*Comunicação e Sociedade, vol. 42, 2022, pp. 205–220*
https://doi.org/10.17231/comsoc.42(2022).3984

# Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematizações

**Paulo Victor Melo**
Instituto de Comunicação da NOVA, Faculdade de Ciências Sociais e Humanas, Universidade Nova de Lisboa, Lisboa, Portugal
Concetualização, curadoria dos dados, análise formal, investigação, metodologia, redação do rascunho original, redação – revisão e edição

**Paulo Serra**
LabCom – Comunicação e Artes, Faculdade de Artes e Letras, Universidade da Beira Interior, Covilhã, Portugal
Concetualização, análise formal, investigação, metodologia, supervisão, redação do rascunho original, redação – revisão e edição

**Resumo**

A partir da identificação e análise de propostas apresentadas por gestores públicos municipais, o presente artigo tece apontamentos sobre a relação entre tecnologias digitais e segurança pública no Brasil. Como corpus de pesquisa, foram selecionados os programas de governo elaborados pelos atuais prefeitos de todas as capitais do país na última eleição municipal (2020) e protocolados no Tribunal Superior Eleitoral. Como principais resultados da análise, apontam-se aqui: a previsão de uso de tecnologias digitais na segurança pública por 15 dos atuais 26 prefeitos de capitais, a pulverização partidária e a diversidade geográfica desses gestores, o ocultamento de potenciais problemas na aplicação dessas tecnologias. Adotando as noções de capitalismo de vigilância (Zuboff, 2018/2020) e racismo algorítmico (Silva, 2019) compreende-se em termos conclusivos que, sobretudo em um país marcado pelo racismo estrutural, as tecnologias digitais aplicadas à segurança pública devem ser pautadas considerando as possíveis implicações éticas, sociais, políticas e culturais, de modo que, na busca pelo combate à criminalidade e por ampliação da segurança, não se perpetue violências contra grupos historicamente discriminados.

**Palavras-chave**
capitalismo de vigilância, tecnologias digitais, reconhecimento facial, segurança pública, discriminações algorítmicas

# Facial Recognition Technology and Public Security in Brazilian Capitals: Issues and Problematizations

**Abstract**

Based on the identification and analysis of proposals presented by municipal public administrators, this paper notes the relationship between digital technologies and general security in Brazil. The government programs prepared by the current mayors of all capitals of the country in the last municipal election (2020), and filed with the Superior Electoral Court, were selected as a research corpus. As the main results of the analysis, we lay out the following: the forecast of the use of digital technologies in public security by 15 of the current 26 mayors of capital cities,

the party pulverization and the geographic diversity of these managers, the concealment of potential problems in the application of these technologies. Adopting the notions of surveillance capitalism (Zuboff, 2018/2020) and algorithmic racism (Silva, 2019), we conclusively understand that digital technologies applied to public security must consider the possible ethical, social, political, and cultural implications, especially in a country marked by structural racism, so that, in fighting crime and expanding protection, violence against historically discriminated groups is not perpetuated.

**Keywords**
surveillance capitalism, digital technologies, facial recognition, public security, algorithmic discrimination

## 1. Introdução

A problemática da violência urbana e da criminalidade é uma das principais preocupações da população brasileira. Às vésperas da eleição presidencial de 2018, a segurança pública foi apontada pelos eleitores como o segundo problema mais grave do Brasil, atrás apenas da saúde (Gelape, 2018). Essa percepção tem como motivações os fatos do país registrar um índice anual superior a 40.000 assassinatos, possuir o maior número absoluto de homicídios do mundo e ter uma taxa cinco vezes superior à média global (Chade, 2019).

Não havendo dúvidas de que a superação deste quadro exige um conjunto de esforços e ações políticas, quais respostas, no que diz respeito ao uso de tecnologias digitais, as gestões públicas das cidades brasileiras têm oferecido na área da segurança pública? Essa é a pergunta motivadora deste artigo, que tem como objetivo principal analisar como propostas que preveem a aplicação de tecnologias, defendidas por prefeitos das capitais do país, se relacionam com discursos de combate à criminalidade.

No sentido de buscar apontamentos sobre a questão apresentada, em termos metodológicos, o trabalho foi iniciado com o levantamento dos programas de governo, registrados no site do Tribunal Superior Eleitoral (s.d.), de todos os atuais prefeitos das 26 capitais estaduais[1], eleitos em 2020 e empossados em 2021.

A partir disso, foram identificadas nesses programas de governo as propostas relacionadas ao uso de tecnologias digitais na segurança pública, tendo como base o emprego de 10 expressões-chave que se aproximam do objeto investigado: "reconhecimento facial"; "inteligência artificial"; "vigilância"; "videomonitoramento"; "monitoramento"; "drone"; "câmera"; "vídeo"; "dados"; "tecnologia".

Reunidos os programas que continham alguma proposta de interesse desse trabalho, foi elaborado um formulário para orientação e padronização da análise, incluindo as seguintes questões:

- Quais os tipos de tecnologias digitais propostos para utilização na segurança pública?
- O uso dessa(s) tecnologia(s) é parte de algum programa específico?
- As propostas são apresentadas como alternativa para combate à criminalidade?

[1] Além das 26 capitais de estados, o Brasil possui uma capital federal, Brasília, mas que não possui prefeito.

- São apresentados possíveis benefícios no uso das tecnologias de informação e comunicação na segurança pública?
- São mencionados possíveis problemas a partir do uso dessas tecnologias na segurança?

Essas perguntas foram definidas com o objetivo de identificar se há, nas propostas dos prefeitos das capitais brasileiras, uma tendência sobre o uso de tecnologias digitais na segurança pública no que diz respeito ao combate à criminalidade.

