exclui os próprios princípios da democracia e da justiça social.

A aplicação seletiva da vigilância por reconhecimento facial no Rio de Janeiro agrava a segregação sociotécnica, criando um ambiente em que a tecnologia é usada de forma desigual, refletindo e reforçando as disparidades sociais e raciais da cidade. Enquanto as áreas mais ricas e de classe média recebem vigilância discreta e "silenciosa", com câmeras de reconhecimento facial instaladas em locais estratégicos e de alto fluxo, as comunidades mais pobres e racializadas, como as favelas e periferias, são monitoradas com tecnologias mais invasivas, muitas vezes acompanhadas de um aparato militarizado. Essa disparidade não se limita ao controle de segurança, mas também está associada à falta de políticas públicas básicas

nessas regiões, com a presença de repressão mais intensa em vez de serviços essenciais.

Essa realidade cria uma "geografia da exclusão", na qual as diferenças espaciais tornam-se evidentes e refletem diretamente no tratamento desigual das populações. Enquanto bairros ricos desfrutam de vigilância discreta voltada à segurança, as favelas e periferias se veem marcadas por uma vigilância excessiva, voltada para o controle e a criminalização de seus moradores. O uso intensivo de tecnologia para monitoramento nessas áreas reforça a narrativa de que seus habitantes são suspeitos em potencial, contribuindo para uma lógica de criminalização da pobreza e da marginalização social.

Essa forma de vigilância não apenas fortalece a ideia de que a pobreza é um crime, mas também intensifica a estigmatização dos moradores dessas comunidades, tratando-os como se fossem sempre uma ameaça em potencial. O efeito disso é uma constante violação dos direitos civis e humanos de pessoas que já enfrentam enormes desafios sociais e econômicos. A vigilância seletiva contribui, assim, para o aprofundamento das desigualdades existentes, perpetuando um ciclo de exclusão e marginalização que afeta a confiança da população nas instituições e na segurança pública.

O impacto dessa vigilância é profundo, pois não se trata apenas de monitorar e controlar, mas de reforçar as divisões sociais e raciais, transformando as cidades em espaços onde as pessoas são constantemente lembradas de sua posição na hierarquia social. Esse processo não só dificulta a luta por direitos e por uma vida digna, mas também impede a construção de uma sociedade mais justa e igualitária, onde todos têm acesso aos mesmos direitos e oportunidades.

O discurso oficial em torno da implementação do reconhecimento facial costuma ser pautado pela narrativa da modernização da segurança pública. A tecnologia é apresentada como uma ferramenta eficiente e neutra, capaz de aprimorar a capacidade do Estado de combater o crime e proteger a população. No entanto, essa retórica ignora os impactos desiguais e os problemas éticos associados ao uso dessa tecnologia. O reconhecimento facial não é neutro; ele carrega em si um viés que reflete as desigualdades raciais e socioeconômicas presentes na sociedade.

Aqueles que estão à margem são os que mais sofrem com os efeitos dessa vigilância ampliada.

A militarização do espaço público, no entanto, não é um fenômeno novo no Brasil. Cidades como o Rio de Janeiro já possuem uma longa história de militarização, onde a presença de forças de segurança nas ruas, favelas e periferias é uma constante. O reconhecimento facial surge como mais uma ferramenta nesse processo de militarização, ampliando a capacidade do Estado de monitorar e controlar os cidadãos. Quando aliado a outras formas de vigilância, como o uso de drones e câmeras de segurança, o reconhecimento facial contribui para uma presença cada vez mais ostensiva do aparato militarizado em áreas urbanas.

Essa militarização, no entanto, não está distribuída de forma equitativa pelo espaço urbano. As áreas mais militarizadas são aquelas onde vivem as populações mais vulneráveis, como os moradores de favelas e periferias. Essas áreas, já estigmatizadas pela violência policial, tornam-se os principais alvos do reconhecimento facial e de outras formas de vigilância. A tecnologia, ao invés de promover a segurança, intensifica as tensões entre os moradores dessas áreas e as forças de segurança, resultando frequentemente em abordagens violentas e arbitrárias.

