Revista Lusófona de Estudos Culturais / Lusophone Journal of Cultural Studies, Vol. 12, No. 1, 2025, e025003
https://doi.org/10.21814/rlec.6259

Technological Surveillance and Potential Discrimination: An Analysis of Proposals for the Use of Technology in Public Security in Brazil's 15 Most Populous Cities

Paulo Victor Melo
Instituto de Comunicação da NOVA, Faculdade de Ciências Sociais e Humanas, Universidade Nova de Lisboa, Lisboa, Portugal

Abstract

This exploratory, qualitative article examines the growing institutional trivialisation of technological surveillance in public security in Brazil, based on an analysis of government programmes from the current mayors of the 15 most populous cities. The *corpus* includes documents filed with the Superior Electoral Court during the 2024 elections by mayors who were candidates at the time. Compared to a study published in 2022, there has been an expansion in the devices and technologies adopted, alongside a continued focus on combating crime and ensuring security as the primary motivations. The analysis reveals that the large-scale adoption of digital technologies by security agencies, particularly facial recognition, occurs in a regulatory vacuum, marked by a lack of statistical data and opacity surrounding their use, operations, and funding. The study also highlights the ethical challenges concerning the protection of privacy rights, especially for vulnerable groups, which are notably absent in the discourse of local administrators. This situation is exacerbated by reports indicating that Black individuals are disproportionately affected by misidentification and related injustices from facial recognition technologies in the country.

Keywords

surveillance studies, facial recognition, modernity, public security, Brazil

Tecnovigilância e Potenciais Discriminatórios: Análise Sobre Propostas de Uso de Tecnologias na Segurança Pública nas 15 Cidades Mais Populosas do Brasil

Resumo

Com base em uma análise dos programas governamentais dos atuais prefeitos das 15 cidades mais populosas do Brasil, este artigo, de natureza exploratória e qualitativa, discute a crescente banalização institucional da tecnovigilância na segurança pública no país. O *corpus* abrange os documentos registrados pelos prefeitos, à época candidatos, no Tribunal Superior Eleitoral nas eleições de 2024. Em comparação com um estudo publicado em 2022, verificou-se a ampliação dos dispositivos e tecnologias adotados, bem como a manutenção dos discursos de enfrentamento à criminalidade e garantia da segurança como motivações principais. A análise permitiu relacionar também que a adoção em larga escala das tecnologias digitais por órgãos de segurança, especialmente o reconhecimento facial, ocorre num contexto de ausência regulatória sobre a matéria, e tem como características a ausência de dados estatísticos e a opacidade sobre os seus usos, operações e financiamento. O trabalho identificou ainda que desafios éticos, no tocante à proteção do direito à privacidade da população de um modo geral, e de grupos vulnerabilizados em específico, não são referidos pelos gestores. Este cenário é mais desafiador dado o fato das pessoas negras serem constantemente, conforme casos noticiados, as principais vítimas das injustiças promovidas com base em identificações erradas de tecnologias de reconhecimento facial no país.

Palavras-chave
estudos de vigilância, reconhecimento facial, modernidade, segurança pública, Brasil

1. Introduction

What proposals are public managers in Brazilian cities putting forward for the use of digital technologies in the field of public security? Moreover, what do these proposals reveal about their underlying conception of technology? These guiding questions are grounded in two key observations. The first concerns the centrality of public security within the Brazilian political agenda. In this regard, on the eve of the 2024 municipal elections, residents of the four most populous cities in the country identified public security as their primary concern (Rupp, 2024). The second observation draws on previous research (Melo, 2024; Melo & Serra, 2022), which has highlighted a process of institutional trivialisation of technological surveillance in Brazil. This process is marked by the recurrent and uncritical adoption of technologies — such as facial recognition systems — by police forces and other security agencies, primarily as rhetorical tools in the fight against crime.

In order to address the research questions, this study adopts a qualitative approach to analyse the proposals presented by the current mayors of the 15 most populous cities in Brazil[1] regarding the use of digital technologies in public security. The *corpus* for analysis comprises the government programmes submitted by these mayors — then candidates — to the Superior Electoral Court as part of the country's most recent electoral process, held on October 6 (first round) and October 27, 2024 (second round). Following an initial exploratory reading of the documents, all proposals directly related to public security were catalogued. These included references to 10 key expressions associated with surveillance studies, namely: "artificial intelligence", "biometrics", "algorithms", "data", "technologies", "facial recognition", "surveillance", "video monitoring", "cameras", and "drones".

It is worth noting that, together, the 15 cities selected for this study — listed in Table 1 — account for 20.5% of the Brazilian population (Belandi, 2024) and represent all five of the country's geographical regions (North, Northeast, Central-West, Southeast, and South). For these reasons, the sample is considered significant, given the potential impact of public security policies implemented in these territories.

[1] Although Maceió is officially the 16th most populous city in Brazil, its inclusion in the analysis is justified by the fact that Brasília — the third most populous city — does not have a mayor, owing to its status as the capital of the Federal District.

It is also important to note that the current mayors began their terms on January 1, 2025, therefore, the proposals analysed here are current and may contribute to ongoing debates regarding the uses and implications of technological surveillance in Brazil.

