DOI 10.20396/tematicas.v33i65.19902

TECNOLOGIAS DE CONTROLE E A PRODUÇÃO DA HUMANIDADE: INTELIGÊNCIA ARTIFICIAL, RACISMO E SEGURANÇA PÚBLICA NO BRASIL

Kaue Felipe Nogarotto Crima Bellini[1]
Fagner Carniel[2]

RESUMO: Este artigo analisa o uso de tecnologias de Inteligência Artificial (IA) nas políticas públicas de segurança no Brasil, discutindo como tais ferramentas, ao serem mobilizadas pelo Estado, produzem e reforçam uma dada concepção de humanidade. A partir de uma abordagem crítica e interseccional, e com base na análise de casos concretos, o texto argumenta que essas tecnologias não operam apenas como instrumentos de controle, mas corporificam valores históricos, sociais e culturais que se traduzem em práticas de vigilância seletiva. Assim, o uso da IA na segurança pública é entendido não apenas como uma questão técnica, mas como expressão de um projeto político que define quem importa, quem deve ser protegido e quem pode ser eliminado.

PALAVRAS-CHAVE: Inteligência artificial. Colonialismo. Racismo. Tecno-diversidade.

TECHNOLOGIES OF CONTROL AND THE PRODUCTION OF HUMANITY: ARTIFICIAL INTELLIGENCE, RACISM, AND PUBLIC SECURITY IN BRAZIL

[1] PhD candidate and lecturer in Social Anthropology at the University of Basel. Email: k.crimabellini@unibas.ch. Orcid: https://orcid.org/0000-0002-5834-7424.
[2] Professor at the Department of Social Sciences at the State University of Maringá. Email: fagnercarniel@yahoo.com.br. Orcid: https://orcid.org/0000-0002-7453-1993

ABSTRACT: This article examines the use of Artificial Intelligence (AI) technologies in public security policies in Brazil, discussing how such tools, when mobilized by the state, produce and reinforce a particular conception of humanity. Adopting a critical and intersectional approach grounded in the analysis of concrete cases, the text argues that these technologies function not merely as instruments of control but also embody historical, social, and cultural values that materialize in practices of selective surveillance. In this sense, the use of AI in public security is understood not simply as a technical matter, but as the expression of a political project- one that determines who matters, who deserves protection, and who may be subjected to elimination.

KEYWORDS: Artificial intelligence. Colonialism. Racism. Technodiversity.

TECNOLOGÍAS DE CONTROL Y LA PRODUCCIÓN DE LA HUMANIDAD: INTELIGENCIA ARTIFICIAL, RACISMO Y SEGURIDAD PÚBLICA EN BRASIL

RESUMEN: Este artículo analiza el uso de las tecnologías de Inteligencia Artificial (IA) en las políticas públicas de seguridad en Brasil, discutiendo cómo estas herramientas, cuando son movilizadas por el Estado, producen y refuerzan una determinada concepción de humanidad. Desde un enfoque crítico e interseccional, y a partir del análisis de casos concretos, el texto argumenta que estas tecnologías no sólo operan como instrumentos de control, sino que encarnan valores históricos, sociales y culturales que se traducen en prácticas de vigilancia selectiva. Así, el uso de la IA en la seguridad pública se entiende no sólo como una cuestión técnica, sino como expresión de un proyecto político que define quién importa, quién debe ser protegido y quién puede ser eliminado.

PALABRAS CLAVE: Inteligencia artificial. Colonialismo. Racismo. Tecno-diversidad.

INTRODUCTION

This paper explores how artificial intelligence (AI) - particularly facial recognition technologies deployed within Brazil's public security policies - operates as a tool of racial subjugation, producing new forms of colonial control. Drawing from documented cases of misidentification

disproportionately affecting Black individuals, we argue that these systems not only reflect but actively reinforce structural racism embedded in the state's surveillance apparatus. Far from being neutral governance instruments, AI technologies embody and reproduce a hegemonic conception of humanity rooted in Western epistemologies of difference, exclusion, and hierarchy.