Visando o cumprimento do objetivo proposto e a partir destes procedimentos metodológicos, o artigo obedece à seguinte estrutura: num primeiro momento, (a) é feita uma breve revisão teórico-conceitual sobre capitalismo de vigilância e o papel das tecnologias digitais nesse processo; em seguida (b) são apresentadas, e problematizadas pela perspectiva das opressões algorítmicas, informações sobre casos de erros e falhas na identificação de pessoas por tecnologias digitais na área da segurança pública no Brasil; em sequência, (c) são expostos os resultados principais da análise e desenvolvidas algumas observações críticas; e, por fim, (d) são apontadas as considerações conclusivas.

## 2. Capitalismo de Vigilância e Tecnologias Digitais: Algumas Notas

Apesar de muitas vezes serem vistas como uma etapa seguinte à das sociedades disciplinares estudadas por Foucault (1970/1975), assentes na vigilância panótica, as "sociedades de controlo" tematizadas por Deleuze (1992) não implicam menos vigilância do que as anteriores — o que fazem é basear o dispositivo de vigilância nas tecnologias que permitem a produção, difusão e recolha de informação. A vigilância, longe de desaparecer, torna-se ainda mais profunda e radical: se nas sociedades disciplinares os indivíduos são vigiados de forma presencial, localizada, pontual e involuntária, nas sociedades de controlo eles passam a ser vigiados de forma virtual, deslocalizada, omnipresente e voluntária. A designação "sociedade em rede" (Castells, 1996/1999) exprime bem, *malgré soi*, esta ideia do indivíduo preso numa teia (web) de que só conseguiria escapar se, como Robinson Crusoé, ficasse perdido numa qualquer ilha desligada do mundo — mas correria sempre o risco de encontrar o seu Sexta-Feira, agora munido do seu celular.

Não admira, assim, que no seu texto clássico sobre o tema, Lyon (1994) fale de um novo panótico que emerge na sociedade de informação, o "olho eletrónico", assente na recolha sistemática de dados sobre os cidadãos pelo estado e pelas empresas, registando os mais pequenos gestos da sua vida quotidiana. É precisamente este processo que está na base daquilo a que Lyon (1994) chama a "sociedade de vigilância", sendo o termo "vigilância" usado aqui, precisamente, "como um termo abreviado para abarcar as muitas, e em expansão, gamas de contextos nos quais os dados pessoais são coletados por agências de emprego, comerciais e administrativas, bem como no policiamento e segurança" (p. ix). Este tema da vigilância é retomado e aprofundado por Lyon em outros textos posteriores, com destaque para o livro *The Culture of Surveillance: Watching as a Way of Life* (A Cultura da Vigilância: A Vigilância Como um Modo de Vida; Lyon, 2018). Nesta obra, o conceito de "sociedade de vigilância" é revisto num duplo sentido (a síntese é nossa): em primeiro lugar, no facto de que a vigilância não é apenas uma atividade exercida, sobre si, por

entidades externas ao sujeito — mas é o próprio sujeito que, livre e voluntariamente, fornece dados sobre si próprio e as suas diversas atividades (nomeadamente através das redes sociais); em segundo lugar, porque a hétero e a autovigilância se tornam uma prática normal e normalizada e, por assim dizer, natural. Ora, é esta "naturalidade" — artificial — das normas e práticas da vigilância que constitui uma cultura, a "cultura da vigilância".

Por seu lado, inspirando-se em Foucault, Rouvroy e Berns (2013) designam o tipo de vigilância que emerge nas "sociedades de controlo" como "governamentalidade algorítmica". A inspiração em Foucault situa-se no facto de os autores verem a governamentalidade algorítmica na continuidade de uma forma de "poder" que se exerce não sobre o corpo físico (a lei, a disciplina) ou a consciência moral (o pastoreio, a confissão), assentes na interdição ou na prescrição, mas através dos "dispositivos de segurança", assentes na regulação:

> a regulação de um meio no qual não se trata tanto de fixar os limites, as fronteiras, no qual não se trata tanto de determinar as localizações, mas sobretudo essencialmente de permitir, de garantir, de assegurar as circulações: circulação de pessoas, circulação de mercadorias, circulação de ar, etc. (Foucault, 2004, como citado em Rouvroy & Berns, 2013, p. 175)

Neste sentido, os autores definem a governamentalidade algorítmica como "um certo tipo de racionalidade (a)normativa ou (a)política que repousa sobre a recolha, agregação e análise automática de dados em quantidade massiva de maneira a modelizar, antecipar e afetar [ou seja, a regular] antecipadamente os comportamentos possíveis" (Rouvroy & Berns, 2013, p. 173). Os dados que os sujeitos fornecem voluntariamente acerca de si próprios e das suas vidas às plataformas e redes tecnológico-informacionais são utilizados, por estas e pelos diversos poderes económicos, políticos, militares e policiais que com elas se articulam, para a construção de "perfis" que permitem dirigir e orientar os comportamentos individuais em certos sentidos em vez de outros, assim determinando percursos, definindo atividades, delimitando escolhas. A "liberdade" e "autonomia" dos sujeitos não deixam de existir, mas elas são condicionadas a certos quadros de funcionamento cuja escolha não depende deles próprios, a quadros que são, por assim dizer, laterais à sua "liberdade" e "autonomia".

Também a partir da perspectiva de Foucault sobre a "genealogia da alma moderna", em que as subjetividades são inseparáveis dos dispositivos de visibilidade, Bruno (2004) enfatiza que as tecnologias comunicacionais contemporáneas se caracterizam pela incidência do foco de visibilidade sobre o indivíduo comum, um aspecto que é determinante na produção de subjetividades e identidades.

