PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 4 Number 5 October 2025

# Effects of Biometrics on Public Security in Brazil: An Analysis of Facial Recognition and Algorithmic Racism

**Pablo Ornelas Rosa[1], Clécio José Morandi de Assis Lemos[2], Aknaton Toczek Souza[3] & Eudson Ferreira Bento[4]**

[1] Doctor of Social Sciences; Professor, Universidade Vila Velha (UVV) & University Center of Vale Cricaré (UNIVC); Productivity Grant Holder, Fundação de Amparo à Pesquisa do Espírito Santo (FAPES), Brazil
[2] Doctor in Law; Professor, Federal University of Espírito Santo (UFES) & University Center of Espírito Santo (UNESC), Brazil
[3] Doctor of Sociology and Law; Professor, Catholic University of Pelotas (UCPEL), Brazil
[4] Master in Public Security; Chief of the Civil Police of Espírito Santo (ES), Brazil
Correspondence: Pablo Ornelas Rosa, Doctor of Social Sciences; Professor, Universidade Vila Velha (UVV) & University Center of Vale Cricaré (UNIVC); Productivity Grant Holder, Fundação de Amparo à Pesquisa do Espírito Santo (FAPES), Brazil.

doi:10.56397/SLJ.2025.10.08

**Abstract**

This article presents a literature review on the relationship between racism and the use of facial recognition technology by Brazilian Public Security. The text is organized into four sections: the first presents phenomena such as platformization, the datafication of life, data colonialism, platform capitalism, and surveillance; the second sets out some characteristics of this technology; the third highlights studies on racial discrimination through algorithms; finally, the fourth presents the main consequences of algorithmic racism in Public Security. It concludes that there is a need for a broad debate on these discriminatory algorithmic practices, in order to avoid the violation of fundamental rights and guarantees.

**Keywords:** racism, algorithm, public security, fundamental rights

## 1. Introduction

Tools such as artificial intelligence, digital certification, the Internet of Things, among many others, are just some examples of how technology has been transforming the everyday lives of individuals, companies, and the State itself. As it becomes embedded in our practices, producing changes in behavior, technology also presents impasses. One of these questions concerns the new guise that racism takes on, including involuntarily, in this ocean of bytes, contaminating it with its structural characteristics, particularly algorithmic blocking operations targeting Black people and the use of

digital robots (bots)[1] for supremacist discourses, most of the time operating without being noticed (SILVA, 2020).

The subtlety of this new form of discrimination arises from the fact that we have come to live in a society characterized by the intensive use of software that becomes the primary form of social interaction, which implies a broad mobilization of algorithms used for predictive purposes (SILVEIRA, 2016; DA EMPOLI, 2019; ZUBOFF, 2020). The normalized use of mobile phones, tablets, and other gadgets indicates the growing presence of these technologies in our everyday lives, intensely permeating our relationships.

However, neither software nor the algorithms contained in it operate in a neutral manner. On the contrary, they produce effects because they are created and developed by human beings with certain purposes in mind. Thus, although they are immaterial and apparently invisible, they have a starting point and a goal that may express discrimination, even if in an unintentional way.

These facts become even more concerning with the application of facial recognition by Public Security agencies, which makes it essential to study the precedents involving artificial intelligence and racism, including their concepts, history, and structure. Accordingly, this article aims to analyze this new facet of racial discrimination, contributing to its understanding and investigation insofar as it seeks to grasp how it occurs today. For some time now, this method of facial recognition has been surrounded by controversy, especially when studies indicate that such technology is prone to errors in the analysis of the faces of Black people or other minorities, which deserves our concern (SILVA, 2020; BEIGUELMAN, 2021; AMARAL, MARTINS & ELESBÃO, 2021; NOBLE, 2021).

The text that follows is organized as follows: the first section sets out some of the assumptions that address the phenomena of platformization and the datafication of life; the second addresses some of the main characteristics of facial recognition technologies; the third highlights the elements that constitute them; and, finally, the last section presents some of the main consequences of this form of social control, with an emphasis on the field of Public Security.

**2. Platform and Surveillance Capitalism**

On the way into the twenty-first century, significant transformations took place in the ways in which people began to relate to one another, as well as in how they are constituted as subjects, due to the gradual intensification of the use of digital platforms in their communication, altering access to information, which had previously been marked by the primacy of face-to-face interaction (ROSA, AMARAL & NEMER, 2021, p. 02).

Therefore, it is important to describe the process of platformization and the datafication of life, from whose influence Public Security is not immune. With regard to platformization, it is necessary to highlight the contributions of Poell, Nieborg, and Dijck (2020, p. 05), who define it as a form of "penetration of platform infrastructures, economic processes, and governmental structures into different economic sectors and spheres of life."

Following the same authors, it is possible to clarify that platforms are programmed digital models that act upon interactions between people and complementors, doing so through the systematized collection of data, the use of algorithms, and monetization.

Nevertheless, it is also necessary to highlight other significant contributions on this phenomenon, characterized by the conditioning of human relations on social networks, described sometimes as "surveillance capitalism" (ZUBOFF, 2020) and sometimes as "platform capitalism" (SRNICEK, 2018).

