


IN THE DIGITAL PENAL COLONY: FRANZ KAFKA'S LESSONS FOR THE PROPER IMPLEMENTATION OF FACIAL RECOGNITION SYSTEMS IN BRAZIL

 <https://doi.org/10.56238/arev7n3-178>

Submitted on: 02/18/2025

Publication date: 03/18/2025

Milton Pereira de França Netto¹, João Araújo Monteiro Neto² and João Paulo Allain Teixeira³

ABSTRACT

The article aims to investigate the dangers associated with the uncritical implementation of facial recognition systems in Brazil, with a special focus on the scope of public security, from a contemporary rereading of the short story "In the Penal Colony", by Franz Kafka. Using the bibliographic review and documentary research, the study resorts to the literary work to establish comparisons with the current dilemmas faced during the state implementation of facial recognition systems, presenting cases of errors in the identification of individuals. Next, the work draws on doctrinal lessons from national and foreign authors, and reports provided by the "O Panopticon" initiative to outline the contours of the phenomena of digital neocolonialism and algorithmic discrimination and to ascertain their harmful impacts on the black population. Finally, the article examines the provisions on the subject contained in the most recent version of Bill No. 2,338/2023, which proposes to regulate Artificial Intelligence in Brazil, and in the Artificial Intelligence Act (AI Act), of the European Union, suggesting the normative improvement of the national text in light of foreign experience.

Keywords: Facial Recognition. Franz Kafka. Algorithmic Discrimination. Digital Neocolonialism. Bill No. 2,338/2023. Artificial Intelligence Act (AI Act).

¹ Doctor student in Law at the Catholic University of Pernambuco and the University of Seville. Master's degree in Law from the Cesmac University Center. Researcher and Professor of Digital Law.

E-mail: milton.00000849969@unicap.br

ORCID: <https://orcid.org/0000-0002-3671-1897>

² Doctor in Law from the University of Kent in the United Kingdom. Incident Response Improvement Course by the Organization of American States in partnership with the Institute of Cybersecurity of Spain (INCIBE) and the University of Leon in Spain. A former researcher at the University of Malta and Volunteer in the Mandate of the UN Special Rapporteur on the Right to Privacy. Professor of Digital Law, Personal Data Protection, and Legal Engineering in the Law course at the University of Fortaleza. Lawyer specialized in Data Protection and Privacy, President of the Digital Law Commission of OAB/CE. Certified Information Privacy Professional/Europe (CIPP/E) by the International Association of Privacy Professionals (IAPP) and Privacy Fellow by Onetrust. Coordinator of the Study Group on Technology, Information and Society - GETIS with activities in the areas of Information Technology Law, Internet Governance and Regulation, Digital Human Rights, Privacy and Personal Data Protection, Artificial Intelligence, and Cybersecurity.

E-mail: joaoneto@unifor.br

³ Doctor in Law from the Federal University of Pernambuco. Master in Law from the Federal University of Pernambuco, Master in Critical Theories of Law from the Universidad Internacional de Andalucía, Spain. Graduated in Law from the Federal University of Pernambuco. Professor at the Catholic University of Pernambuco.

ORCID: <https://orcid.org/0000-0001-9467-6973>

INTRODUCTION

The constant fear of being watched symbolizes contemporary reality. With the mass digitization of social relations, idiosyncrasies are converted into mathematical data, used to induce behaviors under the silent command of *big techs*. Artificial intelligence (AI) emerges as the battering ram of this hyper-connected era, automating tasks by discovering underlying patterns in oceanic *informational* Big Data.

Among their most controversial applications, facial recognition systems stand out for the evolution given to such spy eyes. Ubiquitous on streets, football stadiums, airports, residential and business buildings, subway stations and commercial stores, they allow the instant identification of people after capturing biometric data of their faces and comparing them with pre-existing image banks.

Publicized as definitive answers to the problems that plague public security, these devices arouse the fascination of enthusiasts for new technologies, materializing the fictional warnings about the excessive admiration for scintillating machines that were underlined by Frank Kafka, more than a hundred years ago, in the short story "In the Penal Colony".

This article uses the deductive methodology, linked to bibliographic review and documentary research, to analyze the dangers arising from the reckless use of facial recognition instruments in light of the teachings left by the Czech writer in the work in question.