> O olhar não mais incide naqueles que exercem o poder, mas naqueles sobre quem o poder é exercido. Sobre o indivíduo comum, ordinário, e ainda mais sobre aqueles que estão aquém do comum e mediano — o desviante,

> o anormal. Trata-se, de fato, de um olhar individualizante, de um poder que individualiza pelo olhar, tornando visível, observável, analisável, calculável o indivíduo comum. Deste modo, o poder torna-se cada vez mais anônimo enquanto o indivíduo comum ou desviante, exposto à visibilidade, torna-se cada vez mais objetivado e atrelado a uma identidade — o criminoso, o doente, o louco, o aluno, o soldado, o trabalhador têm seus comportamentos, sintomas, manias, vícios, falhas, desempenhos, aptidões, méritos e deméritos investidos, conhecidos, registrados, classificados, recompensados, punidos por uma maquinaria de vigilâncias hierarquizadas. (Bruno, 2004, p. 111)

A ironia — trágica — deste novo sistema de vigilância é que o seu principal agente é o próprio sujeito, que, passe o paradoxo, livremente se sujeita a si próprio no contexto do que Zuboff (2018/2020) chama "capitalismo de vigilância" — um regime que, iniciado com a Microsoft, continua com a Google, o Facebook e outras redes sociais, encontrando-se hoje generalizado a todos os produtos, serviços e dispositivos que podem integrar-se na chamada "internet das coisas".

Em um texto introdutório sobre o tema, Zuboff (2019) aponta quatro características fundamentais na constituição do capitalismo de vigilância: a massiva extração e análise de dados; o desenvolvimento de novas formas contratuais usando monitoramento computacional e automação; o desejo de personalizar e customizar os serviços oferecidos para os usuários de plataformas digitais; e o uso de infraestrutura tecnológica para executar experimentos futuros em seus usuários e consumidores.

> A lógica de acumulação que garantiria o sucesso do Google aparece claramente em uma patente registrada em 2003 por três dos melhores cientistas da computação da empresa, intitulada "Gerar informações do usuário para publicidade direcionada". A invenção, explicam, buscaria "estabelecer as informações dos perfis do usuário e usá-las para a disseminação de anúncios". Em outras palavras, o Google não se contentaria mais em extrair dados comportamentais para melhorar seus serviços. Ele passaria a ler o pensamento dos usuários a fim de fazer os anúncios corresponderem aos seus interesses, que, por sua vez, seriam deduzidos dos traços colaterais do comportamento on-line. A coleta de novos conjuntos de dados, denominada *User Profile Information*, melhoraria consideravelmente a precisão dessas previsões. ( ... ) A invenção do Google revelou novas possibilidades de deduzir pensamentos, sentimentos, intenções e interesses de indivíduos e grupos, por meio de uma arquitetura de extração automatizada que funciona como um espelho unidirecional, sem se preocupar com a consciência e o consentimento dos envolvidos. Esse *imperativo de extração* resultou em economias de escala que proporcionariam uma vantagem competitiva única no mundo, em um mercado no qual os prognósticos dos comportamentos individuais representam um valor que se compra e se vende. Mas,

> sobretudo, o espelho unidirecional simboliza as relações sociais de vigilância particulares baseadas em uma espetacular assimetria de conhecimento e poder. (Zuboff, 2019, paras. 9, 11)

Apresentado em linguagem mais ou menos "económica", um tal regime tem como matéria-prima a nossa experiência com as tecnologias e os dados que cedemos no decurso dessa experiência. A partir desses dados, os processos de fabricação assentes na "inteligência da máquina" permitem a manufatura de "produtos de predição" que alimentam um "mercado de comportamentos futuros" (Zuboff, 2018/2020, p. 13). São estes comportamentos futuros que, verdadeiramente, tecnológicas como a Microsoft, a Google, a Meta (proprietária do Facebook, Instagram e WhatsApp) e muitas outras vendem às empresas que produzem os mais diversos bens e serviços, bem assim como aos diversos poderes político-militares e policiais.

Ora, os dados que as tecnologias digitais e as respetivas bases (de dados) recolhem e arquivam são, cada vez mais, da ordem da imagem, com destaque para as imagens dos nossos rostos; e aquelas tecnologias têm vindo a aperfeiçoar cada vez mais, ao longo do tempo, a sua capacidade de processamento dessas imagens. É a conjugação destes processos — recolha, arquivo e processamento de imagens — que possibilita, precisamente, o reconhecimento facial. Que empresas como a Amazon, a Google, a Microsoft ou a IBM têm vindo a desenvolver, nos últimos anos, programas de reconhecimento facial a partir das bases de dados de imagens comprovam-no notícias como as surgidas em meados de 2020, de acordo com as quais a três primeiras daquelas empresas estavam a ser processadas por cidadãos devido ao facto de estarem a ser utilizadas as suas forografias, existentes numa base de dados da IBM, sem a sua permissão (Musil, 2020).

## 3. Reconhecimento Facial e Discriminações

> Eu sofri, porque fui julgado pelos vizinhos. Perdi muitos serviços, porque disseram que eu era traficante. Falei que era inocente e a delegada falou para mim para eu pensar no que tinha feito. Pensei muito na família, que eu não ia voltar mais. (Bomfim, 2022, para. 12)

Essas foram as palavras ditas por José Domingos Leitão, 52 anos, em depoimento ao portal R7, após passar 3 dias preso, em outubro de 2020.

José Domingos Leitão, que vive no município de Ilha Grande, Piauí, foi erroneamente identificado por uma tecnologia de reconhecimento facial como autor de um crime. O fato de José residir a mais de 2.000 km do local onde ocorreu o crime e nunca ter ido à cidade onde o fato aconteceu nem sequer foram considerados, já que a sua imagem constava em um banco de dados nacional utilizado pela Polícia do Distrito Federal.

Grosso modo, o reconhecimento facial inicia com o scanner do rosto de um indivíduo. A partir disso, os traços e características do rosto são transformados em "pontos de referência", que são analisados, como um identificador associado àquela pessoa, para

que o banco de dados possa, então, normalizar com outras faces classificadas em padrões ou tipos, a partir de determinado nível de semelhança.