Understanding that we have entered an era characterized by what he called platform capitalism, Nick Srnicek (2018, pp. 44–45) identified five specific types of digital platforms that operate on the basis of distinct business models: (a) advertising platforms, which extract and use user data as products sold to advertisers, as in the cases of Google and Facebook; (b) cloud platforms, owners of business hardware and software that are dependent on the digital and that generate profits according to the needs of their client firms, on the basis of an enormous logistical network, such as Amazon and Web Services; (c) industrial platforms, such as General Eletric and Simens, which produce the hardware and software necessary for the transformation of

[1] "Bots are autonomous applications that run on the Internet while performing some type of predetermined task" (GARRET, 2022).

traditional manufacturing into processes connected to the internet; (d) product platforms, such as Rolls Royce and Spotify, which transform a traditional good into a service and charge a rental fee or subscription fee; and (e) lean platforms, such as Uber and Airbnb, which operate through subcontracting, charging a high cost for their use. The author further clarifies that these categories may coexist within the same company.

According to Zuboff (2020, p. 247), the impact of what she called surveillance capitalism, characterized by the intensive use of digital platforms, is felt in the infrastructures of markets, governance, and, notably, data.

In this last case, it is possible to see that it gives rise to the so-called datafication of life, understood by André Lemos (2021, p. 02) as "forms of transforming actions into quantifiable data, allowing extensive tracking and predictive analyses," with the potential to expand into many other fields, such as politics, the economy, culture, etc., reaching the field of Public Security through its consequent biometric use via facial recognition technologies.

As we deepen our understanding of the datafication of life, it is possible to understand it as a new way of producing knowledge, involving a digital requisition or even translation of the world that makes it possible to exercise a certain control over objects and/or actions, with the aim of simulating and testing them in advanced computer systems operated by artificial intelligence (AI). Thus, we have a new hegemonic way of knowing and managing life on the planet (LEMOS, 2021, p. 197).

In this process, the datafication of life has influenced various forms of knowledge, including scientific knowledge, since it has become evident that data do not function in a neutral way, insofar as they produce biases, favoring a technocratic power operated under the tutelage of specialists in algorithms and with public interests.

Lemos (2021, p. 198) further adds that the datafication of knowledge could promote a power led by an "epistocracy," operated through an "algocracy" grounded in the technical neutrality of algorithmic performativity, which would decide about doing and knowing, insofar as it would introduce into human interactions a kind of lens that, just as mathematics was instrumentalized by Newton in the seventeenth century, could be treated as "the great book of nature."

The understanding of this phenomenon perhaps becomes clearer in the analyses carried out by Siva Vaidhyanathan (2011, p. 40) when he deals with the Googlization of everything. According to the author, "Google collects the gigabytes of personal information and creative content that millions of its users provide free of charge to the network every day, and sells this information to advertisers of millions of products and services." In this way, by noting that Google asserts itself by persuading us that it knows exactly what to do to improve our lives, Vaidhyanathan (2011, p. 29) found that this company has come to determine our behavior, controlling the network without raising any suspicion that it exercises authoritarian practices.

The datafication of life is understood by André Lemos (2021, pp. 199–200) as a new era of digital culture, anchored in some dimensions that can be systematized in the form of: (a) knowledge, as it involves a new production through the extraction and management of data; (b) sociability, since it makes the surveillance and collection of personal information routine; and (c) nature, insofar as it negatively impacts the environment through the way natural goods (especially minerals) are consumed and electronic waste is discarded, in addition to the high energy consumption of data centers. Thus, although these impacts seem to be completely unknown to the public, it is important to remember that:

Data are not found in nature, as Couldry and Mejias (2019) have warned. This is a crucial point of the phenomenon of datafication. They are designed and depend on extraction and storage algorithms. As Tarleton Gillespie (2014) aptly pointed out, data are presented as objective and the algorithms that process them are portrayed as above suspicion and incapable of adopting ideological positions, thus becoming a powerful weapon for overcoming controversies. [...]. However, debates and research are advancing that consider not only the biases and prejudices embedded in data structures but also in the codes and algorithms that carry the outlook of their developers and funders (SILVEIRA, 2016, pp. 159–160).

Once created, data can be extracted within a process known as data colonialism, in a way that

is not very transparent to their owners, such that people's habits become a commercializable resource, as they are essential in the relationship between corporations and platforms and can also be used for political competition (SILVEIRA, 2016), as well as for biometric use through facial recognition technologies. Thus, in this combination of state–corporate actors, coloniality ends up being updated, with new instruments but still perpetuating the same destructive and dehumanizing designs inherent to capitalism (GERVASONI & DIAS, 2023, p. 155).

In this sense, it is possible to consider how the massive use of data has ended up enabling a government of conduct, managed in a complex and targeted way by platforms and their algorithms, in a progressive accumulation of information that will be useful to secure positions of strategic advantage.

Silveira (2016) found that digital platforms increasingly began to create datafication projects aimed at converting any digitizable element into a process of capital reproduction. According to the author, this happens because the relations between producers and consumers of a given product, or even between providers and users of certain services, are gradually instrumentalized by platforms managed through algorithms that allow these relations to be consolidated ever more quickly and in line with advertising interests: "Simultaneously, these algorithmic managers extract data from markets and store them with the aim of expanding the knowledge and control of their platforms" (SILVEIRA, 2016, p. 168).