Our analysis adopts a critical and intersectional framework to interrogate the values inscribed in designing and implementing AI systems. These technologies, we contend, materialize a selective politics of visibility: deciding whose lives are rendered intelligible, whose presence is marked as threatening, and whose bodies are rendered disposable. In this context, AI does not merely automate tasks, it automates discrimination, producing what Achille Mbembe (2006) calls "necropolitical" effects within the logic of public safety.

We further argue that the current deployment of AI in Brazil cannot be disentangled from broader socio-political dynamics, including urban segregation, neoliberal security agendas, and historical patterns of racialized state violence. The increasing reliance on digital surveillance, framed through campaign slogans such as "smart cities" or "digital fences," reveals a deep fascination with technologies of control that serve to normalize inequality under the guise of innovation and efficiency. According to Luca Belli and Nina da Hora (2023), the integration of artificial intelligence into security policies in Brazil highlights a significant lack of oversight, which exacerbates racial inequalities rather than alleviating violence. The absence of regulation concerning these technologies enables a form of algorithmic governance that disproportionately impacts Black and marginalized communities.

It is crucial to understand facial recognition technologies and other algorithmic security systems as modern expressions of colonial ideologies, rather than as unbiased advancements, ones that impose racialized structures disguised as technological neutrality. This perspective aligns with Aníbal Quijano's (2000) view of colonialism as not concluding with the dissolution of empires, but evolving into coloniality, a pervasive power system that is sustained within contemporary institutions. Coloniality entrenches itself

in hierarchies of race, knowledge, and labor, consistently favoring Western Eurocentric perspectives while systematically undermining others, such as Afro-diasporic and indigenous traditions (CARNIEL *et al.*, 2024). By exposing the technical "errors" and biases in these systems, this paper positions AI as a kind of Trojan horse: a seemingly progressive tool that, in reality, extends and conceals long-standing regimes of racial control. Our aim is not simply to critique AI's failures, but to propose alternative, anti-racist strategies for technological design and data governance that prioritize ethical accountability and epistemic justice. This requires a shift from performative inclusion to a genuine transformation of the logics that govern technological production and deployment.

RACISM IN BRAZILIAN FACIAL RECOGNITION SYSTEMS

The growth of urban violence has troubled the Brazilian population for decades (ZALUAR, 1999). It can be understood as a structural consequence of the current crisis in the criminal justice system and the deepening of historical inequalities that have led to socio-spatial segregation in cities across all regions of the country (MISSE, 2006). Hence, the lack of opportunities for a dignified life for different socially excluded groups is aggravating (ADORNO, 2002). The problem of urban violence, however, does not affect all people equally. In 2021, for example, there were more than 65,000 homicides that victimized mainly the Black and young population (CERQUEIRA *et al.*, 2021). Given this scenario, there is no shortage of political promises to solve the issue and make cities fairer and safer. The use of new surveillance technologies appears to be a prominent feature in the public security management of various municipalities.

By analyzing the government programs of the mayors who took office in the 26 Brazilian capitals in 2021, Paulo Victor Melo and Paulo Serra (2021) found that digital surveillance technologies have acquired enormous popularity in campaign proposals for public safety areas. According to the study, among the recommendations that were successful in the last electoral campaign are installing monitoring cameras in public spaces, acquiring facial recognition systems, and using drones to optimize

costs, to provide more intelligent mechanisms to combat crime. All this technological paraphernalia was accompanied by political slogans such as "digital wall," "digital fence," or "more security," denoting the fascination that surveillance, control, and segregation techniques exert over the modern social imaginary. In addition, a political litany is often sponsored by those proposing neoliberal models of "smart cities" that reassemble old disciplinary practices of surveillance, normalization, and punishment through new predatory digital modeling (MOROZOV & BRIA, 2018).

Michel Foucault (2014) argued that the panopticon is not just a physical structure but a model for a type of power that operates not through explicit commands and punishment but through subtle, unseen surveillance and control. He saw the panopticon as a metaphor for modern society, which is increasingly subject to surveillance and control through institutions such as prisons, schools, and hospitals. According to Foucault, the panopticon is an example of a "disciplinary society," where individuals are trained to internalize rules and regulations, and their behavior is monitored and regulated rather than controlled through explicit coercion.