> O reconhecimento facial é uma forma de biometria, que é a ligação entre um elemento único do corpo humano de um indivíduo com uma unidade de registro. O elemento corporal utilizado pode ser a digital, a face, o modo de caminhar. As unidades de registro mais comuns são os cadastros, como o Registro Geral (RG), o número da Previdência Social ou a conta bancária. A parte do corpo utilizada na biometria, seja a digital ou a face, nunca é analisada por completo. Isto quer dizer que são escolhidos alguns pontos do rosto ou do dedo e, com base nas distâncias entre esses pontos, é calculada a probabilidade de aquela digital ou de aquela face ser da pessoa cadastrada no banco de dados. No caso do rosto humano, as possibilidades de haver diferenças ou modificações nessas distâncias são bem maiores do que numa digital, já que uma pessoa envelhece, pode estar bocejando, piscando. (Nunes, 2019, pp. 67–68)

Deste modo, além de um uso para monitoramento coletivo, o reconhecimento facial é capaz de identificar, seguir, destacar individualmente e rastrear pessoas nos locais em que elas transitam, podendo, assim, exercer vigilância específica e violar direitos como privacidade, proteção de dados e não-discriminação.

Nos Estados Unidos, um caso semelhante ao de José Domingos Leitão foi registrado em 2019, quando Robert Williams passou 30 h preso, em Detroit, também por um erro no sistema de reconhecimento facial da Polícia do Estado de Michigan. De acordo com a organização estadunidense American Civil Liberties Union, Williams foi "a primeira pessoa presa injustamente com base nessa tecnologia" (Robertson, 2021, para. 1).

Alguns anos antes, porém, a American Civil Liberties Union já alertava para possíveis problemas neste sentido. Utilizando uma ferramenta de reconhecimento facial desenvolvida pela empresa Amazon, Rekognition FR, a organização aplicou uma pesquisa junto a parlamentares dos Estados Unidos e concluiu que 28 membros do congresso foram identificados erroneamente com outras pessoas já presas por algum crime, sendo a maioria de pessoas negras (Snow, 2018).

Desde então, os erros da tecnologia de reconhecimento facial têm se acumulado nos Estados Unidos (O'Neill, 2020), no Brasil (*Sistema de Reconhecimento Facial da PM do RJ Falha, e Mulher É Detida por Engano*, 2019) e em outros países. No Reino Unido, por exemplo, um relatório produzido por investigadores da Universidade de Essex identificou uma taxa de 81% de erro nos casos de uso do reconhecimento facial pela Polícia Metropolitana de Londres (Fussey & Murray, 2019).

No Brasil, dados da Rede de Observatórios de Segurança (Ramos, 2019) apontam que, entre março e outubro de 2019, em quatro estados pesquisados (Bahia, Paraíba, Rio de Janeiro e Santa Catarina), 151 pessoas foram presas a partir da tecnologia de reconhecimento facial, sendo que 90,5%, nos casos em que havia informações sobre raça e cor, eram negras.

Diferentes autores (Broussard, 2018; Lohr, 2018; Nakamura, 2008) têm apontado que, para além de erros e falhas "naturais", esses casos evidenciam o caráter discriminatório dessas tecnologias. Broussard (2018) lembra que os algoritmos

> são projetados por pessoas, e as pessoas incorporam seus vieses inconscientes em algoritmos. Raramente é um algo intencional, mas isso não significa que devemos deixar de analisar. Significa que devemos ser críticos e vigilantes em relação às coisas que sabemos que podem dar errado. (p. 289)

Ao formular o conceito de racismo algorítmico, Silva (2019) ressalta que há, na concepção das tecnologias digitais, uma opacidade dupla quanto ao aspecto da racialização, caracterizada pela ideia de tecnologia e algoritmos como neutros e, ao mesmo tempo, pela ideologia de negação e invisibilidade da raça enquanto uma categoria social.

> Elaboro o conceito de "racismo algorítmico" para descrever como interfaces e sistemas automatizados, tais como plataformas de mídias sociais, podem reforçar e, pior, ocultar as dinâmicas racistas das sociedades onde são usados e empregados. É importante frisar que o problema não é um algoritmo ou outro tomado de forma isolada, mas "como sociedades racistas constroem consequentemente tecnologias com potenciais ou aplicações discriminatórias". (Silva, 2019, para. 6)

Numa espécie de "linha do tempo" do racismo algorítmico, Silva (2019) apresenta uma diversidade de casos, dados e reações de processos de racialização em interfaces, bancos de dados, algoritmos e inteligência artificial, como: sistemas do Google que permitem empresas exibirem anúncios sobre crime especificamente a afro-americanos; resultados no Google Imagens que apresentam conteúdos hiper-sexualizados para buscas como "garotas negras"; marcação de fotos de jovens negros com a tag "gorila" pelo Google Fotos; robôs conversacionais de startups que não encontram face de mulher negra e sistemas de visão computacional que erram gênero e idade de mulheres negras; mecanismos de busca de bancos de imagens que invisibilizam famílias e pessoas negras; aplicativos que transformam selfies e equiparam beleza à brancura; ferramentas de processamento de linguagem natural que possuem vieses contra linguagem e temas negros; análise facial de emoções que associa categorias negativas a atletas negros.

Na mesma direção apontada por Silva (2019), um estudo desenvolvido por Buolamwini e Gebru (2019), do Massachusetts Institute of Technology, revelou que as margens de erro do reconhecimento facial foram bastante diferentes de acordo com a cor da pele e o gênero: 0,8% no caso de homens brancos, 26% quando homens negros e 34% no caso de mulheres negras, sendo uma das motivações a baixa representação de rostos de tonalidades mais escuras nos conjuntos de dados, deixando, assim, o reconhecimento mais impreciso quanto a esse grupo étnico-racial.

> Estudos recentes demonstram que algoritmos de aprendizado de máquina podem discriminar com base em classes como raça e gênero. ( ... ) As disparidades substanciais na precisão da classificação de mulheres mais escuras, mulheres mais claras, homens mais escuros e homens mais claros em sistemas de classificação de gênero requerem atenção urgente se as empresas comerciais quiserem construir algoritmos de análise facial genuinamente justos, transparentes e responsáveis. (Buolamwini & Gebru, 2019, p. 1)

Os resultados de estudos como os mencionados acima têm gerado reações contra a adoção do reconhecimento facial em diferentes partes do mundo. Alguns exemplos são Big Brother Watch (https://bigbrotherwatch.org.uk/) e Liberty Human Rights (Liberty, s.d.), ambas na Inglaterra; a campanha "Ban Facial Recognition" (Banir o Reconhecimento Facial; https://www.banfacialrecognition.com/), nos Estados Unidos; e a Internet Freedom Foundation (s.d.), na Índia.