Although commonly associated with Information and Communication Technology (ICT), the concept of the algorithm dates back to the beginnings of mathematics and exists independently of today's digitalization. Since the time of Egyptian civilization, algorithms were used to create formulas that solved everyday challenges, such as predicting the floods of the Nile River, representing a specific sequence of written steps to solve a particular problem. Today, they remain an essential element in the entire computing process, aimed at mediating human activities and reducing the number of repetitive procedures (ROCHA, PORTO & ABAURRE, 2020).

Algorithms play a fundamental role in the operation of artificial intelligences, being essential for the execution of tasks. Although there is no universally accepted concept of Artificial Intelligence (AI), it is commonly understood as the capacity of machines to reproduce behaviors typical of human beings, grounded in the manipulation of algorithms. Currently, AI is applied in three main areas: machine learning, deep learning, and natural language processing (BON, SCHONS & LOPES-FLOIS, 2023, p. 227).

According to Costa (2021), the use of machine learning programs and their more advanced variant, known as deep learning, has given machines a remarkable ability to evolve through experience, as well as to make decisions autonomously. This means that, after the development of the algorithm, many subsequent steps can be carried out without the need for human intervention.

With regard to facial recognition, understood as the capacity to identify individuals by means of characteristics determined by their faces, several authors adopt an optimistic approach to its use for purposes of social control, arguing that the identification of people through the use of such techniques may become a safe and minimally invasive alternative, as recognized by Pablo Nunes et al. (2016).

In this case, the argument in favor of the use of this type of strategy in the field of Public Security, in general, presupposes the development of technologies driven by facial recognition in association with existing video surveillance systems, "which could operate as effective tools in combating crime, especially in locating and identifying fugitives, criminals, missing persons, etc." (Nunes et al., 2016, p. 114).

However, in promising to fight national crime with a supposedly efficient and objective technological resource, there is a serious risk of adopting it without the necessary critical analysis, disregarding those risks that disproportionately affect certain social groups.

**3. Facial Recognition Technology**

Facial recognition "is a biometric identification technique, like fingerprinting, in which software maps facial lines and, by means of algorithms, compares them to a digital image, recognizing (or denying) the person's identity" (MAGNO & BEZERRA, 2020, p. 46). Its concept was first developed in the 1960s, when Woodrow Wilson Bledsoe, Helen Chan Wolf, and Charles Bisson

created the first semi-automatic recognition system (TRASLAVIÑA, 2015, p. 55).

Over the course of the 1970s, 1980s, and 1990s, other techniques were added and improved. However, only in 2001, during a Super Bowl game of the National Football League (NFL), were images of fans' faces captured by means of surveillance cameras for later comparison with a database, demonstrating the potential of this technology (NUNES et al., 2016, p. 117).

It is not by chance that, in 2019, in Hong Kong, an autonomous territory of China, participants in protests against that country's government destroyed video surveillance cameras in public areas. This attitude should not be treated as mere vandalism, but as a form of defense against future individual repression, by avoiding being recognized (ELESBÃO, SANTOS & MEDINA, 2020, p. 247).

As for its functioning, facial verification is carried out basically in two stages: the moment of detecting the face itself and the moment of its verification, using, simultaneously or separately, two approaches: the global approach, in which an image of thousands of pixels is reduced to a set of numbers, known as Holistic Methods; and the local approach, in which the "local" characteristics of the face are extracted, such as eyes, mouth, and eyebrows, using their positions on the face, known as Structural or Local Methods (NUNES et al., 2016, pp. 119–120).

According to research presented in the Aguará Project (Otegui et al., 2006, p. 80), the algorithm must take into account aspects that complicate the recognition process, such as: "the person's emotional state, due to the recognition of expressions (sad, happy, angry, etc.); location of relevant features found in the eyes, mouth, eyebrows, chin, ears, etc.; face size; presence of glasses, beard, caps, etc.; facial expression; lighting problems; image conditions; unknown number of faces in the image, etc."

That said, we can affirm that this technology has gradually developed over recent decades, moving toward an increasingly broad and complex mode of operation as it assimilates new variables. This is because the possibility of collecting more data and processing them more quickly has allowed significant advances in the accessibility of such mechanisms, making this device increasingly common for purposes of social control, both in the private and in the public sector.

According to Nunes (2019), Brazil officially adopted the use of facial recognition technologies in the area of Public Security only in 2019, after a year of experimentation in some states of the country, worsening mass incarceration mainly as a result of the arrest of young Black people from Brazilian peripheries. In that year, the state of Bahia was the first to adopt this type of technology during Carnival, resulting in the arrest of 74 people.

Although the promises associated with these biometric technologies are tempting, seeing in the use of facial recognition a way to increase the efficiency of police work, great caution is required in a country where the police are questioned for their racist bias. There is a constant risk that the dangers of racial prejudice in these technologies will be minimized, insofar as it is assumed that the algorithm is "neutral" in the task of selecting potential suspects (NUNES, 2019).