Thus, the study resorts to the Kafkaesque narrative to draw comparisons with the current dilemmas faced in the state implementation of facial recognition systems, plagued by numerous cases of identification errors. Later on, the research uses the doctrinal lessons of Alexandre Pimentel, Byung-Chul Han, Cathy O'Neil, Joy Buolamwini, Timnit Gebru, Giselle Beiguelman, Walter Lippold, and Deivison Faustino to outline the contours of digital neocolonialism and investigate how facial evaluation algorithms behave about socially underprivileged groups.

Next, the work examines data and reports published by the "O Panopticon" initiative to ascertain the level of implementation of such devices in Brazil and their harmful impact on the black population, considered the central target of the problem of algorithmic discrimination.

Finally, the text scrutinizes the provisions on the subject contained in the most recent version of Bill No. 2,338/2023, which proposes to regulate artificial intelligence in

Brazil, and in the *European Union's Artificial Intelligence Act (AI Act)*, which inaugurated the discipline of the area at a global level, to seek normative solutions to the obstacles associated with it.

THE REREADING OF FRANZ KAFKA IN THE LIGHT OF NEW TECHNOLOGIES

Conceived in 1914 and published in 1919, the short story "In the Penal Colony" explores the daily life of an island penitentiary facility that has been affected by discussions around its main punitive apparatus: an autonomous machine of slow torture that is worn out after years of continuous operation (Kafka, 2020).

To this end, the narrative resorts to two protagonists: a) the Traveler, invited by the current commander of the facility to evaluate it and representative of the reader's "eyes and ears"; and b) the Officer, equipped with the functions of a judge in the district and operator of the aforementioned apparatus. The pair's interactions touch on the execution of a Convict, who found himself under the escort of a Soldier for the (alleged) practice of the crime of disobedience⁴.

In addition to mirroring the colonialist tone that gave rise to the First World War, the work acquires relevance by allowing reflections on its contemporary evolution, digital neocolonialism, whose fabric comprises the uninterrupted monitoring of citizen-users, often exercised through facial recognition tools.

Several parallels can be drawn about the events of the plot to explain how modern technological phenomena have the power to cyclically reshape past problematic issues. This is what is intended to be done next.

"IT'S A PECULIAR DEVICE": THE MODERN FASCINATION AROUND FACIAL RECOGNITION TOOLS

"It is a peculiar device" (Kafka, 2020, p. 18). With this inaugural sentence, Kafkaesque's text anticipates the controversies associated with the torture machine, which could no longer attract the interest of the island's residents as it once did, but persisted as an object of fascination for the Officer, who was in charge of its maintenance and start-up. The latter's affection for the device designed by his former commander constitutes the

⁴ Although the original material highlights the names of the characters in lowercase letters, the present text uses initial capital letters in the mentions of the quartet in order to facilitate the reader's understanding.

motto of the writing, aimed at debating the punitive zeal of the time — orchestrated, nowadays, by the oppressive use of new technologies, especially artificial intelligence (AI).

Curiously, the character's dazzle resembles that of enthusiasts of contemporary facial recognition systems, ubiquitous on public roads, residential and business buildings, commercial establishments, airports, soccer stadiums, and subway stations. As taught by the European *Artificial Intelligence Act (AI Act)*, considered the proposal for regulation of the most advanced area in the world, such remote observation machines represent AI systems aimed primarily at "identifying natural persons without their active participation, usually at a distance, by comparing a person's biometric data with the biometric data contained in a reference database" (art. 3, No. 41) (European Union, 2024).

Like the colony's apparatus, these solutions carry a series of dangers. Starting with the unauthorized capture and processing of sensitive personal data that is protected by the General Law for the Protection of Personal Data (Law 13.709/2018) and the Federal Constitution⁵.

As clarified by the National Data Protection Agency (ANPD) in the report "Technological Radar No. 2: Biometrics and Facial Recognition", although item III, of article 4, of the LGPD, excludes the processing of personal data for the exclusive purposes of public security, national defense, State security or activities of investigation and prosecution of criminal offenses from the scope of application of the law, the determinations provided for in paragraphs 1 to 5 of the provision remain mandatory (Cebrian, 2024, p. 8-9).

