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

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

Paulo Victor Melo
Instituto de Comunicação da NOVA, Faculdade de Ciências Sociais e Humanas, Universidade Nova de Lisboa, Lisbon, Portugal
Conceptualization, data curation, formal analysis, investigation, methodology, writing – original draft, writing – review & editing

Paulo Serra
LabCom – Comunicação e Artes, Faculdade de Artes e Letras, Universidade da Beira Interior, Covilhã, Portugal
Conceptualization, formal analysis, investigation, methodology, supervision, writing – original draft, writing – review & editing

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

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

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

1. Introduction

The problem of urban violence and crime is one of the main concerns of the Brazilian population. On the eve of the 2018 presidential election, public security was indicated by voters as the second most serious problem in Brazil, second only to healthcare (Gelape, 2018). This perception is motivated by the fact that the country has an annual rate of over 40,000 murders, the highest absolute number of homicides worldwide, and a rate five times higher than the global average (Chade, 2019).

Since no doubt overcoming this issue requires a set of efforts and political actions, what answers have the public administrations of Brazilian cities offered in general security concerning the use of digital technologies? That is the driving question of this article, of which the primary objective is to analyze how proposals that foresee the application of technologies, defended by mayors of the country's capitals, relate to discourses on fighting crime.

Methodologically, delving into the question presented, the work began with the survey of government programs registered on the website of the Superior Electoral Court (n.d.) of all the current mayors of the 26 state capitals[1], elected in 2020 and sworn in in 2021.

From this, we identified in these government programs the proposals related to the use of digital technologies in public security, based on the use of 10 key expressions that are close to the researched object: "facial recognition"; "artificial intelligence"; "surveillance"; "video surveillance"; "monitoring"; "drone"; "camera"; "video"; "data"; "technology".

After gathering the programs that contained some proposals of interest to this work, a form was prepared to guide and standardize the analysis, including the following questions:

- What types of digital technologies are proposed for use in public security?
- Are those technologies integrated into a specific program?
- Are the proposals put forward as an alternative to fight crime?

[1] Aside from its 26 state capitals, Brazil has a federal capital, Brasília, that does not have a mayor.

- Are the possible benefits of using information and communication technologies in public security showcased?
- Are possible issues arising from using those technologies in the safety contexts mentioned?

These questions were defined to identify if there is, in the proposals of the mayors of Brazilian capital cities, a tendency to use digital technologies in public security regarding the fight against crime.

To fulfill the proposed objective and based on these methodological procedures, the article is structured as follows: firstly, (a) a brief theoretical-conceptual review on surveillance capitalism and the role of digital technologies in this process is made; then (b) information on cases of errors and failures in the identification of people by digital technologies in the area of public security in Brazil are presented and problematized from the perspective of algorithmic oppressions; in sequence, (c) the main results of the analysis are exposed, and some critical remarks are developed; and, lastly, (d) the conclusive considerations are pointed out.

2. Surveillance Capitalism and Digital Technologies: Some Remarks

Although they are often seen as the next stage after the disciplinary societies studied by Foucault (1970/1975), based on panoptic surveillance, the "control societies" themed by Deleuze (1992) do not imply less surveillance than the previous ones. The surveillance device is based on technologies that allow information production, diffusion, and collection. Surveillance, far from going away, becomes even more ingrained and radical: if in disciplinary societies, individuals are watched in an on-site, localized, punctual, and involuntary way, in control societies, they are now watched in a virtual, delocalized, omnipresent, and voluntary manner. The term "network society" (Castells, 1996/1999) expresses well, *malgré soi*, this idea of the individual trapped in a web from which he could only escape if, like Robinson Crusoe, drifted away to some island cut off from the world — but he would always risk meeting his Friday, now carrying a cell phone.