A study conducted by the "O Panóptico" project, which monitors facial recognition practices in Brazil, reveals that in 2019, during a police operation at the Maracanã Stadium in Rio de Janeiro, seven out of 11 cases of people arrested using the technology were erroneous. In other words, the system failed in 63% of the cases above (ALMA PRETA, 2022). Furthermore, during the period from 2012 to 2020, 73 mistakes in identification were made, of which 80% (58) were Black and men of color. Of these 58 men, 86% (50) were held in custody and imprisoned for three days to one year (VALENTE, 2020; ROSA, 2022).

This situation is alarming. This type of "algorithmic racism," as Tarcízio Silva (2022) defines it, evokes echoes of colonial-modern histories of genocide, racial selectivity of the criminal system, and hygienist policies undertaken against the black Brazilian population. Moreover, it reproduces the long duration of systematic practices of violence, exploitation, and social debasement, whose origins and responsibilities the ruling elites have always strived to conceal in the country (SCHWARCZ, 2001). In other words, it is about what Cida Bento (2022) has already called a tacit and

narcissistic pact of Brazilian whiteness that aims at maintaining its ethnic-racial privileges and blaming all people who occupy inferior positions in the social hierarchy of color for their social condition.

This dynamic is evident in the case of a woman who was wrongfully arrested in Copacabana, highlighting how facial recognition technologies disproportionately expose Black and marginalized individuals to state violence. This incident was one of the most frequently reported by the Brazilian media. It occurred in July 2019 in the Copacabana neighbourhood of Rio de Janeiro's South Zone. The woman was sitting on a public bench without her identification when she was arrested after being identified by one of the 12 security cameras installed in the area as a suspect in the murder and concealment of a corpse by the Military Police's facial recognition system. Developed by the telecommunications company *Oi in a public-private partnership, the system analyzes the anatomical features of each person's face as filmed, measuring the distance between the eyes, the size of the nose, mouth, and chin, and identifying* the jawline. This information is then fed into an algorithm that creates a biometric identity for each person. Luckily, on that occasion, it was discovered that the author of the crime had already been arrested in 2015, and thus, the woman was released (G1, 2019).

Biometric data from Black and marginalized individuals becomes a point of suspicion rather than a representation of identity, reflecting colonial notions that link Blackness with criminality and guilt. For example, consider the case of José Domingos Leitão, a 52-year-old bricklayer residing in Ilha Grande, Piauí. José had an arrest warrant issued due to a report from the Identification Institute of the Civil Police of the Federal District. The institute linked his photo, which is available in the national registry of individuals, to the image of a suspect robbing a department store in Brasília, over 2,000 km away from where the alleged crime occurred. On the same date, José was at work, building a wall at his neighbor's house. Despite his innocence, he was unable to defend himself and was arrested and flown to the capital, where he was detained for three days at the Specialized Police Department (DPE) (BOMFIM & RIOS, 2021). This case illustrates how biometric surveillance systems rely on biased databases and lack oversight, exacerbating the criminalization of Blackness within society.

Such "misidentifications" appear as tools of a kind of "necropolitics," to mention a notion coined by Achille Mbembe (2006), which mobilizes recent technological mechanisms to determine who can or cannot have their existence respected. In the public life of a country like Brazil, there are substantial social disparities in internet access and literacy, particularly in digital literacy. After all, if we understand that the State has become responsible for the biopolitical administration of the social body in the most diverse contexts and latitudes in the modern West, as Foucault (2019) teaches, the current digitalization policies that have taken shape in the Bolsonaro administration seem to have leveraged unequal and discriminatory ratification of citizenship in Brazil, especially in the area of public safety.

One of the primary concerns with facial recognition systems is that they are frequently trained using biased datasets. These datasets typically consist of images of individuals collected from various sources, such as social media, driver's license databases, and mugshot databases. However, these sources are often biased and do not accurately represent the diversity of the population. For example, mugshot databases tend to be disproportionately composed of people of color, leading to a bias in the training data. As a result, facial recognition systems often need to be more accurate for people of color, leading to higher false positive and negative rates.