In these cases, the processing will be guided by its legislation, respecting the due process of law and the general principles and rights of the holder contained in the LGPD (§1) and preserving the prohibitions imposed by it on legal entities governed by private law (§§2 and 4). The above document is also an unfolding of the openness granted to the ANPD to issue opinions and recommendations on the aforementioned exceptional scenarios (paragraph 3) (Cebrian, 2024, p. 8-9). Therefore, regardless of their public or private destination, facial recognition solutions must pay attention to the protective law in question.

Another threat lies in the risks of algorithmic discrimination, in which damage is (re)inflicted on historically underprivileged individuals or groups, such as the female, black,

⁵ "Article 5 - All are equal before the law, without distinction of any kind, guaranteeing to Brazilians and foreigners residing in the country the inviolability of the right to life, liberty, equality, security and property, in the following terms: [...] LXXIX - the right to the protection of personal data, including in digital media, is ensured, under the terms of the law (Included by Constitutional Amendment No. 115, of 2022)".

and LGBTQIAPN+ populations. In the direct modality of the institute, the biases are noticeable, as they are based on the flagrant misrepresentation of very personal attributes (e.g. race, gender, ethnicity, political ideology, religious orientation, sexual preference, and/or biometric data) throughout the functioning of the AI system. However, the main obstacles lie in its indirect form, whose models appear statistically irreproachable, but end up hiding dangerous discriminations (França Netto; Ehrhardt Júnior, 2022).

In its opening lines, the fictional writing signals the submission of the Convict, who "seemed to be delivered in such a canine way that the impression was that it would be possible to let him roam freely on the slopes and it would be enough to whistle at the beginning of the execution for him to come" (Kafka, 2020, p. 17), to the figure of the Officer. Unrestricted subjection is also a product of modern surveillance instruments, capable of silently monitoring multitudes of people at the same time under the pretext of ensuring their safety, as well as social networks, ideal environments for the use of stealth techniques by *big techs* to capture and maintain the attention of users.

In the following pages, it is seen that the Officer communicates with the Traveler in French — a language foreign to the Convict — to graphically report the operation of the machine, whose purpose was to engrave on the skin of the convicts the commandments they had not complied with, configuring an automated process of torture that would lead to their death. Tied face down to a cotton bed, they would be pierced by needles stuck in a rake, which would engrave on their backs the figures submitted to the "designer" from sketches made by the former commander⁶.

The story portrayed a "one-man court", composed only of the Officer and devoid of reviewing bodies, in which the axiom that "guilt is always indubitable" prevailed. The Convict was not aware of his sentence or the possibility of defense, being sent to the mortal apparatus for the practice of the crime of disobedience by (supposedly) failing to salute his former captain. Subject to summary judgment, he was on the verge of being marked, literally and figuratively, for a crime he might not have committed.

⁶ A visual representation of the fictional torture machine devised by Kafka is available at: https://thefunambulistdotnet.wordpress.com/wp-content/uploads/2013/04/kafka_torture-machine640.jpg. Accessed on 20 Aug. 2024.

"IN THE DIGITAL PENAL COLONY": THE MISTAKES IN THE IDENTIFICATION OF PEOPLE THROUGH ARTIFICIAL INTELLIGENCE SYSTEMS

Similar stigmas are forged by the panopticism of facial recognition lenses. Under the initial investment of R\$ 18 million, the Video Surveillance System of the Military Police of Rio de Janeiro will integrate tools of this type into the 21 cameras of the Rio Operations Center (COR) in operation in the Lapa neighborhood, "aiming to increase the sense of security in the population". When it locates people with pending legal issues, the apparatus activates the nearby police team to make stops and, eventually, arrests (Lisbon, 2024) — however, since its inauguration on *New Year's Eve* 2023, the machine has been gaining notoriety for consecutive cases of identification errors.

In January 2024, a woman was detained after it was found that there was an open arrest warrant in her name. After the investigation, the Civil Police realized that it had already been served and that the sentences restricting freedom had been replaced by sanctions restricting rights in his conviction in an open regime (Coelho *et al.*, 2024). In addition, an Argentine was arrested after the detection of an active arrest warrant for the robbery of a supermarket. At the custody hearing, it was found that the release warrant about the crime had been previously issued (Saleme, 2024).