City	Region	Estimated Population
São Paulo	Southeast	11,895,578
Rio de Janeiro	Southeast	6,729,894
Fortaleza	Northeast	2,574,412
Salvador	Northeast	2,568,928
Belo Horizonte:	Southeast	2,416,339
Manaus	North	2,279,686
Curitiba	South	1,829,225
Recife	Northeast	1,587,707
Goiânia	Central-West	1,494,599
Belém	North	1,398,531
Porto Alegre	South	1,389,322
Guarulhos	Southeast	1,345,364
Campinas	Southeast	1,185,977
São Luís	Northeast	1,088,057
Maceió	Northeast	957,916

Table 1. *Most populous cities in Brazil*
Note. Data taken from the 2022 Census of the Brazilian Institute of Geography and Statistics (https://censo2022.ibge.gov.br/panorama/).

In addition to this introduction, the article is structured as follows: the first section provides a theoretical and conceptual framework on surveillance as part of the concept of modernity and as a structuring element of contemporary social dynamics; the second section presents data and reflections on the expansion of surveillance technologies in Brazil, particularly facial recognition; the following section analyses the results of research on proposals for the use of technological surveillance in the government programmes of the mayors of the 15 most populous cities in the country; finally, the last section presents the conclusions.

2. Surveillance and Modernity

The simple act of walking down streets and avenues in different cities around the world, entering and leaving airports, or even accessing metro and train stations is now characterised by the presence of technological surveillance devices that have the potential to capture and record our images, as well as register our movements, interactions, and conversations. As a complement to the cameras, information signs posted alongside the devices typically indicate that their purpose is "protection" or "security".

This expansion of surveillance technologies is not an isolated phenomenon but rather a component of so-called "smart" or "hyper-connected" cities, and thus a fundamental part of the very concept of modernity (Bauman, 2012/2013) and of everyday contemporary relations (Lyon, 2018; Marcolini, 2015). Whether through the actions of public authorities in defining responses to citizens, the commercial activities of companies seeking to profile and map the behaviour of their users, or even through individual actions, surveillance has become a ubiquitous and routine practice (Brayne, 2022).

Cameras are the visible, material aspect, but surveillance also operates through more sophisticated and complex techniques, in which a significant part of the personal information that feeds databases is made available on the applications and websites we access through computers and mobile phones. As Lyon rightly says, surveillance today is part of us, and

> we do not even notice the cameras around us. We think they can protect us, which is false. No one will say, "I want to be watched". However, our activities create the information that companies and agencies want. Many people still think that surveillance is tapping the phone. It is not the content that matters but the metadata. Who are your friends, who do you call, how long do you spend on the phone, and where do you travel. (Marcolini, 2015, para. 5)

In public spaces, this expansion is evident in the growing presence of various technological surveillance devices in places and services accessible to the public. Examples include video surveillance of streets and avenues (Zolezzi & Herrera, 2017), the use of cameras on buses, trains, and underground stations (Seshukumar et al., 2012), biometric identification systems at airports and other public spaces (Khan & Efthymiou, 2021), as well as facial recognition cameras for accessing personal technologies like mobile phones or services in education and healthcare (Francisco et al., 2020). Also noteworthy is the deployment of artificial intelligence at major sporting events (La Quadrature du Net, 2024) and the use of devices to monitor entries and exits in taxis and vehicles driven by app-registered drivers (Evangelo & Oliveira, 2021), among other examples.

This scenario fosters and reinforces the convergence of multiple surveillance logics, discourses, and practices. On the one hand, there is a logic that encourages video surveillance as a solution to security problems (La Vigne et al., 2011). On the other, it appears to justify the need for greater control over public spaces based on the notion that those who have nothing to hide should surrender their privacy so the State can act to prevent violence by "enemies" (Graham, 2016).

In this context, two issues are particularly important to consider: the growing difficulty in drawing boundaries between public and private (Viseu et al., 2006), where police departments rely on technological solutions provided by the private sector to carry out citizen surveillance operations (Brayne, 2022; Bridges, 2020); and the discursive appeal to feelings of insecurity, sustained by the perpetuation of the "other" as a suspect category (Bauman, 2012/2013). Who is this "other" who must be watched? If I am not the "other", are protection and security — discursively invoked to justify the expansion of surveillance — truly intended for me?

> It is for that double reason — to be protected from the dangers and from being cast into the class of a danger — that we develop vested interests in a dense network of surveilling, selecting, separating and excluding measures. We all need to mark the enemies of security in order to avoid being counted among them. We need to accuse in order to be absolved; to exclude in order to avoid exclusion. (Bauman, 2012/2013, p. 72)

This context becomes even more challenging, given the increasing use of artificial intelligence to automate surveillance. In a study on the deployment of real-time facial recognition technologies in public spaces, Fontes et al. (2022) warn that such systems expose populations to heightened risks of power asymmetries by accessing privileged information about individuals' private lives. These systems can exceed privacy boundaries and grant excessive control to public authorities, potentially eroding democratic values and undermining individual rights and freedoms. The authors also highlight that, while surveillance ostensibly covers the entire population, certain groups are disproportionately affected due to the ways they navigate and interact in public spaces.