In response to the widespread use of digital facial recognition technologies in Brazilian public security, digital rights activists launched the "Get My Face out of Your Sight" campaign in May 2022 to denounce these automated systems' abusive and non-transparent application. According to the movement, the mechanisms for individual identification and digital tracking of people violate fundamental human rights, including the rights to privacy and data protection, freedom of expression and assembly, and equality and non-discrimination (ALMA PRETA, 2022). From this perspective, reclaiming control over technologies, data, and infrastructures becomes an essential ethical and political task for constructing anti-racist, decolonial, democratic, and inclusive societal projects. Quijano (2000) describes decoloniality as a continuous effort to dismantle lingering

colonial frameworks, such as technological governance, within modern institutions. Recognizing the deep-rooted colonial structures is vital for comprehending how security policies are racially constructed today.

Furthermore, studies have shown that facial recognition systems are less accurate for people of color. For example, a survey conducted by Joy Buolamwini and Timnit Gebru (2018, p. 8; 11) at the Massachusetts Institute of Technology found that the leading facial recognition systems had an error rate of 0.8% for white men but over 34% for dark-skinned women. This means that people of color are more likely to be misidentified or wrongly accused by these systems. Another example is a 2019 study published by the National Institute of Standards and Technology (NIST), which found that facial recognition systems trained on predominantly white male faces performed significantly worse on Asian and African American faces compared to white faces (BOUTIN, 2019).

One of the critical causes of racial bias in facial recognition systems is the lack of diversity in the training data used to identify individuals. Most facial recognition systems are trained on large datasets of images. If the dataset is not representative of the racial and ethnic diversity of the population, the system will be less accurate for individuals from underrepresented groups. For example, a study by Buolamwini and Gebru (2018) found that facial recognition systems trained on predominantly white male faces performed significantly worse on Asian and African American faces compared to white faces.

Luca Belli and Nina da Hora (2023) argue that the unchecked advancement and usage of facial recognition technology in Brazil represent not only a technical flaw but also a political failure rooted in the state's racialized structure. Tarcízio Silva (2022) similarly asserts that algorithmic systems in Brazil serve as "instruments of racial surveillance," perpetuating the colonial rationale of policing Black bodies in the digital era. Their insights highlight the critical need to reevaluate technological design and governance through an anti-racist and decolonial perspective. Racism is a form of structural inequality that permeates various aspects of life and social constructions. Data gathering in a scientific field is one of them, not because people corrupt a "pure" method. Instead, both are intersected by

racism. Science has been used in numerous historical contexts to justify, among others, genocides, slavery, misogyny, and homophobia. Scientific methods were applied and developed to corroborate the social narratives. Black bodies were tested for invasive and "unethical" procedures. To affirm all of this is to lay the foundation for the argumentation presented in this paper.

These recurring "errors" are not accidental malfunctions; they represent structural features of a socio-technical apparatus built on racialized data, logics, and histories. Following Achille Mbembe's (2006) notion of necropolitics, such systems determine whose lives are made grievable and whose can be algorithmically erased. Therefore, the evidence that AI systems reinforce or deepen inequalities and racial discrimination in the social body suggests that technological knowledge is not monolithic, neutral, or universal but localized in partial expressions of knowledge and power that participate in weaving our collective lives and humanity. In this case, by questioning the relationships between social inclusion and exclusion promoted through and from digital technologies, we are challenging the very idea of humanity that organizes the bio-sociotechnical and colonial projects of our time—an idea that presents itself in an increasingly claustrophobic manner in the modern West.

FOR A LESS CLAUSTROPHOBIC NOTION OF HUMANITY

The prerogative of a closed, exclusive, and limited humanity ignores and marginalizes people, producing what we call here a claustrophobic humanity. This notion is so exclusionary that it leaves no room for anything other than its very definition, creating a mirrored world where technology is built to control and maintain the mirrors. In this metaphor, there is no space for understanding and acknowledging plurality. We propose the idea of claustrophobic humanity as a critical lens for understanding how algorithmic infrastructures reinforce colonial boundaries regarding who is considered human and who is deemed disposable in digital systems.