No Brasil, em maio de 2022, centenas de organizações de direitos digitais, ativistas e investigadores lançaram a campanha "Tire o Meu Rosto da Sua Mira", que reivindica o banimento total das tecnologias digitais de reconhecimento facial na segurança pública, dado o potencial de abusos e violações de direitos.

> As tecnologias de vigilância nos trazem insegurança em razão da violação a nossos direitos, sem que nos sejam dadas chances de evitar ou mesmo consentir com sua implementação e com o fato de nos tornarmos seus alvos. Destacam-se as violações de nossa integridade, pela coleta e pelo processamento de dados pessoais biométricos; de nossa liberdade de ir e vir e de autodeterminação, pois podemos estar sob vigilância 24 horas por dia, 7 dias por semana, criando um contexto amedrontador; do nosso direito ao devido processo legal, pois a vigilância em massa considera todas as pessoas culpadas por princípio, minando a garantia constitucional da presunção de inocência como um pressuposto jurídico básico. (Tire o Meu Rosto da Sua Mira, 2022, para. 6)

Outras iniciativas, também no sentido do banimento do reconhecimento facial, que merecem destaque são o Projeto de Lei 824/2021 (2021), protocolado pelo Vereador Reimont (Partido dos Trabalhadores ), que propõe a proibição de uso dessa tecnologia pela prefeitura do Rio de Janeiro, e a Ação Civil Pública, assinada por órgãos públicos e entidades da sociedade civil, que pretende vedar o uso do reconhecimento facial no metrô de São Paulo (Intervozes, 2022).

## 4. Resultados Principais

Como resultado da primeira etapa metodológica do trabalho, foi identificado, a partir das expressões-chave previamente definidas, que 15 dos atuais 26 prefeitos de capitais do Brasil apresentaram, em seus programas de governo da última eleição, propostas que envolvem o uso de tecnologias digitais na área da segurança pública.

A distribuição geográfica e a pulverização partidária desses 15 prefeitos — que contemplam cidades das cinco regiões (Norte, Nordeste, Centro-Oeste, Sudeste e Sul) e integram 11 partidos políticos[2] diferentes — sinaliza que a perspectiva de utilização das tecnologias como estratégia para as ações de segurança não é uma questão restrita a uma ou outra parte do país ou a determinados agrupamentos ideológicos.

Dentre os tipos de tecnologia propostos pelos 15 prefeitos[3], como pode ser verificado na Figura 1, 13 prefeitos citaram a instalação ou ampliação de videomonitoramento ou câmeras de monitoramento, seja em transportes públicos, em vias urbanas ou outros espaços de circulação, como parques e praças; oito prefeitos propuseram a aplicação de reconhecimento facial; quatro apresentaram ações utilizando drones; e cinco fizeram referência a outras tecnologias.

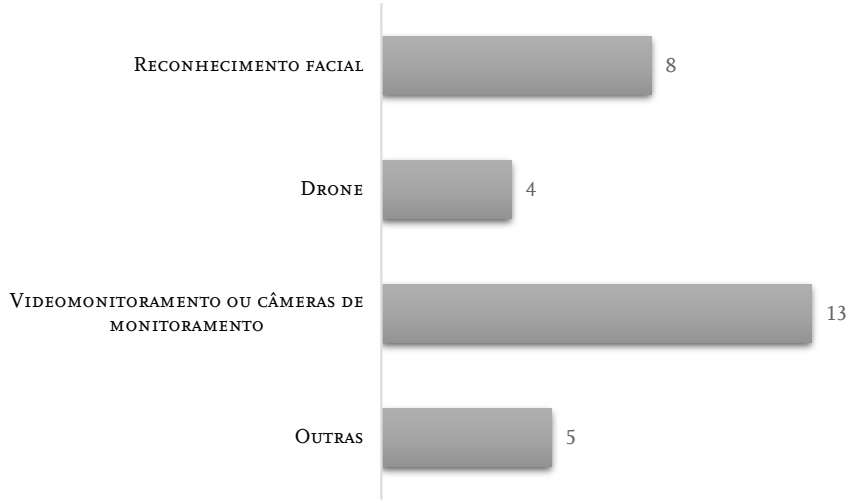


**Figura 1** *Tipos de tecnologia*

A investigação demonstrou também que sete dentre os 15 prefeitos incluíram as propostas de uso das tecnologias em iniciativas mais amplas de segurança pública. A presença de expressões como "muralha", "cercamento", "segurança" e "seguro", dentre outras, conforme visto na Tabela 1, denota uma perspectiva de segregação, controle e vigilância da aplicação dessas tecnologias pelos gestores públicos.

[2] Os seguintes partidos políticos estão representados pelos 15 prefeitos com propostas de interesse deste trabalho: Avante (um), Democratas (dois), Movimento Democrático Brasileiro (dois), Partido Democrático Trabalhista (um), Partido Socialista Brasileiro (um), Partido Social Democrático (dois), Partido da Social Democracia Brasileira (três), Podemos (um), Progressistas (dois), Republicanos (um), União Brasil (um).

[3] Vale registrar que alguns prefeitos mencionaram o emprego de mais de uma tecnologia.

| Nome do programa | Cidade |
|---|---|
| *Muralha Digital* | Curitiba |
| *Cercamento Eletrônico da Cidade* | Aracaju |
| *City Câmeras* | São Paulo |
| *De Olho na Rua* | Goiânia |
| *Teresina Segura* | Teresina |
| *Vitória Segura* | Vitória |
| *Andar Seguro* | João Pessoa |

**Tabela 1** *Nomes de programas que relacionam tecnologias e segurança pública nas capitais brasileiras*

Outro aspecto evidenciado na leitura dos programas de governo foi a previsão de estratégias que propõem o envolvimento direito da população na vigilância da cidade.