It must be explained that the parts of the body most used in biometrics, whether fingerprints or the face itself, will never be fully analyzed, since only some of their points are selected in order to calculate the probability that they are features of the person registered in the database. If similarity levels below the established 90% are set, this may lead to a large number of identifications, generating a significant quantity of false positives. Conversely, "if the level of similarity required by the algorithm is 99.9%, for example, the likelihood that the system will issue alerts will be very low" (NUNES, 2019, p. 68). It is not difficult to conclude that such false positives would inevitably translate into public humiliation, arbitrary arrests, and clear violations of fundamental rights and guarantees.

The Rede de Observatórios da Segurança has monitored cases of arrests and police stops resulting from the use of facial recognition, as well as projects to implement this form of surveillance and control in the country. According to its reports, it was found that, from March to October 2019, cases of arrests resulting from the use of facial recognition technology were monitored in four Brazilian states: Paraíba, Bahia, Rio de Janeiro, and Santa Catarina. "Of the cases monitored by the Rede, Bahia accounted for 51.7% of arrests, followed by Rio de Janeiro with 37.1%, Santa Catarina with 7.3%, and Paraíba with 3.3%" (NUNES, 2019, p. 69).

Although in some monitored cases, it was difficult to find precise information about the profile of the people arrested or stopped by the police, taken as a whole, that is, for all 66 identified cases, there was information on sex, age, race/color, and motivation. Among those investigated, it was possible to verify that 87.9% of the suspects were men and 12.1% women; the average age of the group under scrutiny was 35 years; and 90.5% of the people were Black and 9.5% were white. With regard to motivation, the highest numbers were for the crimes of drug trafficking and robbery, each with 24.1% (NUNES, 2019, p. 69).

In this case, it seems necessary to emphasize that, while countries such as Belgium have begun to adopt a ban on facial recognition technology, as Nunes (2019) highlights, in Brazil this approach appears to be moving in the opposite direction, insofar as the number of enthusiasts is increasing. States such as Minas Gerais, Espírito Santo, Pará, and the Federal District have already declared that they are in the process of contracting or implementing this type of technology in the field of Public Security. The same seems to be occurring in all the states of the Northeast, driven by projects of Chinese companies that are being implemented in this region.

The federal government has contributed significantly to the expansion of this type of technology, as can be seen in Ordinance No. 793 of 24 October 2019, which regulates the use of money from the National Public Security Fund for the "promotion of the implementation of video surveillance systems with facial recognition solutions, Optical Character Recognition – OCR, the use of artificial intelligence, or others" (NUNES, 2019, p. 69).

Thus, it becomes troubling to consider that, in a country where the basic principles of data transparency in the field of public security have historically been disrespected, and where current projects fully disregard the Lei Geral de Proteção de Dados Pessoais (LGPD – General Data Protection Law), there seems to be no concern with developing accountability mechanisms for facial recognition technologies, nor protocols aimed at ensuring the security of the data collected.

This concern grows when we see that projects involving the use of facial recognition by police forces in some Brazilian states operate in line with the creation of the National Multibiometric and Fingerprint Database proposed by the then Minister of Justice, Sérgio Moro. This database was presented as an important and necessary form of modernization of police practice; however, according to specialists, it has been regarded as a step backwards in terms of efficiency, transparency, and the protection of the population's personal data (NUNES, 2019).

**4. Algorithmic Racial Discrimination**

Silva argues that algorithms and artificial intelligence, increasingly present in our daily lives through the use of biometrics to unlock smartphones and facial recognition to access certain spaces, can raise various concerns related to prejudice associated with race, gender, social class, location, and neurodivergence. According to the author, such technologies do not operate in a neutral manner, since they entail a process of racialization and algorithmic oppression that results in discriminatory experiences. Thus, programming can be responsible for perpetuating various prejudices and errors (SILVA, 2020).

Although they were conceived with the aim of impartiality, seeking to overcome the limits of human rationality, algorithms absorb the choices, inclinations, and prejudices of their programmers, even if unintentionally, which justifies concern with racial algorithmic discrimination (FRAZÃO, 2021).

In analyzing growing racial discrimination on the World Wide Web, Cardozo (2022) found that Black women are commonly victims of hate speech on social media. According to the author, racial algorithmic discrimination has emerged contemporaneously as the main challenge in confronting this issue, which is consolidated in the infrastructure and interface of digital technologies, in image-processing resources, in content recommendation, among other aspects that highlight the need to discuss the "whiteness" expressed on the internet.

Scholars point to a significant example of algorithmic discrimination in the operation of COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), an artificial intelligence system used by U.S. courts to estimate a defendant's likelihood of recidivism. The criteria assessed—such as place of residence, history of involvement with drugs, family background, and school performance—resulted in a classification of

"high risk" of recidivism for Black people significantly more frequently and in greater numbers than for white individuals. This scenario exposes the prejudices embedded in the algorithms, stemming from the parameters defined by programmers (SOARES et al., 2022).

According to Taute (2020), an algorithm is like a recipe, an instruction that the machine follows and, in order to execute it, it must query a database. If this database contains racial prejudices, many people will be included in and excluded from the process, accentuating disparities. In this regard, it is worth recalling the research carried out by Joy Buolamwini, a 30-year-old Black woman and researcher at the Media Lab of the Massachusetts Institute of Technology (MIT).