Surveillance in public spaces thus tends to focus not on those who hold positions of privilege but on groups categorised as suspicious — those perceived to threaten the maintenance of order (Bruno, 2004). In Brazil, where the use of surveillance technologies by public security agencies is expanding, Black people have been the main victims of wrongful arrests resulting from mistaken identifications by facial recognition systems (Magno & Bezerra, 2020; Santos et al., 2023; Silva & Silva, 2024), as the next section discusses.

3. One Mistake at a Time, Facial Recognition Expands

In April 2024, in Aracaju, Sergipe, Brazil, 23-year-old João Antônio Trindade was apprehended by police during the half-time break of the final match of the Sergipe State Football Championship. Surrounded by fellow supporters of his team, he was handcuffed and taken to a Military Police station. The reason: facial recognition cameras installed at the stadium entrance had incorrectly identified him as a murder suspect. Upon arrival at the station, it was quickly confirmed that João Antônio was not the individual being sought (Durães, 2024). Following the incident, the governor of Sergipe, Fábio Mitidieri, announced via social media the suspension of the facial recognition system used by the State's Military Police. While acknowledging "the importance of technology for public safety" and the potential to "help fight crime", he also noted that "in light of the episode", he had ordered "the suspension of the system's use until a new protocol is implemented" (Durães, 2024, para. 28).

However, despite the suspension ordered in Sergipe, this was not the only reported case of mistaken identification using facial recognition technology. Another incident occurred during the "Pré Caju" festival, which Sergipe's governor mentioned. Thaís Santos, 31, was stopped twice by police officers at the same event after being falsely identified by facial recognition cameras as a fugitive from justice (Carmo, 2024).

In 2024, Natan de Oliveira Silva, 23, was also approached by police officers after the facial recognition system of the Military Police of Rio de Janeiro mistakenly identified him as a suspect in a crime he did not commit (Millan, 2024). Two years earlier, José Domingos Leitão, 52, was wrongly identified as a credit card fraudster by the Federal District's facial recognition system, resulting in his wrongful imprisonment for three days until the Military Police acknowledged the error (Bomfim, 2022).

It is worth emphasising that the successive cases reported occur within the context of the expanding use of this technology in Brazil and, more specifically, its adoption as a tool by public security agencies. A survey conducted by the online magazine Consultor Jurídico indicated that in just four states of the country, over 1,700 people have been arrested after being identified by facial recognition technology (Tajra, 2024). The study also revealed that these states do not maintain records of misuse rates, such as those reported in the cases mentioned.

While other countries, particularly after confirmed incidents of identification errors, have introduced bans on facial recognition[2] or issued court rulings declaring its use illegal[3], Brazil has experienced an institutional trivialisation of technological surveillance, with facial recognition emerging as a “flagship” of modern public security practices (Melo, 2024).

According to monitoring by the project *O Panóptico* (https://www.opanoptico.com.br/), there are currently 337 active[4] facial recognition projects in Brazil, predominantly utilised by public security agencies, potentially subjecting over 81 million people to surveillance.

Another survey indicates that at least 16 states and the Federal District already use facial recognition in transport, schools, parks, squares, and access to public services. Even in smaller cities, in terms of territory and population, technological surveillance is expanding (Igarapé Institute, 2024). An example of this is the report "O Mecenas" by The Intercept Brasil (Rebello, 2023), which revealed how a former federal deputy and mayors in Goiás allocated R$ 30,000,000 for the installation of facial recognition systems in 130 cities in the State, many of which lack even basic sewage treatment infrastructure.

This institutional trivialisation of technological surveillance in Brazil, particularly concerning facial recognition, can be attributed to three main factors: the lack of transparency about how it operates, who is responsible for its implementation, and the associated costs; the absence of a specific legal framework to regulate the use of these technologies, which allows individual managers discretion in their adoption; and the lack of

[2] In 2019, the city of San Francisco in the United States banned the use of facial recognition technology by the police and other security agencies (Conger et al., 2019).

[3] In 2020, the British courts declared the use of facial recognition technology by the South Wales Police illegal, ruling that it violated privacy rights (Rees, 2020).

[4] Active projects are defined as “those that are being tested, in use, in the process of implementation, or projects that already have established terms of reference. This indicates that all planning and preparation phases are either ongoing or have been completed, and facial recognition technologies are being implemented as a public security policy" (O Panóptico, 2024, p. 2). The data presented here are from January 21, 2025, the date of the most recent monitoring update prior to the publication of this paper.

consolidated statistical data regarding both their effectiveness in crime prevention and their acceptance by the population.

A decisive measure for the expansion of technological surveillance in Brazil was the financial incentive for the adoption of more technologies in the public security sector, such as Ordinance No. 793 (Portaria n.º 793, 2019), which regulated the National Public Security Fund. One of the actions was the allocation of resources for the "promotion of the implementation of video surveillance systems with facial recognition solutions, Optical Character Recognition (OCR), artificial intelligence, or other technologies (...) to combat violent crime" (Portaria n.º 793, 2019, p. 1).