No wonder, then, that in his classic text on the subject, Lyon (1994) speaks of a new panopticon that emerges in the information society, the "electronic eye", based on the systematic collection of data on citizens by the state and by companies, registering the smallest gestures of their daily lives. It is precisely this process that underlies what Lyon (1994) calls the "surveillance society", the term "surveillance" is used here precisely "as a shorthand term to encompass the many and expanding ranges of contexts in which personal data are collected by employment, commercial, and administrative agencies, as well as in policing and security" (p. ix). This theme of surveillance is taken up and deepened by Lyon in other later texts, most prominently in the book *The Culture of Surveillance: Watching as a Way of Life* (Lyon, 2018). In this work, the concept of "surveillance society" is reviewed in a double sense: first, in the fact that surveillance is not only an activity exercised, on oneself, by entities external to the subject — but it is the subject itself who, freely and voluntarily, provides data about itself and its various activities

(namely through social networks); second, because hetero and self-surveillance become a regular and normalized practice and natural. This artificial "naturalness" of the norms and practices of surveillance constitutes a "surveillance culture".

In turn, inspired by Foucault, Rouvroy and Berns (2013) designate the type of surveillance that emerges in "control societies" as "algorithmic governmentality". The inspiration in Foucault lies in the fact that the authors see algorithmic governmentality in the continuity of a form of "power" exercised not over the physical body (law, discipline) or the moral conscience (herding, confession), based on interdiction or prescription, but through "security devices", based on regulation:

> the regulation of a means in which it is not so much a question of fixing limits, borders, in which it is not so much a question of determining locations, but above all essentially of allowing, of guaranteeing, of ensuring circulations: circulation of people, circulation of goods, circulation of air, etc. (Foucault, 2004, as cited in Rouvroy & Berns, 2013, p. 175)

In this sense, the authors define algorithmic governmentality as "a certain type of (a)normative or (a)political rationality that rests on the automatic collection, aggregation, and analysis of massive amounts of data to model, anticipate and affect [i.e., to regulate] possible behaviors in advance" (Rouvroy & Berns, 2013, p. 173). The data that subjects voluntarily provide about themselves and their lives to technological-informational platforms and networks are used by these and by the various economic, political, military, and police powers that articulate with them to build "profiles" that allow directing and guiding individual behaviors in specific directions instead of others, thus determining paths, defining activities, delimiting choices. The "freedom" and "autonomy" of subjects do not cease to exist, but they are conditioned to specific frameworks whose choice does not depend on themselves. These frameworks are lateral to their "freedom" and "autonomy".

Also, from Foucault's perspective on the "genealogy of the modern soul", in which subjectivities are inseparable from visibility devices, Bruno (2004) emphasizes that contemporary communication technologies are characterized by the focus of visibility on the ordinary individual. This aspect is determinant in the production of subjectivities and identities.

> The gaze is no longer on those who exercise power but on those over whom power is exercised. On the typical, ordinary individual, and even more on those below the usual and average — the deviant, the abnormal. It is, in fact, an individualizing gaze, a power that individualizes by looking, making the common individual visible, observable, analyzable, and calculable. Thus, power becomes more and more anonymous. In contrast, the standard or deviant individual, exposed to visibility, becomes more and more objectified and tied to one identity — the criminal, the sick, the crazy,

> the student, the soldier, and the worker have their behaviors, symptoms, manias, addictions, failures, performances, aptitudes, merits and demerits invested, known, registered, classified, rewarded, punished by the machinery of hierarchical surveillance. (Bruno, 2004, p. 111)

The tragic irony of this new surveillance system is that its leading agent is the subject itself, who paradoxically freely subjects itself in the context of what Zuboff (2018/2020) calls "surveillance capitalism". A regime that started with Microsoft continues with Google, Facebook, and other social networks and is now generalized to all products, services, and devices that can integrate into the so-called "internet of things".

In an introductory text on the topic, Zuboff (2019) points to four key features in the constitution of surveillance capitalism: the massive extraction and analysis of data; the development of new contractual forms using computational monitoring and automation; the desire to personalize and customize the services offered to users of digital platforms; and the use of technological infrastructure to perform future experiments on its users and consumers.