O caso do Projeto Piloto de reconhecimento facial implementado no Rio de Janeiro é um exemplo claro de como a tecnopolítica da securitização está intimamente ligada à militarização do espaço público. O projeto foi distribuído de maneira estratégica, priorizando áreas de grande circulação e proximidade com favelas, com o objetivo de monitorar e identificar pessoas com mandados de prisão em aberto. No entanto, o impacto do projeto foi muito além da simples identificação de suspeitos. Ele criou uma atmosfera de vigilância constante que afeta a liberdade de movimento e a privacidade dos cidadãos.

A militarização do espaço urbano também tem consequências graves para o convívio social. A presença constante de forças de segurança e de tecnologias de reconhecimento facial cria um ambiente de medo e desconfiança, onde o espaço público se transforma em um local de controle e repressão. Em vez de promover a segurança, a militarização frequentemente resulta em uma deterioração das relações

sociais, tornando o espaço urbano menos acessível e mais perigoso para aqueles que já vivem em condições de vulnerabilidade.

A segregação sociotécnica gerada pelo uso do reconhecimento facial e outras formas de vigilância reforça as desigualdades raciais e socioeconômicas que estruturam as cidades brasileiras. Ao tratar certas áreas e populações como alvos preferenciais da vigilância, o Estado contribui para a perpetuação de um sistema de controle que marginaliza e criminaliza os mais pobres. Essa segregação não é apenas espacial, mas também tecnológica, já que as tecnologias de vigilância são aplicadas de maneira seletiva, reforçando a divisão entre aqueles que são vigiados e aqueles que não são.

No Brasil, onde a desigualdade racial e socioeconômica é uma característica estrutural, o reconhecimento facial assume um papel especialmente problemático. A vigilância seletiva afeta principalmente os grupos mais vulneráveis, exacerbando a discriminação e a criminalização de suas existências. Jovens negros e moradores de favelas, que já enfrentam uma realidade de violência policial e estigmatização, são os mais afetados por essa tecnologia, que amplia ainda mais a desigualdade no acesso à cidade e à cidadania.

Ao discutir a implementação do reconhecimento facial no Rio de Janeiro através do projeto piloto, é crucial considerar os impactos sociais e éticos dessa tecnologia, bem como as dinâmicas de poder que ela reforça. A tecnopolítica da securitização, ao aliar vigilância e militarização, cria uma sociedade em que o controle sobre os corpos e movimentos dos cidadãos é cada vez mais intensificado.

Isso afeta profundamente o direito à cidade, a liberdade de circulação e a privacidade de todos os indivíduos, mas especialmente daqueles que já vivem à margem da sociedade. A crítica ao reconhecimento facial e à militarização do espaço público precisa, portanto, ser parte de um debate mais amplo sobre a segurança pública e os direitos humanos no Brasil. É necessário repensar as estratégias de segurança que priorizam a repressão em vez da inclusão, e que tratam certas populações como inimigos a serem controlados. Somente a partir de uma reflexão crítica sobre o uso dessas tecnologias será possível promover uma convivência urbana mais justa e democrática.

O futuro das cidades brasileiras depende de nossa capacidade de resistir à tentação de resolver problemas complexos de segurança pública com soluções tecnológicas simplistas. O reconhecimento facial, assim como outras tecnologias de vigilância, pode ser útil em certos contextos, mas quando aplicado de maneira indiscriminada e seletiva, ele contribui para a militarização do espaço urbano e para a perpetuação das desigualdades. É fundamental que o uso dessas tecnologias seja regulado de maneira transparente e democrática, garantindo que os direitos dos cidadãos sejam protegidos e que a vigilância não se transforme em um instrumento de opressão.