In order to highlight the complexity of the Brazilian context, various articles and reports on the subject indicate that the majority of individuals misidentified by facial recognition systems are Black. João Antônio Trindade, Thaís Santos, Natan de Oliveira Silva and José Domingos Leitão all share a common characteristic: they are Black. A study by the Rede de Observatórios de Segurança (Security Observatory Network), drawing on data from five states that provided this type of information on race, found that 90% of individuals arrested through facial recognition in Brazil were Black (Ramos, 2019). The lack of detailed data on all cases of misuse prevents a more comprehensive analysis. However, it is crucial to consider the extent to which, in a country whose official history includes a prolonged slave-owning regime[5] and that today registers high incarceration rates among the Black population (Tvsenado, 2024), the adoption of facial recognition technologies constitutes a continuation — an update — of historical practices designed to surveil, classify, and segregate racialised bodies (Melo, 2024). Such practices have included branding enslaved people, using newspapers to advertise escaped enslaved people and employing photographic recognition in police stations as a means of identifying suspects.

Furthermore, the disproportionate impact of technologies such as facial recognition on racialised individuals is already evident in other countries. In the United Kingdom, for example, a report by researchers at the University of Essex indicated an error rate of 81% in the use of facial recognition by the London Metropolitan Police (Fussey & Murray, 2019), with most misidentifications involving Black people and migrants. In the United States, a study by Buolamwini and Gebru (2018) demonstrated significant disparities in error rates based on racial and gender identification: 0.8% for white men compared to 26% for Black man, and 34% for Black women.

4. Which Technologies? Which Discourses?

Following the presentation of the theoretical and conceptual framework underpinning this study, along with a brief overview of the adoption of surveillance technologies in public security in Brazil, attention now turns to an examination of the proposals for

[5] For almost four centuries — 388 years — the Brazilian economy was sustained by slave-based relations, which were central to the European colonisation of the country through the exploitation of Indigenous peoples and the transatlantic trade of enslaved Africans (Moura, 2014).

the use of technological surveillance in the electoral programmes of the administrators of the 15 most populous cities in the country.

A point that stands out even prior to an analysis of the documents submitted to the Tribunal Superior Eleitoral (Superior Electoral Court) for the 2024 elections is that all 15 mayors are men, and 13 of them self-identify as white, as shown in Table 2[6]. This is significant for two main reasons. First, it reflects the broader over-representation of men and white individuals in Brazil's political institutions[7] (Instituto de Estudos Socioeconômicos, 2024), a phenomenon rooted in what Bento (2022) terms the "narcissistic pact of whiteness"[8], understood here as part of a historical and structural process. Second, it is especially relevant in the context of this study due to the discriminatory potential of technologies such as facial recognition towards Black people and women.

City	Name	Party	Racial Declaration	Situation
São Paulo	Ricardo Nunes	Movimento Democrático Brasileiro (MDB)	White	Re-elected
Rio de Janeiro	Eduardo Paes	Partido Social Democrático (PSD)	White	Re-elected
Fortaleza	Evandro Leitão	Partido dos Trabalhadores (PT)	White	Elected
Salvador	Bruno Reis	União Brasil (UB)	White	Re-elected
Belo Horizonte	Fuad Noman	PSD	White	Re-elected
Manaus	David Almeida	Avante	Brown	Re-elected
Curitiba	Eduardo Pimentel	PSD	White	Elected
Recife	João Campos	Partido Socialista Brasileiro (PSB)	White	Re-elected
Goiânia	Sandro Mabel	UB	White	Elected
Belém	Igor	MDB	White	Elected
Porto Alegre	Sebastião Melo	MDB	Brown	Re-elected
Guarulhos	Lucas Sanches	Partido Liberal (PL)	White	Elected
Campinas	Dário Saadi	Republicanos	White	Re-elected
São Luís	Eduardo Braide	PSD	White	Re-elected
Maceió	JHC	PL	Brown	Re-elected

Table 2. *Mayors of the 15 most populous cities in Brazil*
Note. Own elaboration, based on data from the Superior Electoral Court (https://divulgacandcontas.tse.jus.br/divulga/#/home).

[6] This information the candidates themselves provided is available on the official website for candidates running for elected office in Brazil, accessible at https://divulgacandcontas.tse.jus.br/divulga/#/home, and was accessed on April 20, 2025.

[7] While, in general terms, 51.5% of the Brazilian population is composed of women and 55.5% are Black people (Instituto Brasileiro de Geografia e Estatística, 2024), the situation in positions of political power is markedly different: the majority are white men. In the National Congress, which includes the Chamber of Deputies and the Federal Senate, 71.9% of federal deputies and 66.7% of senators are white men. Regarding cities across the country, only 33.5% of mayors are Black, and just 13.2% are women (Instituto de Estudos Socioeconômicos, 2024).

[8] Cida Bento (2022) defines the "narcissistic pact of whiteness" as an unspoken agreement among those who hold power in public and private institutions, aiming to preserve their racial privileges. This pact is not formalised or regulated but is reinforced by the concept of whiteness as the norm, functioning as a tool to recognise and sustain racial inequalities.

Regarding this second aspect, Monagreda (2024) identifies seven risks associated with the use of digital technologies that disproportionately affect the Black population: (a) loss of privacy and the misappropriation of sensitive personal data, (b) commodification of daily life and the datafication of poverty, (c) the reproduction and automation of racism, (d) racial profiling and discrimination, (e) excessive surveillance and criminalisation, (f) impact on subjectivation processes, and (g) the erasure of the political nature of social issues.