> The accumulation logic that would ensure Google's success appears clearly in a patent filed in 2003 by three of the company's top computer scientists, entitled "Generate user information for targeted advertising". The invention, they explain, would seek to "establish user profile information and use it for ad dissemination". In other words, Google would no longer be satisfied with extracting behavioral data to improve its services. It would move on to reading users' thoughts to match ads to their interests, which in turn would be deduced from collateral traits of online behavior. The collection of new data sets, called *User Profile Information*, would significantly improve the accuracy of these predictions. (...) The invention of Google has revealed new possibilities for deducing the thoughts, feelings, intentions, and interests of individuals and groups through an automated extraction architecture that works as a one-way mirror without regard to the awareness and consent of those involved. This extraction imperative has resulted in economies of scale that would provide a unique competitive advantage in a market in which predictions of individual behavior represent a value that can be bought and sold. But above all, the one-way mirror symbolizes particular social relations of surveillance based on a spectacular asymmetry of knowledge and power. (Zuboff, 2019, paras. 9, 11)

Such a regime, presented in more or less "economic" language, has as its raw material our experience with technologies and the data we yield during that experience. From this data, manufacturing processes based on "machine intelligence" allow the manufacture of "prediction products" that feed a "market of future behaviors" (Zuboff, 2018/2020, p. 13). Through these future behaviors, technologies like Microsoft, Google,

Meta (owner of Facebook, Instagram and WhatsApp), and many others sell to the companies that produce a wide variety of goods and services and to the various political-military and police powers.

Now, the data that digital technologies and their respective databases collect and archive are increasingly pictures, especially pictures of our faces, and those technologies have been improving, over time, their ability to process those images. Combining these processes — image collection, archiving, and processing — makes face recognition possible. That companies like Amazon, Google, Microsoft, or IBM have been developing facial recognition programs from image databases in recent years is proven by news reports such as those that emerged in mid-2020, according to which the first three of those companies were being sued by citizens because their photographs from an IBM database were being used without their permission (Musil, 2020).

3. Facial Recognition and Discrimination

> I suffered because the neighbors judged me. I lost many jobs because they said I was a drug dealer. I said I was innocent, and the police told me to think about what I had done. I thought a lot about my family and that I wouldn't see them again. (Bomfim, 2022, para. 12)

These were the words of José Domingos Leitão, 52, in a statement to the R7 portal, after spending three days in jail in October 2020.

Living in the municipality of Ilha Grande, Piauí, José Domingos Leitão was mistakenly identified by facial recognition technology as the author of a crime. The fact that José lives more than 2,000 km from where the crime occurred and that he had never been to the city where the fact occurred was not even considered since his image was in a national database used by the Federal District Police.

Roughly speaking, facial recognition begins with scanning an individual's face. From this, the features and characteristics of the face are transformed into "reference points" that are analyzed, as an identifier associated with that person, so that the database can then normalize with other faces classified in patterns or types based on a certain level of similarity.

> Face recognition is a form of biometrics that links a unique element of an individual's human body with a unit of record. The body element can be the fingerprint, the face, or the way of walking. The most common units of registration are those such as the General Register (RG), the Social Security number, or the bank account. The part of the body used for biometrics, be the fingerprints or the face, is never analyzed in its entirety. That means that some points on the face or finger are chosen, and based on the distances between these points, the probability is calculated that the finger or face

> belongs to the person registered in the database. In the case of the human face, the possibilities of differences or modifications in these distances are much greater than in a fingerprint since a person ages, might be yawning, or blinking. (Nunes, 2019, pp. 67–68)

Thus, in addition to using for collective monitoring, facial recognition can identify, track, single out and trace people in the places where they transit, thus being able to exercise specific surveillance and violate rights such as privacy, data protection, and non-discrimination.

In the United States, a similar case to that of José Domingos Leitão was registered in 2019, when Robert Williams spent 30 h in jail, in Detroit, also due to an error in the facial recognition system of the Michigan State Police. According to the American Civil Liberties Union, Williams was "the first person wrongfully arrested based on this technology" (Robertson, 2021, para. 1).