REFERÊNCIAS

- ABBAS DA SILVA, L. Franqueira; HARTMANN, I. A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. *Revista Digital de Direito Administrativo*, [S. l.], v. 8, n. 1, p. 171–204, 2021.
- ABDALA, Vitor. Polícia usará reconhecimento facial na final da Copa América. *Agência Brasil*, Rio de Janeiro, 2019. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2019-07/policia-usara-reconhecimento-facial-na-final-da-copa-america>. Acesso em: 10 ago. 2023.
- ABELLO COLAK, Alexandra; LOMBARD, Melanie; GUARNEROS-MEZA, Valeria. Framing urban threats: a socio-spatial analysis of urban securitisation in Latin America and the Caribbean. *Urban Studies*, v. 60, n. 14, 11 abr. 2023. Disponível em: <https://doi.org/10.1177/0042098023116094>. Acesso em: 9 jul. 2024.
- AGAMBEN, Giorgio. *Estado de exceção*. Tradução de Iraci D. Poleti. 2. ed. São Paulo: Boitempo, 2004.
- ARAÚJO, Fábio. *Das “técnicas” de fazer desaparecer corpos*. Rio de Janeiro: Lamparina, 2014.
- BARBOSA, K. de S.; LEHFELD, L. de S. A influência das tecnologias da informação e comunicação (TIC) e da Internet na segurança pública. *Anais do Congresso Brasileiro de Processo Coletivo e Cidadania*, [S. l.], n. 4, 2017. Disponível em: <https://revistas.unaerp.br/cbpcc/article/view/748>. Acesso em: 5 fev. 2024.
- BARCELOS, Iuri. São Paulo condena mais negros por tráfico, mesmo que portem menos drogas. *UOL Notícias*, 2019. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2019/05/06/sao-paulo-condena-mais-negros-por-trafico-mesmo-que-portem-menos-drogas.htm>. Acesso em: 18 set. 2023.
- BARROS, Rachel. Urbanização e "pacificação" em Manguinhos: um olhar etnográfico sobre sociabilidade e ações de governo. Tese (Doutorado). Instituto de Estudos Sociais e Políticos, 2016.
- BARROS, J. N. Big Data, proteção de dados e transparência: desafios para a consolidação da confiança e garantia dos direitos do cidadão. *Revista Culturas Jurídicas*, v. 7, n. 17, 2020.
- BARRY, A. *Political machines: governing a technological society*. London: Athlone Press, 2001.
- BARTIRA, M.; CARDOSO, F. S. O conceito de defesa social e segurança pública na ordem democrática brasileira. Bc.ufg.br, 2020.
- BECK, Ulrich. *World Risk Society: in search of lost security*. Frankfurt (Meno): Suhrkamp, 2007.

BISSI, Thelry David. Reconhecimento facial com os algoritmos Eigenfaces e Fisherfaces. *Bitstream*, 2018. Disponível em: <https://repositorio.ufu.br/bitstream/123456789/22158/3/>. Acesso em: 25 out. 2020.

BAUMAN, Zygmunt. *Comunidade: a busca por segurança no mundo atual*. Rio de Janeiro: Jorge Zahar, 2003.

BAUMAN, Zygmunt. *Globalização: as consequências humanas*. Rio de Janeiro: Jorge Zahar, 1999.

BOURDIEU, Pierre. *Décrire et prescrire. Note sur les conditions de possibilité et les limites de l'efficacité*. [S. l.]: [s.n.], [s.d.].

BRADFORD, B. et al. Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology. Disponível em: https://www.researchgate.net/publication/338499848_Live_Facial_Recognition_Trust_and_Legitimacy_as_Predictors_of_Public_Support_for_Police_Use_of_New_Technology. Acesso em: 24 jan. 2023.

BRAGA, Luiz Felipe Zenicola. *Sistemas de reconhecimento facial*. Monografia (Graduação em Engenharia Elétrica com ênfase em Eletrônica). Escola de Engenharia de São Carlos da Universidade de São Paulo, São Carlos, 2013.

BRASIL, Cristina Índio. Rio: programa de reconhecimento facial entra em operação no carnaval. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2019-01/rio-programa-de-reconhecimento-facial-entra-em-operacao-no-carnaval>. Acesso em: 1 fev. 2022.

BRUNO, F. et al. Tecropolíticas da vigilância: perspectivas da margem. Disponível em: https://www.researchgate.net/publication/329444654_Tecnopoliticas_da_Vigilancia_Perspectivas_da_Margem. Acesso em: 10 ago. 2023.

BRUNO, Fernanda. Máquinas de ver, modos de ser: visibilidade e subjetividade nas novas tecnologias de informação e de comunicação. *Revista Famecos*, 2019.

BUOLAMWINI, J. et al. Gender Shades: intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, v. 81, p. 1–15, 2018.

CALDEIRA, Teresa Pires do Rio. *Cidade de muros: crime, segregação e cidadania em São Paulo*. São Paulo: Edusp/Editora 34, 2001.

CANO, Ignacio; DUARTE, Tais. *No sapatinho: a evolução das milícias no Rio de Janeiro (2008–2011)*. Rio de Janeiro: Laboratório de Análise da Violência (LAV UERJ), 2012.