The mistakes are not limited to the Rio de Janeiro scenario. During a Carnival preview party in Aracaju at the end of 2022, a young woman was mistaken for a fugitive from justice by the facial recognition system in operation, at two different times. In the second approach, after exclaiming that she had not committed any irregularity, she reports having received the reply "You know what you did, right?" from one of the police officers, amid the truculent treatment that was given to her⁷. As the postulate verbalized by the Kafkaesque Officer would say: guilt is always indubitable.

The state of Sergipe hosted another infamous incident during the local football championship final, held in April 2024, when a fan was mistakenly identified by the facial recognition system of the Arena Batistão stadium. After being approached by the police amid the crowd present, the individual was led through the lawn with his hands behind his

⁷ When reconstructing the episode, the young woman reports that: "Later, around 6:30 pm, when they were already accommodating Ivete Sangalo's trio, I passed next to a Military Police car and some approached me in a totally different way. They didn't ask for my name, nor my document. They threw my glass on the ground, took my cell phone, held my hands behind my back, holding it very tightly. I said 'I didn't do anything'. A PM said 'you know what you did, right?'. At this point, I urinated. They put me in the van. All coerced, coerced, everyone looking at me, me asking someone to film. But no one helped me. They took me to a tent, where there were other policemen. I arrived crying, desperate" (RIBEIRO, 2023).

back and detained, being pressured by one of the professionals to "speak the truth", because, supposedly, there would be an open arrest warrant in his name. The episode of embarrassment gained notoriety and led the state government to suspend the use of the tool (Medo, 2024).

The situations described above reveal the dangers of the dissemination of surveillance tools without the proper safeguards of those under their scrutiny. One of the main obstacles to contesting decisions coming from intelligent systems, especially advanced models based on the architecture of artificial neural networks, lies in explainability, that is, in the ability of the lay public to understand them.

Just like the Traveler, who faced difficulties in trying to understand the drawings of the former commander that guided the machine, and like the Condemned, alien to the French language used by the Officer, the average citizen will not succeed in outlining the intricacies of more complex algorithms. Composed of multiple layers between its input and output barriers, which capture patterns from the data, these remain unknown even to their developers⁸.

KAFKA'S LESSONS TO THE VIGILANTISM OF THE PRESENT

By preaching for the continuity of the operation of the machine in the colony, the Officer softened his inclement weather by adding that it was "very complicated, from time to time something breaks or breaks; but one cannot be deceived and misjudged the whole" (Kafka, 2020, p. 52). Similar defenses are brought by the coreligionists of modern technological leaps, who commonly disregard the numerous mishaps intrinsic to such events.

In the last portion of the literary work, the character nostalgically recalls the old executions carried out on the island, which attracted crowds of spectators. Fearful of the changes to end this process in declining popularity, the Officer desperately seeks the support of the Traveler. The latter, in turn, opposes the daily violence in the locality and reports that he will communicate his opinion to the new commander, as requested.

Resignation symbolizes the outcome of the tale when the Officer declares the Condemned Man's freedom — finally communicating in his language — and shows a sheet

⁸ The main distinction between simplified Machine Learning algorithms and their evolutionary form of Deep Learning lies in the existence of multiple layers between the input of data and the output of information of interest.

of his wallet to the Traveler that seems to contain the inscription "be just." Attentive to the commandment, the Officer goes to the machine, inserts this engraving into the "draughtsman" and rests on the bed, starting a self-procedure of torture.

Next to the Convict and the Soldier, the Traveler notices that the machine's gears have begun to loosen and that the rake no longer writes on the Officer's skin, but rather thrusts it over and over again. Going to the last consequences to preserve his belligerent ideology, he becomes the last product of the apparatus he had admired so much, now in ruins, without achieving the redemption usual to all who preceded him.

The character's fateful fate serves as a warning to those who, in an incautious way, defend technological innovations tainted by potential harm to their users and recipients. The reversal of roles between the Officer and the Convict signals how, eventually, the offenders can become offended.