A few years earlier, however, the American Civil Liberties Union was already warning of possible problems in this regard. Using a facial recognition tool developed by Amazon, Rekognition FR, the organization applied a survey to members of the United States Congress. It concluded that 28 members of Congress were mistakenly identified with other people already arrested for some crime, most of them Black people (Snow, 2018).

Since then, facial recognition technology errors have been mounting in the United States (O'Neill, 2020), Brazil (G1 Rio, 2019), and other countries. In the United Kingdom, for example, a report produced by researchers at the University of Essex identified an 81% error rate in cases using facial recognition by the London Metropolitan Police (Fussey & Murray, 2019).

In Brazil, data from the Network of Security Observatories (Ramos, 2019) point out that between March and October 2019, in four states surveyed (Bahia, Paraíba, Rio de Janeiro, and Santa Catarina), 151 people were arrested using facial recognition technology, and in cases where there was information on race and color, 90.5%, were Black.

Different authors (Broussard, 2018; Lohr, 2018; Nakamura, 2008) have pointed out that, beyond "natural" errors and failures, these cases highlight the discriminatory nature of these technologies. Broussard (2018) recalls that algorithms "are designed by people, and people incorporate their unconscious biases into algorithms. It is rarely intentional, but that doesn't mean we should stop analyzing. It means we should be critical and vigilant about things we know can go wrong" (p. 289).

In formulating the concept of algorithmic racism, Silva (2019) points out that there is, in the design of digital technologies, a double opacity regarding the aspect of racialization, characterized by the idea of technology and algorithms as neutral and, at the same time, by the ideology of denial and invisibility of race as a social category.

> I elaborate on "algorithmic racism" to describe how automated interfaces and systems, such as social media platforms, can reinforce and hide the racist

> dynamics of the societies where they are used and employed. It is important to stress that the problem is not this or that specific algorithm but "how racist societies consequently construct technologies with discriminatory potentials or applications". (Silva, 2019, para. 6)

In a kind of "timeline" of algorithmic racism, Silva (2019) presents a diversity of cases, data, and reactions to racialization processes in interfaces, databases, algorithms, and artificial intelligence, such as Google systems that allow companies to display ads about crime specifically to African Americans; results in Google Images that show hypersexualized content for searches such as "Black girls"; tagging photos of young Black men with the tag "gorilla" by Google Photos; conversational robots of startups that do not find Black women's faces; and computer vision systems that miss gender and age of Black women; image bank search engines that render Black families and people invisible; apps that transform selfies and equate beauty with whiteness; natural language processing tools that have biases against Black language and themes; facial emotion analysis that associates negative categories with Black athletes.

In the same direction pointed out by Silva (2019), a study developed by Buolamwini and Gebru (2019) from the Massachusetts Institute of Technology revealed that the margins of error of facial recognition were quite different according to skin color and gender: 0.8% in the case of white men, 26% when Black men and 34% in the case of Black women, one of the motivations being the low representation of faces of darker shades in the datasets, thus leaving the recognition more inaccurate regarding this racial-ethnic group.

> Recent studies show that machine learning algorithms can discriminate based on classes such as race and gender. (...) The substantial disparities in the classification accuracy of darker women, lighter women, darker men, and lighter men in gender classification systems require urgent attention if commercial companies are to build genuinely fair, transparent, and accountable facial analysis algorithms. (Buolamwini & Gebru, 2019, p. 1)

The results of studies like the ones mentioned above have generated reactions against adopting facial recognition in different parts of the world. Some examples are Big Brother Watch (https://bigbrotherwatch.org.uk/) and Liberty Human Rights (Liberty, n.d.), both in England; the "Ban Facial Recognition" campaign (https://www.banfacialrecognition.com/) in the United States; and the Internet Freedom Foundation (n.d.) in India.

In Brazil, in May 2022, hundreds of digital rights organizations, activists, and researchers launched the "Tire o Meu Rosto da Sua Mira" (get my face out of your sights) campaign, which calls for a total ban on digital facial recognition technologies in public security, given the potential for abuses and rights violations.