CARDOSO, Bruno. A lógica gerencial-militarizada e a segurança pública no Rio de Janeiro: o CICC-RJ e as tecnologias de (re)construção do Estado. *Dilemas - Revista de Estudos de Conflito e Controle Social*, v. 0, n. 0, p. 53–74, 2018.

CARDOSO, Bruno de Vasconcelos. Megaeventos esportivos e modernização tecnológica: planos e discursos sobre o legado em segurança pública. *Horizontes Antropológicos*, v. 19, n. 40, p. 119–148, 2013. Disponível em: <https://www.scielo.br/j/ha/a/5bdtVqQWfymmjTkFgyZzrwG/abstract/?lang=pt>. Acesso em: 14 abr. 2023.

CANO, I. *Execuções sumárias no Brasil: o uso da força pelos agentes do Estado (1997–2003)*. Rio de Janeiro: Justiça Global, 2003.

CAMPOS, Ana Cristina. Segurança e defesa para a Copa têm investimento de R\$1,9 bi. Disponível em: <https://exame.com/brasil/seguranca-e-defesa-para-a-copa-tem-investimento-de-r-1-9-bi/>. Acesso em: 10 ago. 2023.

CARVALHO, Monique Batista. Os dilemas da "pacificação": práticas de controle e disciplinarização na "gestão da paz" em uma favela no Rio de Janeiro. Tese (Doutorado). Programa de Pós-Graduação em Ciências Sociais, Universidade do Estado do Rio de Janeiro, 2014.

CASTELLS, Manuel. *A sociedade em rede: a era da informação: economia, sociedade e cultura*. 8. ed. São Paulo: Paz e Terra, 1999.

CASTRO, Demian Garcia; GAFFNEY, Christopher; NOVAES, Patrícia Ramos; et al. O Projeto Olímpico da Cidade do Rio de Janeiro: reflexões sobre os impactos dos megaeventos esportivos na perspectiva do direito à cidade. *Zora*, p. 11–40, 2015. Disponível em: <https://www.zora.uzh.ch/id/eprint/115002/>. Acesso em: 17 abr. 2023.

CERQUEIRA, Carlos Magno Nazareth. Questões preliminares para a discussão de uma proposta de diretrizes constitucionais sobre a segurança pública. *Revista Brasileira de Ciências Criminais*, ano 6, n. 22, p. 139–182, 1998.

COSTA, R. S.; KREMER, B. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. *Revista Brasileira de Direitos Fundamentais & Justiça*, [S. l.], v. 16, n. 1, 2022. DOI: 10.30899/dfj.v16i1.1316. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1316>. Acesso em: 30 nov. 2023.

DIAS, Erasmo. *Doutrina de Segurança e Risco: Segurança dos Cidadãos*. Ofício nº155. São Paulo: Departamento Técnico de Taquigrafia, 2003.

DITTON, J.; SHORT, E. Yes, it works, no, it doesn't: comparing the effects of open-street CCTV in two adjacent Scottish town centres. In: NORRIS, Clive; W., D. *Surveillance, crime and social control*. [S. l.]: Routledge, 2006. p. 201–223.

DINIZ, Fabio Abrantes. RedFace: um sistema de reconhecimento facial baseado em técnicas de análise de componentes principais e autôfaces. *Revista Brasileira de Computação Aplicada*, v. 5, n. 1, 27 maio 2013.

FONSECA, Felipe. *Reconhecimento facial e segurança pública no Brasil: questões jurídicas e éticas*. São Paulo: LTr, 2020.

FREITAS, L. F.; PEREIRA, R. S. Vigilância urbana e políticas de segurança: tecnologia e controle social. *Revista Brasileira de Segurança Pública*, v. 14, n. 2, p. 45–62, 2020.

GIDDENS, Anthony. *Modernity and self-identity: self and society in the late modern age*. Stanford: Stanford University Press, 1991.

GIACOMELLI, R. M. Segurança pública e tecnologias de monitoramento: impactos na vida urbana. *Revista Brasileira de Ciências Sociais*, v. 35, n. 103, p. 1–22, 2020.

GOMES, L. H.; COSTA, M. A. O uso de reconhecimento facial na prevenção de crimes em espaços públicos. *Revista de Direito e Tecnologia*, v. 5, n. 1, p. 87–105, 2021.