In digital neocolonialism, minority groups are underrepresented and often algorithmically oppressed. Examining the founding causes of the situation becomes, therefore, essential.

DIGITAL NEOCOLONIALISM AND THE GEARS OF ALGORITHMIC DISCRIMINATION DYNAMIC

According to Alexandre Freire Pimentel (2023, p. 55-85), modern technological subjugation is characterized by ubiquity, by transcending state geographical limitations and resulting in the "relocation of power" within cyberspace, and by the unnecessary of coercive sanctioning exercise, as adhesions unfold in a "pseudo-spontaneous" way amid the scenario of digital neocolonization.

The main apparatus of this one, technopower translates into the control of human action for various purposes (e.g. political, economic, and social). The panoptic domination of the disciplinary society, founded on the perennial fear of being surveilled, is perfected in the society of digital control, establishing the "real, constant, and acquiescent" monitoring of the citizen-user, whose renunciation or relativization of privacy symbolizes the price of existing in the contemporary artificial conjuncture (Pimentel, 2023, p. 55-85).

In turn, Byung-Chul Han (2022, p. 7-24) describes the transition between the sovereign, disciplinary, and information regimes, from the element of visibility. While the former stood out for the excessive self-promotion of the dominators through theatrical

manifestations of power, the latter directed its spotlight to the dominated, unwillingly exposed in the cells that make up the *Benthian prison structure*.

Intrinsic to surveillance capitalism, the information regime is differentiated by the voluntariness of people to submit to the scrutiny of others, notably in the den of social networks, infested by the hyper-sharing of daily events. The South Korean philosopher underlines how, paradoxically, the alleged sense of freedom actually acts as fuel for domination — now exercised over the psyche (psychopolitics) and infinitely fueled by virtual communications (Han, 2022, p. 7-24).

Giselle Beiguelman (2023, p. 55-96) weaves an interesting perspective on modern monitoring from the image element, increasingly manufactured by machines (e.g. *QR Codes*) or by the instruments they operate (e.g. satellites). The original paradox of the human gaze — according to which we feign who sees us in return — is replaced by a new model, in which the reading unilaterally carried out by algorithms results from the photographs (and other information) we share, so that "the big eyes that monitor us see through our eyes" (Beiguelman, 2023, p. 69).

In addition, the author highlights how the biopolitics of the atmosphere becomes porous, subtly entering our bodies through remote sensing systems, able to capture information without the need for physical contact. By rescuing the notion of "operational images" coined by the German filmmaker Harun Farocki, which are present, for example, in thermal cameras that measure people's spectral signature, she illustrates how fragile privacy is configured in the face of the naturalization of such tools, whose products appear imperceptible and incomprehensible to the human framework, but are decipherable by the artificial entities that take the reins of the surveillance processes (Beiguelman, 2023, p. 55-96).

Deivison Faustino (2023, p. 184-190) and Walter Lippold rightly explain how racism, which engenders past and future colonization, is not addressed by the analyses of theorists of digital colonialism. Typical of this, the conversion of people into commodities at the mercy of *big techs* ignores how such an element impacts the price of blacks in the *digital locus*, still considered inferior.

In this way, they suggest overcoming the popular expression "algorithmic racism", which exempts programmers from responsibility, with the term "digital racialization", which better reflects the conjuncture of algorithm design, tainted by racial prejudices in the filling of technical positions, in the valorization of content creators and the configuration of social

networks and image banks. Among the harmful materializations arising from the phenomenon are facial recognition tools, surrounded by incongruities in the identification of black people (Faustino, 2023, p. 184-190).

Joy Buolamwini and Timnit Gebru (2018) unveil the gears of automated facial analysis mechanisms to study the problem of algorithmic discrimination. By performing tasks such as detecting, classifying, and recognizing faces, these artificial intelligence systems can produce race- and gender-biased results that are detrimental to already historically disenfranchised groups.

Immersed in the branch of Machine Learning (*ML*), its algorithms are intended to find patterns amid large amounts of data, without the need for specific programming, to originate a model that better connects the input information to the output), subsidizing decisions, recommendations, and forecasts. Among the *ML* species, Supervised Learning solutions are distinguished by the attribution of labels to training data, which confer features to the analyzed objects (França Netto; Ehrhardt Júnior, 2022).