No programa de gestão do Prefeito Maguito Vilela (Movimento Democrático Brasileiro), de Goiânia, por exemplo, é apontado que "condomínios com sistemas de câmeras de vídeo serão obrigados a ter parte do equipamento monitorando as ruas".

Medida semelhante ao proposto por Rafael Greca (Democratas), em Curitiba, que defendeu "o incentivo à população (residências, prédios e condomínios) e empresas (comércio/serviços)" na colaboração com o programa *Muralha Digital*.

Em Belo Horizonte, no plano de governo do Prefeito Kalil (Partido Social Democrático) foi sinalizado que o Centro de Operações da Prefeitura

> passará a contar também com as câmeras e sensores instalados pelo próprio cidadão, cujas imagens poderão ser disponibilizadas por meio de uma plataforma colaborativa de monitoramento, ampliando a cobertura da cidade e aprimorando as respostas às diversas situações de segurança e desordem pública.

Vale problematizar que propostas como as apresentadas acima contribuem para uma espécie de "big brother público", em que todos são, ao mesmo tempo, potenciais vigilantes e vigiados, comprometendo a própria noção de espaço público enquanto ambiente para a livre circulação dos cidadãos e cidadãs.

Também como resultado da análise, identificou-se que em 80% dos programas de governo a aplicação de tecnologias na segurança pública é expressamente definida como uma estratégia de combate à criminalidade. Neste sentido, como objetivo do uso das tecnologias, é citada a redução das ações de vandalismo, depredações, furtos, roubos, invasões, pichações, assaltos, violência sexual, dentre outras.

Além disso, em 11 dos 15 programas de governo são apresentadas afirmações genéricas, sem detalhamento, sobre benefícios à população da utilização de tecnologias digitais na segurança pública, como "mais segurança" (programas de governo Teresina, São Paulo, Manaus, Palmas e Curtiba), "ampliação da cobertura da cidade" (programas de governo Aracaju, São Paulo, Campo Grande, Natal e Rio Branco), "aprimoramento das respostas às diversas situações de segurança" (Vitória, Curitiba e Florianopolis).

Por outro lado, ainda que já fossem conhecidas notícias sobre violações de direitos geradas por tecnologias como o reconhecimento facial, a exemplo das mencionadas neste trabalho, nenhum dos programas de governo citou qualquer possível problema na utilização dessas tecnologias na segurança pública nem mesmo alternativas frente a potenciais problemas O que fazer caso o reconhecimento facial resulte em prisão de pessoa inocente na cidade por si governada? Ao menos nas propostas dos atuais prefeitos de capitais do Brasil, este não apareceu como um tópico de preocupação.

A título de observação, importa registrar ainda que outras capitais em que os atuais prefeitos não apresentaram uma proposta específica nos programas de governo das últimas eleições têm sido palco de ações que envolvem o uso de tecnologias digitais na segurança pública. Exemplos disso são Salvador, Recife e Rio de Janeiro, que em edições recentes do carnaval (Intervozes, 2019) têm realizado vigilância e monitoramento via reconhecimento facial, a partir de iniciativas dos governos estaduais em parceria com empresas multinacionais de tecnologia, como a Huawei (Falcão, 2021), Avantia (Ams, 2019) e Oi (Kawaguti, 2019).

No Rio de Janeiro, ainda na fase de testes de câmeras que haviam sido instaladas inicialmente para o carnaval de 2019, uma mulher — que estava sentada em um banco no bairro de Copacabana — foi detida por engano pela Polícia Militar após ser identificada, via tecnologia de reconhecimento facial, como suspeita dos crimes de homicídio e ocultação de cadáver. Porém, horas depois, na delegacia, descobriu-se que a verdadeira autora do crime em questão já estava presa por este motivo desde 2015.

Em Recife, apesar de não constar em seu programa de governo, o Prefeito João Campos (Partido Socialista Brasileiro) anunciou no final de 2021, portanto ainda no 1.º ano de gestão, a intenção de instalar 108 relógios digitais que, além da exibição de hora e informações sobre o tráfego, teriam câmeras de monitoramento com reconhecimento facial (Diário de Pernambuco, 2021). Ainda que a adoção dos relógios digitais tenha sido adiada, a execução da proposta envolve a possibilidade de uma parceria público-privada, com a concessão de exploração por empresas privadas durante 20 anos (Santos, 2021).

Embora a proposta também não tenha sido apresentada em seu programa governamental registrado no período das eleições, o prefeito de Salvador, Bruno Reis (Democratas), anunciou, nos últimos meses de 2021, a instalação de câmeras com reconhecimento facial em pontos turísticos da cidade, sendo o combate à criminalidade uma das motivações expressas pelo gestor (Redação, 2021).

Vale frisar ainda que a adoção dessas tecnologias tem sido estimulada pelo governo federal, a exemplo da Portaria nº 793 (2019) que, ao regulamentar o Fundo Nacional de Segurança Pública, prevê a disponibilização de recursos para o "fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por *Optical Character Recognition* – OCR, uso de inteligência artificial ou outros", como uma das ações financiáveis para o "enfrentamento à criminalidade violenta" (Portaria nº 793, 2019, Artigo 4).

Além dos aspectos evidenciados na análise dos programas de governo, e compreendendo a cada vez maior relevância das tecnologias digitais na segurança pública, cabem questionamentos como: quando os gestores mencionam "pessoas suspeitas", quais dados são coletados para construção desses perfis? Como são construídos e compostos os bancos de dados que sustentam essas tecnologias? Quem, além da ação automatizada dos algoritmos, está por trás das câmeras de reconhecimento facial? Há mecanismos de proteção dos dados pessoais? Quais são os bancos de dados que estão sendo cruzados? Quem armazena, qualifica e indexa esses bancos de dados? A quem é garantido o acesso e a quem é negado? O que está sendo registrado? O que são entendidas como "boas práticas" de utilização dessas tecnologias quando ainda não há legislação vigente normatizando os seus usos?