When developing a prototype of a smart mirror capable of recognizing the face of the person in front of it and projecting features of inspiring figures such as Serena Williams, Joy Buolamwini attached a camera to capture the image of her face and transmit it to her computer which, by means of a facial recognition algorithm, would identify the person and link them to personalized information. However, when she began the experiment, the prototype did not detect her face, only succeeding after she used a white mask, showing that the color of her skin prevented the system from working (NUNES, 2021).

Another example that should be mentioned concerns the choice of who would succeed actor Daniel Craig in the role of James Bond. At first, it was reported that the selection for this role would be made using Artificial Intelligence and that it would point to a Black woman. However, the final selection contradicted what had been reported in 2019, resulting in the hiring of actor Henry Cavill for the role, another white man. What happened was that the AI had been trained on data from the film industry produced in the Global North, where Black people are minimally represented among protagonists (BEIGUELMAN, 2021).

A study by Tarcízio Silva et al. (2020, p. 30) on labeling failures in Google Cloud Vision, focusing on images of Black women, "showed that the photos recurrently received the label 'wig' whenever their hair was prominent," revealing that the database lacked labels for curly or non-straight hair— a culturally rooted limitation on the part of those responsible for the algorithms. Thus, according to the authors, "this universe of social relations at the base of AIs shows that the supposed misogyny and racism of the algorithms have unmistakable human and political dimensions" (SILVA et al., 2020, p. 33).

As indicated by the National Institute of Standards and Technology (NIST) of the United States government, the algorithms normally used are much less accurate in the facial identification of African American and Asian individuals than in that of white people. In this context, Black women had higher probabilities of being misidentified, thereby perpetuating racist practices under a technological guise (NUNES, 2019).

The work of Christina Baker (2005) also stands out for recognizing that media stereotypes attributed to white and Black women differ substantially, insofar as the images most commonly associated with Black women do not reflect the same affability and submissiveness as those associated with white women, who are not recurrently portrayed, from an imagetic standpoint, as sexually aggressive and animalistic, threatening men in their masculinity.

Amaral, Martins, and Elesbão (2021) mention research carried out on the content of image banks regarding racial patterns of families on digital platforms, which predominantly maintain a profile of white people.

In the Getty Images database, of the 300 images returned for the term "family," 107 were of entirely white families, 24 of entirely Black families, and 22 of interracial families and other races/ethnicities. In the Shutterstock image bank, of the 319 images returned, 214 were of entirely white families, 20 of entirely Black families, and 20 of interracial families and other races/ethnicities. Finally, in the Stock Photos image bank, of the 301 images returned for the term "family," 213 were of entirely white families, 14 of entirely Black families, and 15 of interracial families and other races/ethnicities (AMARAL, MARTINS & ELESBÃO, 2021, p. 07).

Thus, discussion of this topic is urgent, since racial inequalities are potentially reflected through algorithms as an extension of the programmer's opinions, values, and social standards, as exemplified by the way images are made available to users on the internet (AMARAL, MARTINS & ELESBÃO, 2021, p. 05).

## 5. Facial Recognition and Racism in Public Security

With regard to the application of facial recognition in the area of Public Security, its history goes back to the terrorist attack that took place in the United States on 11 September 2001. It was from this event that the use of this technology for crime prevention in various countries was driven forward, becoming a true milestone (NUNES et al., 2016, pp. 123–124).

Since then, facial recognition has increasingly been treated as a promising technology in the field of Public Security. Through advanced algorithms, it is said to be capable of identifying individuals on the basis of unique characteristics of their faces, comparing them with databases of previously registered images. Thus, according to its enthusiasts, this would make it possible to quickly identify suspects, people wanted by the courts, and individuals involved in criminal activities (MELO & SERRA, 2022).

According to Rola (2022), the most impactful biometric technology today is facial recognition. Unlike other biometric forms, such as fingerprints, iris or retina scans, and voice, facial recognition is fast and discreet in terms of data collection, since it generally does not require the cooperation of the person being identified. In contrast to other biometric modalities that require the individual's consent, facial recognition emerges as an investigative tool.

However, as already noted, facial recognition can be influenced by environmental factors such as lighting, angle of capture, facial expression, pose, makeup, and accessories like glasses and hats. Thus, possible mistakes in facial recognition highlight a very dangerous weakness in the realm of security. In other words, these errors underscore the importance of improving facial recognition algorithms, should they in fact be implemented, through advances in artificial intelligence so as to make them more robust and accurate, meeting police demands without resulting in reckless criminalization.

Accordingly, continuous investment in research and development can help reduce error rates and increase the reliability of facial recognition as a security tool. Moreover, it is essential to ensure that ethics and data protection are taken into account in the implementation of these technologies, seeking a balance between security and individuals' privacy (ROLA, 2022).

According to Francisco, Hurel, and Rielli (2020, p. 17), in light of the procedural flaws mentioned above, many oppose the use of facial recognition technology by Public Security agencies, because scientific research has shown high error margins when analyzing the faces of women and Black people. Despite the slow development of regulatory control, there has been an increase in its incidence in Brazil, given that the use of facial recognition by police forces, municipal guards, and other Public Security bodies has occurred in at least 30 cities across 16 states of the country up to 2022.