At first, the researchers observed that race and ethnicity labels, used to assess the existence of discrimination in certain types of data, are not suitable for the examination of visual images, given the enormous variety of internal attributes of these categories and the discrepancies that exist between countries. Consequently, they chose to use an intersectional labeling based on two attributes: a) gender, considered as male or female; and b) skin type, in the light of the Fitzpatrick dermatological scale, composed of six gradations — three for lighter skin tones and three for darker skin tones⁹.

Thus, the pair selected the IJB-A and Adience datasets, considered important repositories of photographs of faces for the training of AI systems, and manually identified each of their images based on the two factors. As a result, it was found that the data sets were composed of 79.6% and 86.2% of lighter-skinned individuals, respectively, indicating the glaring underrepresentation of darker-skinned people (Buolamwini; Gebru, 2018).

Under a classification that combines the *features* in four categories (darker man, lighter man, darker woman and lighter woman), ¹⁰it was observed the overrepresentation of lighter men in the two *datasets* (59.4% in the IJB-A and 44.6% in the Adience) and the

⁹ As the researchers emphasize, the methodological choices used are also subject to scrutiny, given that the Fitzpatrick scale does not faithfully categorize the sepia tone that characterizes the rest of the world and that the binary gender classification excludes relevant segments, such as non-binary people and transsexuals.

¹⁰ In the direct translation of the terms *darker male*, *lighter male*, *darker female* and *lighter female*, used in the original text by Buolamwini and Gebru.

almost non-existence of darker women in the IJB-A (4.4%) and darker men in the Adience (6.4%).

In the face of these flagrant imbalances, the scientists formulated their own benchmark, the Pilot Parliaments Benchmark (PPB), which compiles images of parliamentarians from three African countries and three European countries¹¹, chosen for their greater ease of finding institutional photos and for the good performance of the nations in *rankings* gender parity in their legislative bodies. The PPB showed promising results with regard to the harmonious presence of lighter people (53.6%) and darker people (46.4%) in the data sample, equally balanced in relation to the specific categories — darker woman (21.3%), darker man (25.1%), lighter woman (23.3%) and lighter man (30.3%) (Buolamwini; Gebru, 2018).

In the end, three commercial gender classifiers made available on the market by Microsoft, IBM and Face++ were evaluated by the researchers based on the intersectional methodology mentioned. All had higher error rates for women compared to men and for darker people compared to lighter ones. While the group of darker women performed the worst, the group of lighter men performed the best.

If thoughtlessly employed, automated facial assessment systems, especially face recognition tools in the field of public security, can become *Weapons of Math Destruction (WMD)*, as Cathy O'Neil (2020, p. 81-99) warns, dressing up as digitized versions of the analog "stop-and-search" initiative.

Popularized under the lens of zero-tolerance policies, this encourages the police authority to carry out combative approaches to all types of crime, which, in theory, would ensure the reduction of crime rates through discouragement. As well as predictive policing solutions (e.g. PredPol), which use AI to predict which crimes tend to be committed in a given location at a certain time, optimizing the targeting of their personnel contingents, this type of practice proves to be harmful to the black and Latino populations (O'Neil, 2020, p. 81-99).

Both are not very effective in the face of major crimes (e.g. homicide and rape), with greater application to those of lesser importance (e.g. possession of small amounts of drugs and vagrancy), considered endemic problems of poorer neighborhoods. When systems such as PredPol are fed back with arrest data from the aforementioned demographic groups due to the consummation of these mild disturbances, a looping effect

¹¹ Parliamentarians from Rwanda, Senegal, South Africa, Finland, Iceland and Sweden were selected.

is produced that directs more police officers to such areas, in search of suspects with similar phenotypic characteristics, in an infinite cycle of institutionalized persecution (O'Neil, 2020, p. 81-99).

Despite the numerous warnings about the dangers associated with the use of facial recognition systems in public domains, notably with regard to mistakes made during the identification of citizens – which can subsidize wrongful detentions and human rights violations – national projects in the area are booming.