## 5. Conclusões

Os resultados da análise dos programas de governo dos atuais prefeitos das capitais brasileiras apontam que utilização de tecnologias digitais como estratégia de combate à criminalidade demonstra-se como uma tendência nas políticas de segurança pública no país. Tendo em conta esta questão e considerando os crescentes casos de prisões injustas e outros erros na identificação de pessoas a partir do reconhecimento facial, faz-se necessário que a aplicação dessas tecnologias seja acompanhada por um processo de discussão e acompanhamento públicos, envolvendo os diferentes segmentos da sociedade.

Neste sentido, deve ser objeto de alerta o fato de nenhum dos programas de governo analisados indicar qualquer preocupação com possíveis riscos de violação aos direitos dos cidadãos e cidadãs a partir de erros no uso das tecnologias digitais.

Num país que já possui histórico de prisões equivocadas por reconhecimento fotográfico não digital (*Exclusivo: 83% dos Presos Injustamente por Reconhecimento Fotográfico no Brasil São Negros*, 2021), majoritariamente de pessoas negras, que tem a terceira maior população carcerária de todo o mundo (Pastoral Carcerária, 2018) e caracterizado pelo genocídio da população negra como lógica estruturante do estado (Nascimento, 1978), torna-se fundamental também que a implementação das tecnologias digitais, sobretudo o reconhecimento facial, seja pautada a partir de todas as possíveis implicações éticas, sociais, políticas e culturais, de modo que, na busca pelo combate à criminalidade e por ampliação da segurança, não se perpetue violências contra grupos historicamente discriminados.

## Referências

Ams. (2019, 27 de março). Reconhecimento facial: Uma alternativa de combate ao crime. *Avantia*. https://www.avantia.com.br/blog/reconhecimento-facial-uma-alternativa-de-combate-ao-crime/

Bomfim, F. (2022, 21 de janeiro). *Reconhecimento facial erra de novo e acusa inocente*. R7 Brasília. https://noticias.r7.com/brasilia/reconhecimento-facial-erra-de-novo-e-acusa-inocente-21012022

Broussard, M. (2018). *Artificial unintelligence: How computers misunderstand the world*. MIT Press.

Bruno, F. (2004). Máquinas de ver, modos de ser: Visibilidade e subjetividade nas novas tecnologias de informação e comunicação. *Revista Famecos*, *11*(24), 110–124. https://doi.org/10.15448/1980-3729.2004.24.3271

Buolamwini, J., & Gebru, T. (2019). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, *81*, 1–15. https://proceedings.mlr.press/v81/buolamwini18a.html

Castells, M. (1999). *A sociedade em rede* (R. Majer, Trad.). Paz e Terra. (Trabalho original publicado em 1996)

Chade, J. (2019, 4 de abril). *Brasil tem maior número absoluto de homicídio do mundo, diz OMS*. Uol. https://jamilchade.blogosfera.uol.com.br/2019/04/04/brasil-tem-maior-numero-absoluto-de-homicidio-do-mundo-diz-oms/

Deleuze, G. (1992). *Conversações 1972-1990*. Editora 34.

Diário de Pernambuco. (2021, 26 de outubro). Prefeitura do Recife pede opinião pública sobre a instalação de 108 novos relógios eletrônicos. *Diário de Pernambuco*. https://www.diariodepernambuco.com.br/noticia/vidaurbana/2021/10/prefeitura-do-recife-pede-opiniao-publica-sobre-a-instalacao-de-108-no.html

*Exclusivo: 83% dos presos injustamente por reconhecimento fotográfico no Brasil são negros* (2021, 21 de fevereiro). G1. https://g1.globo.com/fantastico/noticia/2021/02/21/exclusivo-83percent-dos-presos-injustamente-por-reconhecimento-fotografico-no-brasil-sao-negros.ghtml

Falcão, C. (2021, 20 de setembro). *Lentes racistas*. The Intercept_Brasil. https://theintercept.com/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/

Foucault, M. (1975). *Vigiar e punir – Nascimento da prisão* (R. Ramalhete, Trad.). Editora Vozes. (Trabalho original publicado em 1970)

Fussey, P., & Murray, D. (2019). *Independent report on the London Metropolitan Police Service's trial of live facial recognition technology*. Human Rights Centre – University of Essex. https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf

Gelape, L. (2018, 11 de setembro). *Saúde e violência são os principais problemas para os eleitores brasileiros, segundo Datafolha*. G1. https://g1.globo.com/politica/eleicoes/2018/eleicao-em-numeros/noticia/2018/09/11/saude-e-violencia-sao-os-principais-problemas-para-os-eleitores-brasileiros-segundo-datafolha.ghtml

Internet Freedom Foundation. (s.d.). *The Delhi Police must stop it's facial recognition system.* https://internetfreedom.in/we-demand-the-delhi-police-stop-its-facial-recognition-system/

Intervozes. (2019, 14 de março). Reconhecimento facial no carnaval: riscos tecnológicos nada divertidos. *CartaCapital*. https://www.cartacapital.com.br/blogs/intervozes/reconhecimento-facial-no-carnaval-riscos-tecnologicos-nada-divertidos/

Intervozes. (2022, 4 de março). *Ação quer vedar o uso de tecnologias de reconhecimento facial pelo Metrô de São Paulo*. Intervozes: coletivo brasil de comunicação social. https://intervozes.org.br/acao-quer-vedar-o-uso-de-tecnologias-de-reconhecimento-facial-pelo-metro-de-sao-paulo/

Kawaguti, L. (2019, 24 janeiro). *Câmera inteligente no RJ terá sistema da Oi, multada por violar privacidade.* Uol. https://noticias.uol.com.br/cotidiano/ultimas-noticias/2019/01/24/cameras-monitoramento-carnaval-rio.htm

Liberty. (s.d.). *Resist facial recognition*. https://www.libertyhumanrights.org.uk/campaign/resist-facial-recognition/

Lohr, S. (2018, 9 de fevereiro). Facial recognition is accurate, if you're a white guy. *The New York Times*. https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. University of Minnesota Press.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

Musil, S. (2020, 14 de julho). *Amazon, Google, Microsoft sued over photos in facial recognition database*. CNET. https://www.cnet.com/science/amazon-google-and-microsoft-sued-over-photos-in-facial-recognition-database/

Nakamura, L. (2008). *Digitizing race: Visual cultures of the internet*. University of Minnesota Press.