> Within the politics of fear, which fuels the criminalisation and incarceration of the Black population, discourses surrounding public security emphasise surveillance, control, and punishment as central elements in the processing of personal data and the deployment of data-driven technologies. This reveals an intrinsic connection between racial profiling, surveillance, and criminalisation (...). The use of facial recognition cameras perpetuates and updates historical practices of biometric surveillance of the racialised Black body, promising to predict the moral character and the likelihood of criminal behaviour based on the measurement of facial features. (Monagreda, 2024, pp. 121–122)

With regard to gender, the study by Buolamwini and Gebru (2018) revealed that facial recognition software from major technology companies misidentified the gender of public figures, including Oprah Winfrey and Michelle Obama. The research found that facial recognition applications from IBM, Microsoft, and Face++ exhibited higher error rates when identifying faces in photographs of women, particularly Black women.

In this context, it is important to highlight that while the decision-making power concerning the use of surveillance technologies in public security in Brazil, such as facial recognition, rests predominantly with white men, the more severe consequences are disproportionately experienced by Black people and women.

In general, an analysis of the electoral programmes of the current mayors of the 15 most populous cities in Brazil revealed three gradations in proposals for the use of surveillance technologies in public security: (a) explicit and direct mentions of the technologies to be applied and their objectives; (b) reinforcement and expansion of existing programmes that already employ technologies such as facial recognition; and (c) general indications of intentions to use certain technologies.

In the first category, the proposals of the mayors of Salvador, Goiânia, Porto Alegre, and Guarulhos stand out, as they explicitly reference the use of drones, artificial intelligence technologies, facial recognition, and behavioural analysis, among other tools. Some of these proposals are outlined below.

- "Implement the Observatório Salvador (Salvador Observatory), which (...) will allow the city government to monitor the city in real-time through video screens, employing various artificial intelligence and data analysis technologies" (Salvador).
- "Acquisition of drones equipped with artificial intelligence for city surveillance" (Goiânia).
- "Deployment of cameras with facial recognition and artificial intelligence at key locations throughout the city" (Goiânia).

- "Establish a 'digital belt' with an extensive video surveillance network to enable quicker responses from the Metropolitan Guard and Military Police" (Goiânia).
- "Integrate video surveillance systems with databases of fugitives and missing persons, utilising artificial intelligence technologies for facial recognition, behavioural analysis, and video summaries, as implemented in this administration" (Porto Alegre);
- "Install security cameras with facial recognition as a measure to monitor and prevent crime. These cameras can identify faces and compare them with databases of wanted or suspected individuals, aiding in the identification and capture of criminals. This system's implementation aims to enhance the efficiency of identifying individuals and improve public safety" (Guarulhos).

In the second level of proposals, the mayors of São Paulo, Salvador, Belo Horizonte, and Porto Alegre — each re-elected — highlighted actions already in place that use digital technologies, emphasising, though without presenting statistical data, the benefits for crime prevention. Below are some of the proposals included in the government programmes:

- "To monitor and prevent crime, we have implemented the Smart Sampa programme, which involves the installation of thousands of smart cameras throughout the city, alongside Dronepol, using drones for surveillance" (São Paulo).
- "The expansion of the Smart Sampa video surveillance programme aims to integrate information systems and enhance city security. These actions seek to reduce crime and disturbances, ensuring public order and a sense of security" (São Paulo).
- "Mayors in Bahia have increasingly invested in public safety within their legal remit. Bruno Reis is among the most proactive, continuously working to improve safety through all available legal and generational means, focusing on surveillance, prevention, and the protection of the population (...). The city, which previously lacked smart cameras in public spaces and buildings, now has 1,900 cameras connected to the Municipal Guard" (Salvador).
- "In order to enhance security in the city centre, more than 460 video surveillance cameras have been installed" (Belo Horizonte).
- "[For Carnival 2024,] surveillance included 4,589 cameras across the city, 819 of which were new and modern, equipped with analytical software and artificial intelligence capable of detecting movements or risky situations that required special attention from the security forces. During Carnival 2023, 3,737 cameras were used for surveillance" (Belo Horizonte).
- "We expanded the functionality of the Detetive Cidadão app and modernised the Integrated Service Coordination Centre (...). Electronic vehicle fencing and video surveillance have been enhanced, including new artificial intelligence software" (Porto Alegre).

The Smart Sampa programme, cited by São Paulo Mayor Ricardo Nunes, is emblematic of the discussion here regarding the use of digital technologies based on suspicious categories. In the initial version of the tender for the acquisition of 20,000 facial recognition cameras, certain provisions suggested that monitoring should identify instances of "loitering and prolonged stay", that the search for wanted individuals should rely on "characteristics such as colour, face, and others", and that "tracking a suspicious person" should involve monitoring "all movements and activities" (Augusto, 2022, para. 4).