THE CONTROVERSY SURROUNDING THE IMPLEMENTATION OF FACIAL RECOGNITION SYSTEMS IN BRAZIL

Conceived in 2019 by the Center for Security and Citizenship Studies (CESeC) integrated with the Cândido Mendes University (RJ), the "O Panopticon" initiative directs its attention to national projects that employ facial recognition technologies in public security, compiling statistics and studies on the subject. Its most recent calculation (updated on 01/27/2025) accounts for 337 active projects in the country¹², distributed among the North (27), Northeast (56), South (63), Southeast (102) and Midwest (89) regions, which together reach the expressive mark of 81 million people potentially surveilled¹³.

In his report "A Rio of selective eyes: use of facial recognition by the Rio de Janeiro police", it is possible to observe the timeline of such applications in the state of Rio de Janeiro, inaugurated by the video surveillance pilot project carried out by the State Secretariat of Military Police (SEPM) in collaboration with the company Oi in 2019, whose coverage covered, at first, the Copacabana neighborhood, later extending to the vicinity of Maracanã and Santos Dumont airport (Nunes, 2022).

The symbolism of the choice of the noble area as a starting point lays bare the underlying intent of removing the peripheral populations from their spaces through the management of the movement of people. During the first phase of the experiment, 2,993,692 faces were captured and 2,465 were recognized, totaling a tiny correlation rate of 0.082%. In its second phase, in the course of a soccer game, eleven people were

¹² From a methodological point of view, "active projects" are those that are in the bidding, testing, occasional use or regular use phase, whose planning and preparation stages are in progress or completed, with facial recognition technologies being implemented as a public security policy. The calculation of the number of people potentially monitored is based on the population indices of the municipalities affected by such tools in light of the numbers made available in the "2022 Demographic Census" by the Brazilian Institute of Geography and Statistics (IBGE) (METHODOLOGY, 2024).

¹³ The states of Goiás and São Paulo lead the list, respectively, in terms of the number of active projects (72) and potentially surveilled people (18.6 million).

identified and detained in the vicinity of Maracanã, however, only four of them had open arrest warrants, configuring an error rate of 63% (Nunes, 2022).

Despite the reduced efficiency of such devices, the "Integrated City" project emerged in 2022 with the purpose of installing 22 cameras (4 with facial recognition) in the Jacarezinho favela, located in the North Zone of Rio de Janeiro, motivating criticism based on the exemption from the bidding procedure and the high burden on the public budget. Its most alarming aspect lies in the emphasis given by the preliminary technical study formulated to the function of the system to assist in the production of evidence ratifying police reports in lawsuits, contrasted by the silence in relation to the common violence in operations carried out in communities (Nunes, 2022).

Analogous concerns underpinned the open letter addressed to the current Mayor of Recife, João Campos, by the Institute for Research in Law and Technology of Recife (IP.rec) together with several scientific associations, motivated by the promise of installing 108 digital clocks in the city, which, in addition to basic functions, such as temperature measurement and access to *Internet connection* via *WI-FI*, would have facial recognition cameras of citizens (Carta, 2021).

In it, it was suggested that the following be aligned with international positions favorable to the banning of the technology, highlighting the following as problematic aspects: a) the inadequacy of the measure in view of the determinations of the LGPD, especially with regard to the indication of the legal basis of the treatment and the measures to mitigate damages; b) the absence of mention of safety guidelines; c) potential violations of privacy and civil rights, such as freedoms of assembly and demonstration; d) algorithmic biases, capable of producing harmful results for black and brown people; e) legal uncertainty, which led to the judicial suspension of bidding documents in the area in Brazil; and f) questionable confluence of public and private interests. Even so, the Recife City Hall continued with the installation of the equipment in 2022 (Recife, 2022).

The search for technological remedies capable of remedying the ills of public security has also permeated government actions in the state of Ceará in recent decades, from the conception of the "Ronda do Quarteirão" program (2005), marked by the coupling of cameras to vehicles, through video surveillance in renowned sporting events, such as the Confederations Cup (2013) and the World Cup (2014), to the creation of the "Advanced Command Portal" app (2019), which enables facial recognition through police

cell phones, and the solidification of the *segment's informational big data, named "Odin", and its analytical panel, "Cerebrum"* (Martins et al., 2024).