> Surveillance technologies create insecurity by violating our rights without giving us chances to avoid or even consent to its implementation and by making

> us targets. Notably, the violations of our integrity, by the collection and processing of personal biometric data; of our freedom to come and go and self-determination, as we may be under surveillance 24/7, creating a frightening context; of our right to the due legal process, as mass surveillance considers everyone guilty as a matter of principle, undermining the constitutional guarantee of the presumption of innocence as a fundamental legal assumption. (Tire o Meu Rosto da Sua Mira , 2022, para. 6)

Other initiatives also aimed at banning facial recognition are worth mentioning. Such as Bill 824/2021 (Projeto de Lei 824/2021, 2021), filed by Councilman Reimont (Workers' Party), which proposes a ban on the use of this technology by Rio de Janeiro city hall, and the Public Civil Action, signed by public agencies and civil society organizations, which aims to ban the use of facial recognition in the São Paulo subway (Intervozes, 2022).

4. Main Results

As a result of the first methodological stage of the work, based on the previously defined key expressions, 15 of the current 26 mayors of Brazilian capitals presented, in their government programs in the last election, proposals that involve the use of digital technologies in public security.

The geographical distribution and the party distribution of these 15 mayors — which include cities from all five regions (North, Northeast, Central-West, Southeast, and South) and belong to 11 different political parties[2] — indicate that the perspective of using technologies as a strategy for security actions is not an issue restricted to one or another part of the country or specific ideological groupings.

Among the types of technologies proposed by the 15 mayors[3], as shown in Figure 1, 13 mayors mentioned the installation or expansion of video surveillance or monitoring cameras, either in public transportation, on urban roads, or in other circulation spaces, such as parks and squares; eight mayors proposed the application of facial recognition; four presented actions using drones, and five referred to other technologies.

[2] The following political parties are represented by the 15 mayors, having proposals that are of interest to this paper: Avante (one), Democrats (two), Brazilian Democratic Movement (two), Labor Democratic Party (one); Brazilian Socialist Party (one), Social Democratic Party (two), Brazilian Social Democracy Party (three), Podemos (one), Progressive Party (two), Republicans (one), União Brasil (one).

[3] It should be noted that some mayors mentioned the use of more than one technology.

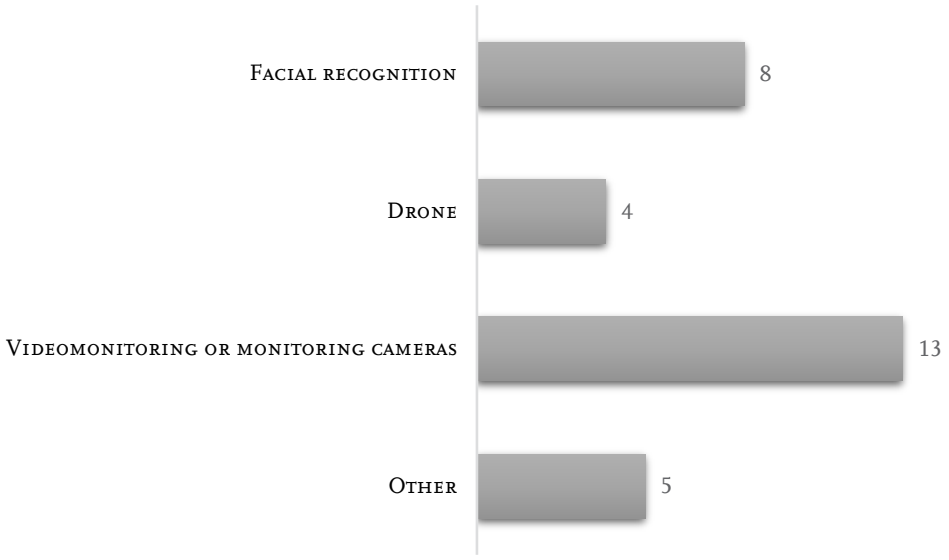

Figure 1 *Types of technology*

The research also showed that seven of the 15 mayors proposed using technologies in broader public security initiatives. Expressions such as "wall", "fencing", "security", and "safe", among others, as seen in Table 1, denotes a perspective of segregation, control, and surveillance in the implementation of these technologies by public managers.