In the third tier, the mayors of Rio de Janeiro, Curitiba, Recife, and São Luís provided more general statements highlighting the importance of surveillance technologies, along with some intentions to adopt them. Below are some of the proposals outlined in their government programmes:

- "Continue expanding public lighting in neighbourhoods, installing security cameras, and advancing the electronic fencing of the Civitas Programme" (Rio de Janeiro).
- "Focus on enhancing security measures within the context of Smart Cities, integrating existing technologies and strategies under this overarching framework" (Curitiba).
- "Aim to strengthen social defence activities through ongoing training, professional development, and initiatives in public lighting, video surveillance, and the development of new social facilities" (Recife).
- "Implement a network of smart cameras at strategic locations throughout the city" (São Luís).

It is important to note that the cities mentioned in the third category do not necessarily have less impactful actions in this area. On the contrary, in some cases, there are well-established and expanding policies that further reinforce the institutional trivialisation of technological surveillance in the country. An example of this is the Digital Wall, a programme implemented by the Curitiba city government that "relies on the rhetoric of technological efficiency to justify a large-scale surveillance apparatus, using fear of urban violence as a driver for the expansion of algorithmic control of the city" (JararacaLab, 2025, para. 3). While Eduardo Pimentel did not explicitly include a proposal related to this initiative in his government programme, he was deputy mayor at the time of the Digital Wall's creation. In the 2024 elections, he listed "more Digital Wall cameras in the most at-risk neighbourhoods and community policing guided by data intelligence from the Wall's Risk Map" as one of his "55 promises for Curitiba" (Ribeiro, 2024, para. 39).

A similar situation can be observed in Recife. Although not explicitly mentioned in his government programme, Mayor João Campos approved and initiated the installation of digital electronic clocks in public spaces across the city in 2022. This project was carried out through a public-private partnership, with a 20-year concession for operation by private companies. In addition to displaying the time, traffic information, and temperature, the clocks are equipped with surveillance cameras featuring facial recognition technology (Prefeitura do Recife, 2022).

Another significant issue in the analysis concerns the partisan fragmentation of administrators who have implemented or proposed the adoption of technologies such as facial recognition in public security. Among the eight political parties represented by the mayors of the 15 cities mentioned here, there is a broad political spectrum — from the far-right (such as the PL, associated with former President Jair Bolsonaro) to centrist parties (PSD, Avante, Republicanos, MDB), the traditional right (UB), and the left (PSB and PT, associated with current President Lula)[9]. This diversity of political affiliation suggests that the widespread use of technological surveillance is not confined to any single ideological group.

It is also important to note that none of the 15 government programmes analysed mentioned the ethical implications of technological surveillance. Discriminatory impacts, known cases of misuse, or issues involving the regulation of technologies were

[9] The association of parties with different ideological profiles was based on a study conducted by Nexo (Zanlorenssi et al., 2024) on the genealogy and profiles of political parties in Brazil since 1945.

not addressed. In the case of ongoing initiatives, no statistical data were provided regarding the use and effectiveness of technologies such as facial recognition. On the contrary, there was a consistent reliance on adjectives to describe technologies in terms of combating crime and ensuring security, signalling a technosolutionist perspective.

5. Conclusions

The proposals for using digital surveillance technologies by public security agencies, as presented by the mayors of the 15 most populous cities in Brazil, underscore the growing institutional trivialisation of technological surveillance in the country — an issue already identified in a previous study by Melo & Serra (2022). This is evident in the increasing adoption of devices such as drones, facial recognition cameras, and behavioural analysis systems.

While the fight against crime and the pursuit of security remain the primary justifications for these technologies, the government programmes analysed do not provide statistical data to support claims of their effectiveness in reducing crime. Furthermore, the administrators fail to address ethical or regulatory concerns, instead resorting to positive descriptors to characterise the technologies. The absence of a specific legal framework governing their use further exacerbates the trivialisation, allowing mayors to unilaterally decide which devices to deploy, where, and how.

These observations, coupled with the opacity surrounding the operational logic, processes, and costs, as well as reported cases in various media outlets regarding errors in facial recognition — particularly in identifying Black individuals (Magno & Bezerra, 2020; Santos et al., 2023; Silva & Silva, 2024) — underscore the need for a deeper reflection on the discriminatory potential of these technologies. They also call into question the very notion of "modernity" often championed in the discourse of public officials. In a country with a history of slavery and deep racial inequalities, such as Brazil, the deployment of these technologies in public security risks exacerbating the logic of surveillance, classification, and the segregation of racialised bodies.

By addressing these concerns, this study contributes not only to the growing body of critical research on the expansion of technological surveillance in Brazil but also highlights the specific risks these technologies pose to the broader population, with a particular focus on Black people. By providing information and analyses on the proposals put forward by public managers, this article contributes to the ongoing assessment of the implementation of these systems in Brazilian cities. It offers a resource for researchers interested in the subject and for civil society organisations that have highlighted issues with facial recognition errors. In terms of limitations, the main challenge of this work lies in the difficulty of gathering systematic statistical data on the impact of technological surveillance in public spaces, particularly concerning its effects on citizens' rights. This challenge could be addressed through active and transparent actions by the State in producing and disseminating information on the operation and use of these systems.

Translation: Anabela Delgado

Acknowledgements

The Portuguese FCT — Foundation for Science and Technology, I.P., is acknowledged for funding the postdoctoral research grant, of which this article is one of the outcomes.