Monitoring carried out by Intervozes revealed that, among the 26 mayors of state capitals sworn in in January 2021, 17 presented proposals concerning the use of Information and Communication Technologies in the field of Public Security, including the implementation of facial recognition technology (GOMES & MOURA, 2022).

In turn, several relevant problems in its use have already been reported, such as the one that occurred during a period of testing of facial recognition technology on Copacabana beach. On the second day of the experiment, a woman was recognized as being Maria Lêda Félix da Silva, convicted of homicide and wanted by the police, for which reason she was arrested and taken to the police station. After all the embarrassment inherent in this type of procedure, the woman was released when her family members brought her documents proving that she was not the person flagged by the algorithm.

The case illustrates yet another example in a series of errors produced by these technologies, but with an aggravating factor: Maria Lêda, the "wanted woman," had already been serving her sentence in a prison for four years. In this case, not only did the algorithms fail, but so did the police, who used an outdated database (NUNES, 2021).

The issue takes on particular significance when there is a widespread view that technology, along with science, is objective, which makes it harder to understand. This supposed objectivity is contestable, since those who fund and manage these systems play an important role in the outcome. This is an area undergoing rapid growth, without an adequate overall political and ethical debate, thus producing what we may call algorithmic racism, understood as "the way

in which the current arrangement of technologies and sociotechnical imaginaries in a world shaped by white supremacy reinforces the racialized ordering of knowledge, resources, space, and violence to the detriment of non-white groups" (SILVA, 2020; SILVEIRA, 2022).

It is therefore worth recalling the case of the city of Oakland, in the U.S. state of California, whose City Council prohibited, in 2019, the use of facial recognition by public agencies, including the police itself, due to the risks it poses to city residents, with the possibility of misidentifying individuals and the subsequent misuse of force, wrongful arrests, and persecution of minorities (MAGNO & BEZERRA, 2020, p. 51).

Recognizing that the risks and harms associated with the use of facial recognition technology outweigh its possible benefits, the city of San Francisco became the first U.S. municipality to ban its use by Public Security agents, in May 2019. According to the arguments presented by legislators, facial recognition allows for the exacerbation of social injustice and threatens to heighten existing risks.

In this context, advocates of banning the use of this type of technology by Public Security forces point out that the algorithmic models used to train facial recognition technology are developed mostly by white men, which significantly increases the likelihood of misidentifying Black people. Furthermore, in order to train this type of technology, the system must scan the faces of those who circulate in public spaces, even if these people are unaware of it, expanding a state of constant surveillance (GOMES & MOURA, 2022).

Thus, although it deals with highly complex concerns that have sparked ethical and political debates, this is still a developing area without the necessary critical approach. The risks of impacting fundamental rights guaranteed by the Constitution of the Brazilian Republic are considerable, especially if we consider that injustices in the field of public security directly entail vexatious public exposure of one's image, restrictions on freedom, and, eventually, even death.

**6. Final Considerations**

This article has presented a literature review on the use of facial recognition technology in the field of Public Security, associating it with the perpetuation of discriminatory practices through so-called algorithmic racism. With this aim, it sought to provide basic notions of platformization, the datafication of life, data colonialism, surveillance and platform capitalism, algorithmic racial discrimination, and so on, as well as to raise questions about its use by Brazilian Public Security agencies.

In this regard, it was possible to observe that algorithms are not impartial by nature and can, in fact, incorporate the biases of their creators or of the data sets used during their training. At this stage, the performance of the algorithm may present a biased tendency, since the prejudices present in the training data will be reflected in its decisions and actions.

This issue is particularly important when it comes to applications that directly affect people's lives, especially through the use of decision-making systems based on this type of biometric technology. If the data used to train these algorithms contain prejudices—whether of gender, race, social class, or any other kind—it is likely that the system will reproduce and even amplify these patterns in its decisions.

In this way, power is exercised subtly: the capacity to kill or to let live is exercised without being noticed, through a technology that does not operate by neutral use of its data. It is therefore necessary to understand and limit its application, under penalty of subjecting part of society to a new tool of racial discrimination, with a broader dissemination of oppressive practices.

Understanding the balance between the right to public security and the right to due process of law is absolutely necessary, given the imperative of guaranteeing the constitutional right not to be subjected to unjustified unequal treatment. In a context in which the State provides the public service of protecting the collectivity, utmost caution is required in light of the history of countless acts of violence and racial discrimination in a country marked by a slaveholding legacy.

**References**

AMARAL, Augusto Jobim do; MARTINS, Fernanda; ELESBÃO, Ana Clara. (2021, out./dez). Racismo algorítmico: uma análise da branquitude nos bancos de imagens digitais. *Revista Pensar, Fortaleza*, *26*(4), p. 1-9, Disponível em: https://ojs.unifor.br/rpen/article/view/11806 Acesso em: 23 jul. 2024.

BAKER, Christina N. (2005, jan.). Images of women's sexuality in advertisements: a content analysis of black and white oriented women's and men's magazines. Sex Roles, 52(1/2), p. 13-27, Disponível em: https://link.springer.com/article/10.1007/s11199-005-1190-y Acesso em: 24 jul. 2024.