Authors such as Yuk Hui (2016) and Anna Tsing (2015) have articulated important philosophical contributions that offer critical

frameworks to rethink technology and its interactions with society, culture, and ecology. Complementing our argument that the problem with facial recognition systems is not just a matter of technical accuracy but also one of ethics and politics. Yuk Hui, for example, interrogates the philosophical foundations of digital objects, which treat digital entities as fixed, controllable, and independent. He points out that technology, in this case facial recognition, is not neutral but reflects and reinforces existing power relations and social hierarchies. In her book, Ann Tsing (2015) examines the lives of mushroom pickers and traders in north-eastern Japan, where the forest industry has declined for decades. Tsing uses the mushroom-picking community as a lens to explore the intersection of capitalism, ecology, and human-nonhuman relationships in the context of environmental destruction and economic decline. The book also explores the concept of "ruins" and the possibility of life and vitality in the aftermath of collapse and destruction. Tsing argues that the mushroom pickers' practices of finding and cultivating mushrooms in ruined landscapes, as well as their reliance on the forest ecosystem to make a living, demonstrate the resilience and creativity of human-nonhuman relationships. Finally, she uses the idea of "the end of the world" to examine the cultural, economic, and ecological factors that shape how people continue to live in the face of destruction, highlighting how the mushroom pickers in Japan are finding new ways to make a living in the front of economic and environmental collapse. The notion of precarity with mushroom pickers draws a powerful metaphor of collaboration, uncertainty, and improvisation in systems of uneven power. In her work, Tsing (2015) has emphasized the importance of considering the broader social and cultural context in which technologies and other systems are deployed. Thus, we must also examine how facial recognition systems are utilized and their impact on various communities.

Yuk Hui critically examines how digital technology shapes our understanding of reality in his book "The Thought of Digital Objects: A Critique of Object-Oriented Ontology (2016). Specifically, he focuses on the concept of the "object" in computer science and the "object-oriented ontology" in philosophy. He argues that these concepts need to

be revised to understand the nature of digital objects. Hui argues that the idea of the "object" in computer science and object-oriented ontology implies that digital objects are self-contained, independent entities that can be fully understood and controlled through computation. However, he contends that this idea needs to be revised because it needs to account for the complexity and interconnectedness of digital objects and their relationship to the world around them. The author also criticizes how object-oriented ontology tends to reify digital objects, treating them as having a fixed, unchanging nature rather than constantly changing and evolving. He points out that digital objects are not only software but also have a physical dimension and are embedded in an ecological network.

Both Hui and Tsing advocate for a more nuanced and critical understanding of the social and cultural factors that shape the development and deployment of systems. Furthermore, they advocate for a more inclusive and participatory approach, one that incorporates diverse perspectives and voices to address these issues. Taking their argument to a broader discussion involves the very concept of humanity. Instead of object-oriented ontology, the philosopher advocates for an alternative perspective, known as process philosophy, which constantly emphasizes the ongoing processes of change and evolution that digital objects undergo. He suggests that a process-based view can help us better understand the nature of digital things and their relationship to the world around us, particularly in critiquing the reductionism and reification of digital objects in the current understanding of object-oriented ontology and computing. It offers an alternative perspective and process philosophy to understand digital things holistically. Hence, our argument that errors are not incidental but constitutive of a technological regime that maintains *claustrophobic humanity* in check. In summary, scholars such as Yuk Hui and Anna Tsing have highlighted the complex and multifaceted issues involved in facial recognition systems, primarily focusing on how these systems reflect and reinforce existing power relations and social hierarchies, including racial biases. A more critical and holistic approach to understanding facial recognition technology's ethical and political dimensions is essential.