References

Augusto, T. (2022, November 28). *SP lança edital para sistema de câmeras que identifica cor e 'vadiagem'*. UOL. https://noticias.uol.com.br/cotidiano/ultimas-noticias/2022/11/28/sp-lanca-edital-para-sistema-de-cameras-que-identifica-cor-e-vadiagem.htm

Bauman, Z. (2013). *Vigilância líquida: Diálogos com David Lyon* (C. A. Medeiros, Trans.). Zahar. (Original work published 2012)

Belandi, C. (2024, August 29). *População estimada do país chega a 212,6 milhões de habitantes em 2024*. Agência IBGE Notícias. https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41111-populacao-estimada-do-pais-chega-a-212-6-milhoes-de-habitantes-em-2024

Bento, C. (2022). *O pacto da branquitude*. Companhia das Letras.

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

Brayne, S. (2022). The banality of surveillance. *Surveillance & Society*, *20*(4), 372–378. https://doi.org/10.24908/ss.v20i4.15946

Bridges, L. (2020). *Material entanglements of community surveillance & infrastructural power*. Association of Internet Researchers in Selected Papers of Internet Research. https://doi.org/10.5210/spir.v2020i0.11179

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. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 77–91.

Carmo, W. (2024, April 19). Erros em série expõem fragilidade do reconhecimento facial como ferramenta de combate ao crime. *Carta Capital*. https://www.cartacapital.com.br/tecnologia/erros-em-serie-expoem-fragilidade-do-reconhecimento-facial-como-ferramenta-de-combate-ao-crime/

Conger, K., Fausset, R., & Kovalesli, S. F. (2019, May 14). San Francisco bans facial recognition technology. *The New York Times*. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Durães, U. (2024, April 28). *Reconhecimento facial: Erros expõem falta de transparência e viés racista*. UOL. https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/04/28/reconhecimento-facial-erros-falta-de-transparencia.htm

Evangelo, N. S., & Oliveira, F. C. (2021). The Black social ranking experience at Uber: A racialized reflection on contemporary surveillance. *Comunicação e Sociedade*, *39*, 83–100. https://doi.org/10.17231/comsoc.39(2021).2838

Fontes, C., Hohma, E., Corrigan, C., & Lütge, C. (2022). AI-powered public surveillance systems: Why we (might) need them and how we want them. *Technology in Society*, *71*(1), 102–137. https://doi.org/10.1016/j.techsoc.2022.102137

Francisco, P., Hurel, L., & Rielli, M. (2020). *Regulação do reconhecimento facial no setor público: Avaliação de experiências internacionais*. Data Privacy Brasil; Instituto Igarapé. https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf

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

Graham, S. (2016). *Cidades sitiadas: O novo urbanismo militar*. Boitempo.

Instituto Brasileiro de Geografia e Estatística. (2024). *Censo IBGE 2022*. https://censo2022.ibge.gov.br/panorama/

Instituto de Estudos Socioeconômicos. (2024). *Em 10 anos, representatividade racial avança pouco na política*. https://inesc.org.br/em-10-anos-representatividade-racial-avanca-pouco-na-politica/

Instituto Igarapé. (2024). *Reconhecimento facial no Brasil*. https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

JararacaLab. (2025, February 5). *A economia política da vigilância "inteligente" em Curitiba*. https://jararacalab.org/digitalwall/

Khan, N., & Efthymiou, M. (2021). The use of biometric technology at airports: The case of customs and border protection (CBP). *International Journal of Information Management Data Insights*, *1*(2), 1–14. https://doi.org/10.1016/j.jjimei.2021.100049

La Quadrature du Net. (2024, May 2). *Against the empire of algorithmic video-surveillance, La Quadrature du Net strikes back*. https://www.laquadrature.net/en/2024/05/02/against-the-empire-of-algorithmic-video-surveillance-la-quadrature-du-net-strikes-back/

La Vigne, N., Lowry, S., Markman, J., & Dwyer, A. (2011). *Evaluating the use of public surveillance cameras for crime control and prevention*. Urban Institute Justice Policy Center. https://www.urban.org/sites/default/files/publication/27556/412403-evaluating-the-use-of-public-surveillance-cameras-for-crime-control-and-prevention_1.pdf

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

Magno, M. E. da S. P., & Bezerra, J. S. (2020). Vigilância negra: O dispositivo de reconhecimento facial e a disciplinaridade dos corpos. *Novos Olhares*, *9*(2), 45–52. https://doi.org/10.11606/issn.2238-7714.no.2020.165698

Marcolini, B. (2015, May 13). *David Lyon, sociólogo: 'A vigilância hoje é parte de nós'*. Globo. https://oglobo.globo.com/brasil/conte-algo-que-nao-sei/david-lyon-sociologo-vigilancia-hoje-parte-de-nos-16143232

Melo, P. V. (2024). Para quais rostos as câmeras apontam? Resistências à banalização institucional do reconhecimento facial no Brasil. *Contemporânea*, *23*(1), 1–18. https://doi.org/10.9771/contemporanea.v22i1.57561

Melo, P. V., & Serra, J. P. (2022). Facial recognition technology and public security in Brazilian capitals: Issues and problematizations. C*omunicação e Sociedade*, *42*, 205–220. https://doi.org/10.17231/comsoc.42(2022).3984

Millan, S. (2024, April 19). *Morador do Alemão é abordado por policiais em Bonsucesso devido a erro de reconhecimento facial*. Voz das Comunidades. https://vozdascomunidades.com.br/casos-de-policia/morador-do-alemao-e-abordado-por-policiais-em-bonsucesso-devido-a-erro-de-reconhecimento-facial/#google_vignette

Monagreda, J. K. (2024). Por que falar de raça quando falamos de dados pessoais, inteligência artificial e algoritmos? In A. Gonçalves, L. Torre, P. V. Melo (Eds.), *Inteligência artificial e algoritmos: Desafios e oportunidades para os media* (pp. 103–134). Labcom Books.