BARROS, Isabel Maria Pereira Paes de; SILVA, Isabel Inês Bernardino de Souza. (2020, jul.). Utilização do reconhecimento facial eletrônico por empresas para identificação de suspeitos: segurança ou violação do estado democrático de direito? *Revista Transgressões: Ciências Criminais em debate*, *8*(1), Disponível em: https://periodicos.ufrn.br/transgressoes/article/view/19909 Acesso em: 23 jul. 2024.

BEIGUELMAN, Giselle. (2021). *Políticas da imagem: vigilância e resistência na dadosfera*. São Paulo: Ubu Editora.

CARDOZO, Glenda Dantas. (2022, dez.). A atuação estratégica de mulheres negras no combate às brechas digitais de gênero e raça. *Internet & Sociedade*, *3*(2), p. 5-19.

COSTA, Diego Carneiro. (2021). A discriminação algorítmica e as novas perspectivas sobre o tratamento de dados pessoais sensíveis. In: REQUIÃO, Maurício (Org.). *Proteção de dados pessoais: novas perspectivas*. Salvador: Editora da Universidade Federal da Bahia.

DA EMPOLI, Giuliano. (2019). *Os engenheiros do caos*. Rio de Janeiro: Vestígio.

ELESBÃO, Ana Clara Santos; SANTOS, Jádia Larissa Timm dos; MEDINA, Roberta da Silva. (2020). Quando as máscaras (do reconhecimento facial) caírem, será um grande carnaval. In: SABARIEGO, Jesús; AMARAL, Augusto Jobim do; SALLES, Eduardo Baldissera Carvalho (Orgs.). *Algoritarismo*. 1. ed. São Paulo. Editora Tirant lo Blanch, p. 247-259.

FOUCAULT, Michel. (1999). *Em defesa da sociedade*. São Paulo: Martins Fontes.

FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie; RIELLI, Mariana Marques. (2020, jun.). Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. Instituto Igarapé + Data Privacy Brasil Research, Disponível em: 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 Acesso em: 13 out. 2023.

FRAZÃO, Ana. (2021, ago.). Discriminação algorítmica: por que os algoritmos preocupam quando acertam e quando erram? Jota, Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-por-que-algoritmos-preocupam-quando-acertam-e-erram-04082021 Acesso em: 07 set. 2023.

GARRET, Filipi. ROBOS (BOTS). Disponível em: https://www.techtudo.com.br/noticias/2018/07/o-que-e-bot-conheca-os-robos-que-estao-dominando-a-internet.ghtml. Acesso em: 21 jan. 2024.

GERVASONI, Tássia A.; DIAS, Felipe V. (2023, set-dez). Violações de Direitos Humanos pelas Big Techs: contribuições do pensamento decolonial e de uma leitura criminológica do dano social. *Revista de Garantias e Direitos Fundamentais*, Vitória, *24*(03), p. 137-173.

GOMES, Sheley; MOURA, Iara. (2022). De Oakland ao Jacarezinho: os sistemas de reconhecimento facial precisam ser banidos. Revista Capital. Disponível em: https://www.cartacapital.com.br/blogs/de-oakland-ao-jacarezinho-os-sistemas-de-reconhecimento-facial-precisam-ser-banidos Acesso em: 21 jan. 2024.

LEMOS. André. (2021, maio-ago.). Dataficação da vida. Revista Civitas. Disponível em: http://dx.doi.org/10.15448/1984-7289.2021.2.39638 Acesso em: 09 jan. 2024.

MAGNO, Madja Elayne da Silva Penha; BEZERRA, Josenildo Soares. (2020, ago./dez.). Vigilância negra: o dispositivo de reconhecimento facial e disciplinaridade dos corpos. *Revista Novos Olhares*, *09*(2). Disponível em: https://www.revistas.usp.br/novosolhares/article/view/165698 . Acesso em: 30 jan. 2024.

MELO, Paulo Victor; SERRA, Paulo. (2022). Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematizações. *Comunicação e Sociedade*, *42*, p. 205-220. Disponível em: https://journals.openedition.org/cs/8111 Acesso em: 23 jul. 2024.

NUNES, Fernanda Todesco *et al*. (2016). Um estudo sobre técnicas de biometria baseadas

em padrões faciais e sua utilização na Segurança Pública. *In*: SPANHOL, Fernando J.; LUNARDI, Giovani M.; SOUZA, Márcio Vieira de (org.) Tecnologias da Informação e Comunicação na Segurança Pública e Direitos Humanos. Coleção Mídia, Educação, Inovação e Conhecimento, *2*, Editora Edgard Blücher Ltda., p. 113-132.

NOBLE, Safiya. (2021). Algoritmos da opressão. Santo André: Rua do Sabão.

NUNES, Pablo. (2019). Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. *In*: REDE de Observatório de Segurança. *Retratos da violência: cinco meses de monitoramento, análise e descobertas*. Centro de Estudos em Segurança e Cidadania.

NUNES, Pablo. (2021, jan. 02). O algoritmo e racismo nosso de cada dia. *Revista Piauí*, Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia/ Acesso em: 23 jul. 2024.