How is humanity being constructed both by human and non-human agents? Is AI inherently racist, or is this issue part of a broader, systemic problem related to extractivism and precarization? When it comes to *racism in AI*, the issues often manifest through an idiom of "mistakes' and misidentification. We argue that the issues presented are not new, although the mechanisms use the latest technological developments. Instead, since its Foucaultian (2014) description, the mass incarceration project has used every possible technology to execute its protocol rather than affirming that the neutrality of technology should be protected from human world-making, which carries its biases and historical oppressions. We differ by demonstrating that the deployment of technology to maintain idioms of precarity is not novel. It is a movement aimed at maintaining a claustrophobic humanity and keeping humanity in check. The play of smoke and mirrors is apt here to understand how these technologies are embedded in logic, as the very science they derive from—producing, reproducing, and maintaining the status quo, the claustrophobic idea of humanity—an idea that does not account for the effervescent plurality of the world.

Technodiversity refers to the existence of multiple and diverse forms of technology within society and the importance of preserving this plurality. Yuk Hui argues that technodiversity allows for diverse expressions of social and cultural identity and acts as a safeguard against the harmful effects of technology on society. For example, if all technologies were developed and controlled by a small group of people or organizations, there would be a greater risk that these technologies would be used in ways harmful to society. Therefore, technodiversity is necessary for maintaining a healthy relationship between humans and technology, as well as for developing new and innovative forms of technology. To promote technodiversity, Hui suggests the need to diversify the ways we conceive and design technology, as well as the way we evaluate its implications and consequences. Additionally, it is essential to ensure diversity in the development and distribution of technology, so that a small group of people or organizations does not monopolize various forms of technology. Hui's work also encourages us to consider technodiversity in the decision-making process and technology's ethical and political implications.

CONCLUSION

Throughout this paper, we aim to present empirical evidence on how structural racism is intertwined with the sociotechnical landscape of AI-based facial recognition systems currently used in Brazilian public security. Thus, we argue that, far from assuming any role of neutrality or objectivity, these machines that learn from their collected data shape automated surveillance systems that reproduce racial inequalities and execute discriminatory punishments. They thus inaugurate a new device of digital colonialism. To normalize the computational decision on people identification, assuming that eventual errors would be nothing more than inevitable accidents to be solved by the technological advances of AI systems, is to hide the multiplicity of power relations involved in the creation, promotion, and use of technology.

More than denouncing the emergence of new racist technologies, the question seems to be how to gather ideas and social forces to resist the mechanisms that feed and legitimize contemporary processes of digitalization of racism and dehumanization. A promising path may be demonstrating the fragility of AI systems through audits, ethnographies, or journalistic accounts. However, a growing alliance between developers, scientists, and activists seems fundamental to expanding the possibilities of technological (re)appropriation and recreating the relations we intend to build with and from the digital world. In this case, we critically reflect on how our humanity interacts with the technologies of our time. Rather than offering prescriptive metaphors, we aim to create space for plural, situated approaches to building just technologies and reimagining humanity. Thus, techniques and technologies are not monolithic but amalgamations of local relations and humanities shaped by differences. Therefore, we argue that closed understandings of technology imply claustrophobic conceptions of humanity. To reimagine humanity beyond these claustrophobic limits requires resisting not only the technologies of control but also the epistemologies that underpin them.

REFERENCES

ADORNO, Sérgio. Exclusão socioeconômica e violência urbana. *Sociologias,* Porto Alegre, ano 4, n.8 jul/dez 2002, p. 84-135.

ALMA PRETA. 'TIRE Meu Rosto da Sua Mira': reconhecimento facial pode ser mais uma ferramenta de violação de direitos. *Alma Preta*, São Paulo, 24 nov. 2022. Disponível em: https://almapreta.com.br/sessao/cotidiano/tire-meu-rosto-da-sua-mira-reconhecimento-facial-pode-ser-mais-um-ferramenta-de-violacao-de-direitos/. Acesso em: 20/maio/2025.

BELLI, Luca; HORA, Nina da. ChatGPT: o que anima e o que assusta na nova inteligência artificial. *Folha de S. Paulo*, São Paulo, 20 jan. 2023. Disponível em: https://www1.folha.uol.com.br/tec/2023/01/chatgpt-o-que-anima-e-o-que-assusta-na-nova-inteligencia-artificial.shtml#:~:text=O%20ChatGPT%20levanta%20quest%C3%B5es%20muito,e%20preparados%20gra%C3%A7as%20a%20ela. Acesso em: 20/maio/2025.