HALL, Stuart. *A identidade cultural na pós-modernidade*. Rio de Janeiro: DP&A, 2003.

HARCOURT, Bernard E. *Exposed: desire and disobedience in the digital age*. Cambridge: Harvard University Press, 2015.

HARVEY, David. *Cidades rebeldes: do direito à cidade à revolução urbana*. São Paulo: Editora UOL, 2013.

HOCHSCHILD, Arlie Russell. *The managed heart: commercialization of human feeling*. Berkeley: University of California Press, 1983.

KITCHIN, Rob. *Data and the city*. London: Routledge, 2014.

LATOUR, Bruno. *Reassembling the social: an introduction to actor-network-theory*. Oxford: Oxford University Press, 2005.

LEVINE, Naomi. *Surveillance, power and everyday life*. Oxford: Oxford University Press, 2019.

LIMA, C. R.; FERNANDES, T. Reconhecimento facial e desigualdade social: desafios éticos e legais. *Revista Brasileira de Políticas Públicas*, v. 12, n. 3, p. 45–67, 2022.

MATTOS, Marcelo. Polícia e território: tecnologias de controle em favelas do Rio de Janeiro. *Cadernos de Sociologia Urbana*, v. 10, n. 2, p. 101–122, 2018.

MIRANDA, L. A.; SOUZA, F. S. Reconhecimento facial e direitos humanos: análise de impacto e responsabilidade. *Revista de Direito Contemporâneo*, v. 15, n. 1, p. 77–95, 2021.

MONTAÑEZ, P. R. O uso de tecnologias de vigilância em megaeventos esportivos no Brasil: segurança e controle social. *Revista de Ciências Sociais Aplicadas*, v. 6, n. 1, p. 33–52, 2019.

MORO, Sergio. Reconhecimento facial: potencial e riscos para a segurança pública. *Jornal de Tecnologia e Sociedade*, v. 8, n. 2, p. 12–29, 2020.

NOGUEIRA, E. C.; BARRETO, J. F. Vigilância e monitoramento urbano: implicações para a cidadania. *Revista Brasileira de Estudos Urbanos*, v. 21, n. 4, p. 55–73, 2021.

OLIVEIRA, R. P. de. *Cidadania, espaço urbano e políticas de segurança no Rio de Janeiro*. Rio de Janeiro: FGV, 2017.

PAES, Eduardo. Armar a guarda: impacto da segurança armada em políticas públicas municipais. Disponível em: <https://www.rio.rj.gov.br/web/guest/seguranca-publica>. Acesso em: 15 set. 2023.

PEREIRA, J. A.; SILVA, D. R. Reconhecimento facial: desafios técnicos e sociais. *Revista de Tecnologia e Sociedade*, v. 7, n. 3, p. 101–120, 2020.

POWELL, J. A. Structural racism and technology: algorithms, bias, and social inequality. *Journal of Ethics and Technology*, v. 15, n. 2, p. 55–78, 2019.

POLANYI, Karl. *A grande transformação: as origens da nossa época*. São Paulo: Martins Fontes, 2000.

RIBEIRO, S. A. Inteligência artificial e a segurança pública: limites e possibilidades no Brasil. *Revista Brasileira de Segurança Pública*, v. 15, n. 1, p. 23–44, 2022.

SANTOS, Milton. *Por uma outra globalização: do pensamento único à consciência universal*. Rio de Janeiro: Record, 2000.

SILVA, L. A.; CARVALHO, M. T. Vigilância, dados e cidadania: impactos do reconhecimento facial em espaços urbanos. *Revista Brasileira de Políticas Urbanas*, v. 10, n. 2, p. 89–110, 2021.

SOUZA, R. M. de. *Segurança, tecnologia e controle social: uma análise crítica do reconhecimento facial*. Brasília: Ipea, 2019.

WACQUANT, Loïc. *Punishing the poor: the neoliberal government of social insecurity*. Durham: Duke University Press, 2009.

WEAVER, M. et al. Facial recognition technology in urban policing: challenges and ethical concerns. *Urban Policy Review*, v. 12, n. 2, p. 101–120, 2020.

WOOD, D.; FARTHING, L.; MINGES, M. *The right to the city: social justice and urban governance*. London: Routledge, 2010.