Moura, C. (2014). *Rebeliões da senzala: Quilombos, insurreições, guerrilhas*. Anita Garibaldi; Fundação Maurício Grabois.

O Panóptico. (2024). *Metodologia de monitoramento*. https://docs.google.com/document/d/1CM4P68Npyr6zR2myvjo1ulqJtpdoqOuPam8TiFah7yI/edit?tab=t.0

Portaria n.º 793, de 24 de outubro de 2019, Diário Oficial da União, Seção 1, 2019-10-24. (2019). http://dspace.mj.gov.br/handle/1/1380

Prefeitura do Recife. (2022). *Relógios eletrônicos digitais*. https://desenvolvimentoeconomico.recife.pe.gov.br/relogio-eletr-digitais

Ramos, S. (Ed.). (2019). *Retratos da violência: Cinco meses de monitoramento, análises e descobertas*. Rede de Observatórios de Segurança.

Rebello, A. (2023). *O mecenas*. The Intercept Brasil. https://www.intercept.com.br/2023/04/05/delegado-waldir-torrou-r-30-milhoes-em-reconhecimento-facial-para-cidades-que-sequer-tem-saneamento-em-goias/

Rees, J. (2020, August 11). *Facial recognition use by South Wales Police ruled unlawful*. BBC. https://www.bbc.com/news/uk-wales-53734716

Ribeiro, G. (2024, October 27). 55 promessas de Pimentel para o povo guardar e cobrar. *Gazeta do Povo*. https://www.gazetadopovo.com.br/eleicoes/2024/curitiba-pr/55-promessas-eduardo-pimentel-para-eleitor-de-curitiba-guardar-e-cobrar/

Rupp, I. (2024, September 20). O que prefeitos e vereadores podem fazer pela segurança. *Nexo*. https://www.nexojornal.com.br/expresso/2024/09/20/seguranca-publica-o-papel-do-prefeito-e-do-vereador

Santos, L. G. de M., Costa, A. B., David, J. S., & Pedro, R. M. L. (2023). Reconhecimento facial: Tecnologia, racismo e construção de mundos possíveis. *Psicologia & Sociedade*, *35*, e277141. http://doi.org/10.1590/1807-0310/2023v35e277141

Seshukumar, A. N., Vasavi, S., & Rao, V. (2012). A study on security within public transit vehicles. I*nternational Journal of Advanced Computer Science and Applications*, *3*(9), 188–191. https://doi.org/10.14569/IJACSA.2012.030928

Silva, F. dos S. R., & Silva, T. (Eds.). (2024). *Inteligência artificial e discriminação racial no Brasil: Questões principais e recomendações*. Instituto de Referência em Internet e Sociedade.

Tajra, A. (2024, May 17). *Ainda sem regulação, estados prendem centenas de pessoas utilizando reconhecimento facial*. Consultor Jurídico. https://www.conjur.com.br/2024-mai-17/sem-regulacao-estados-prendem-centenas-utilizando-reconhecimento-facial/

Tvsenado. (2024, June 27). B*rasil tem a terceira maior população carcerária do mundo*. https://www12.senado.leg.br/tv/programas/em-discussao/2024/06/politica-penitenciaria-esta-em-debate-no-senado-brasil-tem-a-3a-maior-populacao-carceraria-do-mundo

Viseu, A., Clement, A., Aspinall, J., & Kennedy, T. (2006). The interplay of public and private spaces in internet access. Information, *Communication & Society*, 9(5), 633–656. https://doi.org/10.1080/13691180600965633

Zolezzi, J. E. R., & Herrera, P. D. (2017). V*ideovigilancia en el espacio público: El monitoreo de la ciudad como dispositivo del control poblacional* [Tese de graduação, Universidad de Chile]. Repositorio Académico de la Universidad de Chile. https://repositorio.uchile.cl/handle/2250/146569

Zanlorenssi, G., Almeida, R., & Nunes, F. (2024). A genealogia e o perfil dos partidos brasileiros. *Nexo*. https://www.nexojornal.com.br/especial/2024/09/25/politica-origem-partidos-brasil-genealogia

Biographical Note

Paulo Victor Melo is a postdoctoral researcher at the Institute of Communication, NOVA University Lisbon. His research is supported by a national scholarship funded through the project UIDP/05021/2020, sponsored by the FCT under the Ministry of Science, Technology and Higher Education (MCTES). He holds a PhD in Contemporary Communication and Culture from the Universidade Federal da Bahia, Brazil.

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

Email: paulomelo@fcsh.unl.pt

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

Submitted: 10/02/2025 | Accepted: 04/04/2025