OTEGUI, C. A. et al. (2006). *Proyecto Aguará – Reconocimiento de Caras*. Montevideo: Facultad de Ingeniería Universidad de la República.

OTEGUI, C. A. et al. (2021, jan. 02). O algoritmo e racismo nosso de cada dia. Folha de São Paulo [on line], São Paulo, Questões de vida digital. Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia Acesso em: 07 jan. 2024.

POELL, Thomas; NIEBORG, David; DIJCK, José van. Plataformização. (2020, jan. abr.). Plataformização. *Fronteiras - estudos midiáticos*, *22*(1). Disponível em: https://revistas.unisinos.br/index.php/fronteiras/article/view/fem.2020.221.01 Acesso em: 23 jul. 2024.

ROCHA, Jannotti da; PORTO, Lorena Vasconcelos; ABAURRE, Helena Emerick. (2020). Discriminação algorítmica no trabalho digital. *Revista de Direitos Humanos e Desenvolvimento Social*, *1*, e 205201. Disponível em: https://seer.sis.puc-campinas.edu.br/direitoshumanos/article/view/5201/3164. Acesso em: 07 dez. 2023.

ROLA, Eulálio do Carmo da Silva. (2022). Os principais contributos da inteligência artificial para o processamento de imagens digitais a utilizar na Segurança Pública. 2022, 146 f. Dissertação (Mestrado em Segurança e Justiça) – Universidade Lusíada, Lisboa.

ROSA, Pablo Ornelas; AMARAL, Augusto Jobim do; NEMER, David Baião. (2023). Datapolítica, governamentalidade algorítmica e a virada digital: uma genealogia da modulação comportamental através das plataformas digitais. *Revista Eletrônica do Curso de Direito da UFSM*, *18*(03). Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/85510 Acesso em: 23 jul. 2024.

ROUVROY, Antoinette; BERNS, Thomas. (2015). Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação pela relação? *Revista Eco Pós. Rio de Janeiro*, *18*(2), p. 36-56. Disponível em: https://doi.org/10.29146/eco-pos.v18i2.2662 Acesso em: 18 nov. 2023.

SILVA, Tarcízio. (2020). Visão computacional e racismo algorítmico: branquitude e opacidade no aprendizado de máquina. *Revista ABPN*, *12*, p. 428-448. DOI: 10.31418/2177-2770.2020. Disponível em: https://abpnrevista.org.br/site/article/view/744/774 Acesso em: 07 set. 2023

SILVEIRA, Sérgio Amadeu. (2016). Governo dos algoritmos. *Revista de Políticas Públicas*, *02*(01), p. 267-281. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4452794/mod_resource/content/1/S%C3%A9rgio%20Amadeu%20SILVEIRA%20%20Governo%20dos%20Algoritmos.pdf Acesso em: 26 jan. 2024.

SILVEIRA, Sérgio Amadeu. (2020). Sistemas algorítmicos, subordinação e colonialismo de de dados. In: SABARIEGO, Jesús; AMARAL, Augusto Jobim do; SALLES, Eduardo Baldissera Carvalho (organizadores). *Algoritarismo*. 1. ed. São Paulo: Editora Tirant lo Blanch, p. 158-1709.

SOARES, Marcelo Negri et al. (2022). Inteligência artificial e discriminação: um panorama sobre a antagonização entre exclusão e o Estado Democrático de Direito Brasileiro à luz dos direitos da personalidade. *Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE)*, *10*(2), p.

567-597. Disponível em: https://portal.unifafibe.com.br/revista/index.php/direitos-sociais-politicas-pub/article/view/1311 Acesso em: 07 jan. 2024.

SRNICEK, Nick. (2018). *Capitalismo de plataforma*. Buenos Aires: Ed. Caja Negra.

SILVA, Tarcízio et al. (2020, jun. 5). Apis de visão computacional: Investigando mediações algorítmicas a partir de estudo de bancos de imagens. *Logos,* 1(27), pp. 25-54. Disponível em: https://www.e-publicacoes.uerj.br/logos/article/view/51523/33928 *Acesso em: 26 jul. 2024.*

TAUTE, Fabian. (2020 fev. 7). Reconhecimento Facial e suas controvérsias: O reconhecimento facial não só traz a possibilidade de instaurar uma vigilância em massa, mas também contém uma tendência preconceituosa contra certos grupos de nossas sociedades – com as mulheres negras sendo as mais afetadas. Heinrich Böll Stiftung, Rio de Janeiro. Disponível em: https://br.boell.org/pt-br/2020/02/05/reconhecimento-facial-e-suas-controversias Acesso em: 07 set. 2023.

TRASLAVIÑA, C. M. G. (2007). Introducción a la biometría. Disponível em: https://www.academia.edu/9374109/Introducci%C3%B3n_a_la_biometr%C3%ADa Acesso em: 17 nov. 2023.

VAIDHYANATHAN, Siva. (2011). A Googlelização de tudo. São Paulo: Cultrix.

ZUBOFF, Shoshana. (2020). *A era do capitalismo de vigilância: Luta por futuro humano na nova fronteira de poder.* Rio de Janeiro: Ed. Intrínseca.