Nascimento, A. (1978). *O genocídio do negro brasileiro: O processo de um racismo mascarado*. Paz e Terra.

Nunes, P. (2019). *Novas ferramentas, velhas práticas: Reconhecimento facial e policiamento no Brasil*. O Panóptico. https://opanoptico.com.br/novas-ferramentas-velhas-praticas-reconhecimento-facial-e-policiamento-no-brasil/

O'Neill, N. (2020, 4 de setembro). Faulty facial recognition led to his arrest—Now he's suing. *Vice*. https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing

Pastoral Carcerária. (2018). *Luta antiprisional no mundo contemporâneo: Um estudo sobre experiências de redução da população carcerária em outras nações*. https://carceraria.org.br/wp-content/uploads/2018/09/relatorio_luta_antiprisional.pdf

Portaria nº 793, de 24 de outubro de 2019, Diário Oficial da União, Edição 208, Seção 1 (2019). https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575

Projeto de Lei 824/2021, Câmara Municipal do Rio de Janeiro (2021). http://aplicnt.camara.rj.gov.br/APL/Legislativos/scpro2124.nsf/

Ramos, S. (Ed.). (2019). *Retratos da violência: cinco meses de monitoramento, análises e descobertas*. Rede de Observatórios de Segurança. https://cesecseguranca.com.br/textodownload/retratos-da-violencia-cinco-meses-de-monitoramento-analises-e-descobertas/

Redação. (2021, 13 de outubro). Salvador terá câmeras de reconhecimento facial em pontos turísticos. *A Tarde*. https://atarde.com.br/bahia/bahiasalvador/salvador-tera-cameras-de-reconhecimento-facial-em-pontos-turisticos-1174976

Robertson, A. (2021, 13 de abril). *Detroit man sues police for wrongfully arresting him based on facial recognition.* The Verge. https://www.theverge.com/2021/4/13/22382398/robert-williams-detroit-police-department-aclu-lawsuit-facial-recognition-wrongful-arrest

Rouvroy, A., & Berns, T. (2013). Gouvernementalité algorithmique et perspectives d'émancipation: Le disparate comme condition d'individuation par la relation? *Réseaux*, *1*(177), 163–196. https://doi.org/10.3917/res.177.0163

Santos, M. C. (2021, 26 de novembro). Prefeitura do Recife adia discussão sobre implantação de vigilância com reconhecimento facial. *MarcoZero*. https://marcozero.org/prefeitura-do-recife-adia-discussao-sobre-implantacao-de-vigilancia-com-reconhecimento-facial/

Silva, T. (2019). *Racismo algorítmico em plataformas digitais: Microagressões e discriminação em código*. https://tarciziosilva.com.br/blog/racismo-algoritmico-em-plataformas-digitais-microagressoes-e-discriminacao-em-codigo/

*Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano.* (2019, 11 de julho). G1 Rio. 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

Snow, J. (2018, 26 de julho). *Amazon's face recognition falsely matched 28 members of Congress with mugshots*. American Civil Liberties Union. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Tire o meu rosto da sua mira. (2022, 8 de março). *Carta Aberta pelo banimento total do uso das tecnologias digitais de reconhecimento facial na segurança pública.* https://tiremeurostodasuamira.org.br/carta-aberta/

Tribunal Superior Eleitoral. (s.d.). *Eleições Municipais 2020: Divulgação de candidaturas e contas eleitorais.* Retirado a 30 de março de 2022 de https://divulgacandcontas.tse.jus.br/divulga/#/

Zuboff, S. (2019, 3 de janeiro). Um capitalismo de vigilância. *Le Monde Diplomatique Brasil*. https://diplomatique.org.br/um-capitalismo-de-vigilancia/

Zuboff, S. (2020). *A era do capitalismo de vigilância: A luta por um futuro humano na nova fronteira do poder* (G. Schlesinger, Trad.). Intrínseca. (Trabalho original publicado em 2018)

## Notas Biográficas

Paulo Victor Melo é investigador de pós-doutoramento no Instituto de Comunicação da Universidade Nova de Lisboa, Faculdade de Ciências Sociais e Humanas da NOVA, com bolsa apoiada pelo projeto UIDP/05021/2020, financiado em nível nacional pela FCT/MCTES. É doutor em comunicação e cultura contemporâneas pela Universidade Federal da Bahia, tendo realizado pós-doutoramento na Universidade da Beira Interior, junto ao LabCom – Comunicação e Artes. É coordenador do Centro de Comunicação, Democracia e Cidadania da Universidade Federal da Bahia.

ORCID: https://orcid.org/0000-0002-3985-4607

Email: paulomelo@fcsh.unl.pt

Morada: Instituto de Comunicação da Universidade Nova de Lisboa, Avenida de Berna, 26, 1069-061, Lisboa, Portugal

Paulo Serra é licenciado em filosofia pela Faculdade de Letras de Lisboa e mestre, doutor e agregado em ciências da comunicação pela Universidade da Beira Interior, Portugal. Nesta universidade, é professor catedrático no Departamento de Comunicação, Filosofia e Política e investigador na unidade LabCom – Comunicação e Artes. Foi presidente da Associação Portuguesa de Ciências da Comunicação.

ORCID: https://orcid.org/0000-0001-7821-3880

Email: pserra@ubi.pt

Morada: Universidade da Beira Interior, Rua Marques D'Ábila e Bolama, 6201-001, Covilhã, Portugal

**Submetido: 25/03/2022 | Aceite: 03/06/2022**