Program name	City
Muralha Digital (Digital Wall)	Curitiba
Cercamento Eletrônico da Cidade (Electronic City Fencing)	Aracaju
City Câmeras (City Cameras)	São Paulo
*De Olho na Rua (*Watching the Street)	Goiânia
Teresina Segura (Safe Teresina)	Teresina
Vitória Segura (Safe Vitória)	Vitória
Andar Seguro (Walking Safely)	João Pessoa

Table 1 *Program names that connect technologies and public security in Brazilian capitals*

Another aspect evidenced in the reading of the government programs was the forecast of strategies that propose the direct involvement of the population in the city's surveillance.

The management program of Mayor Maguito Vilela (Brazilian Democratic Movement), from Goiânia, points out that "condominiums with video camera systems will be required to have part of the equipment monitoring the streets".

A similar measure is proposed by Rafael Greca (Democrats) in Curitiba, who defended "the incentive to the population (residences, buildings, and condominiums) and companies (commerce/services)" in collaboration with the *Muralha Digital* (Digital Wall) program.

In Belo Horizonte, the government plan of Mayor Kalil (Social Democratic Party)

signaled that the Operations Center of the City Hall "would also have cameras and sensors installed by citizens themselves. Their images could be made available through a collaborative monitoring platform, expanding the coverage of the city and improving responses to various situations of security and public disorder".

It is worth questioning that proposals such as those presented above contribute to a kind of "public big brother" in which everyone is, at the same time, a potential watcher and potentially watched, compromising the very notion of public space as an environment for the free circulation of citizens.

Moreover, the analysis identified that in 80% of government programs, the application of technologies in public security is expressly defined as a strategy to fight crime. In this sense, reducing vandalism, depredations, thefts, robberies, invasions, graffiti, assaults, and sexual violence, among others, are cited as the purpose of using technologies.

Furthermore, in 11 of the 15 government programs, generic statements are presented, without details, about the benefits to the population of using digital technologies in public security, such as "more security" (government programs of Teresina, São Paulo, Manaus, Palmas, and Curtiba), "expansion of coverage of the city" (government programs of Aracaju, São Paulo, Campo Grande, Natal, and Rio Branco), and "improvement of responses to the various security situations" (Vitória, Curitiba, and Florianopolis).

On the other hand, although there was already news about rights violations generated by technologies such as facial recognition, like the ones mentioned in this paper, none of the government programs cited any possible problem in using these technologies in public security, nor even alternatives to potential problems. At least in the proposals of the current mayors of Brazilian capitals, it did not appear as a topic of concern.

It is important to note that other capitals where the current mayors did not present a specific proposal in their mayoral programs in the last elections have witnessed actions involving digital technologies in public security. Examples of this are Salvador, Recife, and Rio de Janeiro, which in recent editions of the Carnival (Intervozes, 2019) have carried out surveillance and monitoring via facial recognition from state government initiatives in partnership with multinational technology companies, such as Huawei (Falcão, 2021), Avantia (Ams, 2019), and Oi (Kawaguti, 2019).

In Rio de Janeiro, when the cameras initially installed for carnival 2019 were still in the testing phase, a woman — who was sitting on a bench in the Copacabana neighborhood — was mistakenly arrested by the Military Police after being identified, via facial recognition technology, as a suspect for the crimes of murder and concealment of a corpse. However, hours later, at the police station, they found out that the real author of that crime had already been arrested for it in 2015.

In Recife, despite not being mentioned in his government program, Mayor João Campos (Brazilian Socialist Party) announced in late 2021, still in the 1st year of his administration, the intention to install 108 digital clocks that, in addition to displaying time and traffic information, would have monitoring cameras with facial recognition (Diário de Pernambuco, 2021). Although the adoption of digital clocks has been postponed, the

proposal's implementation involves the possibility of a public-private partnership, granting the operation to private companies for 20 years (Santos, 2021).