BENTO, Cida. *O Pacto da Branquitude*. São Paulo: Companhia das Letras, 2022.

BOMFIM, Fabiano; RIOS, Alan. 'Disseram que eu era traficante', diz pedreiro preso injustamente. *Notícias R7*, Brasília, 15 dez. 2021. Disponível em: https://noticias.r7.com/brasilia/disseram-que-eu-era-traficante-diz-pedreiro-preso-injustamente-16122021/. Acesso em: 20/maio/2025.

BOUTIN, Chad. NIST Study Evaluates Effects of Race, Age, and Sex on Face Recognition Software. *NIST,* Washington, 19 dez. 2019. Disponível em: https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. Acesso em: 20/maio/2025.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Journal of Machine Learning Research*, v. 81*,* p. 77-91, 2018.

CARNIEL, Fagner; LACRUZ, Adonai José; AMÉRICO, Bruno Luiz; MATHIAS, Meire. Estudos decoloniais nos circuitos hegemônicos da produção acadêmica brasileira. *Cadernos EBAPE.BR*, v. 22, n. 6, p. e2022–0230, 2024.

CERQUEIRA, Daniel et al. *Atlas da Violência 2021*. São Paulo: FBSP, 2021.

FOUCAULT, Michel. *Vigiar e Punir: Nascimento da Prisão*. São Paulo: Editora Vozes, 2014.

FOUCAULT, Michel. *História da Loucura.* São Paulo: Editora Perspectiva, 2019.

G1. Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. *G1*, Rio de Janeiro, 11 jul. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 20/maio/2025.

HUI, Yuk. *On the existence of digital objects*. Minneapolis: University of Minnesota Press, 2016.

MBEMBE, Achille, Nécropolitique. *Raisons Politique*, v.1, n. 1, p. 29-60, 2006.

MELO, Paulo Victor; SERRA, Paulo. Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematizações. *Comunicação e Sociedade,* n. 42, p. 205-220, 2022.

MISSE, Michel. *Crime e violência no Brasil contemporâneo: Estudos de Sociologia do Crime e da Violência Urbana*. Rio de Janeiro: Editora Lúmen Juris, 2006.

MOROZOV, Evgeny; BRIA, Francesca. *Rethinking the Smart City: Democratizing Urban Technology*. New York: Rosa Luxemburg Stiftung, 2018.

QUIJANO, Anibal. Coloniality of Power and Eurocentrism in Latin America. *International Sociology*, v. 15, n. 2, p. 215-232, 2000.

ROSA, Cássio Thyone Almeida de. Quando a Inteligência Artificial é Preconceituosa: O Reconhecimento Facial em xeque. *Fonte segura: Fórum Brasileiro de Segurança Pública*, São Paulo, n. 120, 12 a 18 jan. 2022. Disponível em: https://fontesegura.forumseguranca.org.br/quando-a-inteligencia-artificial-e-preconceituosa-o-reconhecimento-facial-em-xeque/. Acesso em: 20/maio/2025.

SCHWARCZ, Lilia Moritz. *Rascismo no Brasil*. São Paulo: Publifolha, 2001.

SILVA, Tarcízio. *Racismo Algorítmico: inteligência artificial e discriminação nas redes digitais*. São Paulo: Edições SESC, 2022.

TSING, Anna Lowenhaupt. *The mushroom at the end of the world: on the possibility of life in capitalist ruins*. Princeton: Princeton University Press, 2015.

VALENTE, Jonas. Riscos da inteligência artificial levantam alerta e suscitam respostas. *Agência Brasil*, Brasília, 01 set. 2020. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-08/riscos-da-inteligencia-artificial-levantam-alerta-e-suscitam-respostas. Acesso em: 20/maio/2025.

ZALUAR, Alba. Um debate disperso: violência e crime no Brasil da redemocratização. *São Paulo em Perspectiva*, v. 13, n. 3, p. 3–17, 1999.

Texto recebido em 11/08/2024 e aprovado em 13/05/2024