Although the proposal was not included in his government program registered during the election period, the mayor of Salvador, Bruno Reis (Democrats), announced, in the last months of 2021, the installation of cameras with facial recognition at touristic locations in the city, one of the motivations expressed by the manager being the fight against crime (Redação, 2021).

It is also worth noting that the adoption of these technologies has been encouraged by the federal government. For example, Ordinance No. 793 (Portaria nº 793, 2019), when regulating the National Public Security Fund, provides resources for the "promotion of the deployment of video surveillance systems with facial recognition solutions, by Optical Character Recognition – OCR, use of artificial intelligence or others", is one of the fundable actions for the "fight against violent crime" (Portaria nº 793, 2019, Article 4).

In addition to the aspects evidenced in the analysis of government programs and understanding of the increasing relevance of digital technologies in public security, questions such as: when managers mention "suspicious persons", what data are collected to build these profiles? How are the databases that support these technologies developed, and what do they contain? Besides the automated action of algorithms, who is behind the facial recognition cameras? Are there any protection mechanisms for personal data? Which databases are being cross-referenced? Who stores, qualifies, and indexes these databases? Who is granted access, and who is denied it? What is being recorded? What is understood as "good practices" in the use of these technologies when there is still no current legislation regulating their use?

5. Conclusions

The results of the analysis of the government programs of the Brazilian capitals' current mayors suggest that the use of digital technologies to fight crime is a trend in public security policies in the country. Given this issue and the growing cases of wrongful arrests and other errors in identifying people based on facial recognition, these technologies must be supported by public discussion and monitoring involving the different segments of society.

In this sense, we should be alert to the fact that none of the government programs analyzed indicates any concern with possible risks of violating the rights of citizens due to errors in the use of digital technologies.

In a country that already has a history of wrongful imprisonment for non-digital photographic recognition (*Exclusivo: 83% dos Presos Injustamente por Reconhecimento Fotográfico no Brasil São Negros*, 2021), primarily Black people, which has the third largest prison population worldwide (Pastoral Carcerária, 2018) and characterized by the genocide of the Black population as a structuring logic of the state (Nascimento, 1978), it is also essential that the implementation of digital technologies, especially facial recognition, is guided by all possible ethical, social, political, and cultural implications, so that,

in the quest to fight crime and increase security, violence against historically discriminated groups is not perpetuated.

Translation: Susana Valdez

References

Ams. (2019, March 27). 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, 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

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, Trans.). Paz e Terra. (Original work published 1996)

Chade, J. (2019, April 4). *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, October 26). 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, February 21). 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, September 20). *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, Trans.). Editora Vozes. (Original work published 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, September 11). *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. (n.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, March 14). 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, March 4). *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, January 24). *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. (n.d.). *Resist facial recognition*. https://www.libertyhumanrights.org.uk/campaign/resist-facial-recognition/

Lohr, S. (2018, February 9). 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, July 14). *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, September 4). 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, October 13). 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, April 13). *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, November 26). 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, July 11). 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, July 26). *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, March 8). *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. (n.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, January 3). 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, Trans.). Intrínseca. (Original work published 2018)

Biographical Notes

Paulo Victor Melo is a post-doctoral researcher at the NOVA Institute of Communication, NOVA Faculty of Social Sciences and Humanities, with grant supported by the project UIDP/05021/2020, nationally funded by FCT/MCTES. He has a PhD in contemporary communication and culture from the Federal University of Bahia and did post-doctoral work at the University of Beira Interior with LabCom – Communication and Arts. He is the coordinator for the Center for Communication, Democracy, and Citizenship at the Federal University of Bahia.

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

Paulo Serra has a degree in philosophy from Lisbon's School of Arts and Humanities and a master's, a doctorate, and an aggregate degree in communication sciences from

the University of Beira Interior, Portugal. At this university, he is a full professor at the Department of Communication, Philosophy, and Politics and a researcher at LabCom – Communication and Arts. He was the president of the Portuguese Association of Communication Sciences.

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

Email: pserra@ubi.pt

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

Submitted: 25/03/2022 | Accepted: 03/06/2022