With large investments that exceed the mark of half a billion reais – much of it destined to a Brazilian company (IPQ Tecnologia Ltda), with ties to a Chinese corporation (Dahua Technology) – the surveillance structure designed on Ceará soil is characterized by an opaque tangle of public and private interests, whose additional knots come from the participation of the local academic community (Martins et al., 2024).

More than 3.6 thousand cameras maintained by the state government and 4.5 thousand cameras under the sieve of the municipal administration of Fortaleza are in operation (Martins, 2024). It is worth remembering that, in early 2022, the capital attracted national attention in an unwanted way when the Civil Police cataloged the image of *Hollywood* star Michael B. Jordan, who is African-American, for photographic recognition purposes as one of the suspects in a massacre that left five dead (Photo, 2022).

The potential discrimination resulting from the use of automated facial recognition systems also surrounds the gender element, affecting the transsexual population by resulting in the misidentification of the transsexual population or the non-recognition of the person after transition procedures. Subject to habitual body modifications, this demographic is not satisfactorily represented by algorithmic metrics trained to identify allegedly male and female faces, which can contribute to discriminatory classifications, obstructions of access to certain public spaces (e.g. changing rooms and bathrooms) and violations of the right to identity (Silva, 2021).

As Heloísa Silva (2021) points out, the consolidation of this permeates the recognition by others, often passed over due to transsexual passability in everyday life. In a scenario of scarcity of research focused on this population cut, which amplifies its invisibility and the fading of the demands around the above problems, it is necessary to understand that

surveillance technologies can be instrumentalized for (a) the reproduction of consolidated power structures, based on norms about the body, gender, sexuality, and other expressions of identity, which identify, track, and exclude certain segments as threats (SILVA, 2021, p. 57).

In the absence of specific disciplines that protect the groups affected by such AI applications, it is appropriate to investigate the proposals for its regulation in Brazil and in its greatest legislative inspiration on the matter, the European Union.

FACIAL RECOGNITION FROM THE PERSPECTIVE OF BILL NO. 2,338/2023 AND THE ARTIFICIAL INTELLIGENCE ACT (AI ACT)

Conceived as the future legal framework for artificial intelligence in Brazil, Bill No. 2,338/2023 (Brasil, 2024) made significant progress in its processing on December 10, 2024, when, after an intense period of confronting the big tech *lobby*, it was approved by the Federal Senate. Since its original version, the normative text has adopted a twofold approach in the regulation of this technology, which is intended to classify its uses in the light of the risks they carry (*risk-based approach*) and to ensure a series of rights to those affected by it (*rights-based approach*) (Nunes, 2023).

Thus, the document allows AI agents (developers, distributors, and applicators) to¹⁴ carry out preliminary assessments (art. 12) to catalog their respective systems as excessive risk (art. 13) or high risk (art. 14), if they perform any of the purposes listed, or, residually, as low or moderate risk.

The category of excessive risk prohibits the development, implementation and use of systems that affect natural persons or groups with the aim of: a) instigating or inducing their behavior, resulting in damage to their own health, safety or other fundamental rights or those of third parties; b) exploit any of its vulnerabilities, with similar purposes; c) to assess their personality traits, characteristics or past behaviours, criminal or not, to assess the risk of committing crimes, infractions or recidivism; and d) to enable the production or dissemination, or facilitate the generation of materials illustrating the sexual abuse or exploitation of children and adolescents (art. 13, I, paragraphs a, b, c and d).

In addition to the prohibitive hypotheses, the following are added: a) the applications of technology by the government to evaluate, classify or rank individuals, based on their social behaviors or personality attributes, by means of a *universal score*, which conditions access to goods and services and public policies, in an illegitimate or disproportionate manner (art. 13, II); b) autonomous weapons systems (SAA) (art. 13, III); and c) biometric identification systems at a distance, in real time and in spaces accessible to the public (art. 13, IV).

Considered as the central object of this scientific article under the guise of public security, these monitoring tools are only authorized to be implemented in four scenarios (art. 13, IV, paragraphs a, b, c and d):

¹⁴ Carrying out a preliminary assessment is only mandatory for developers of general-purpose or generative AI systems (art. 29).

Article 13. The development, implementation, and use of AI systems are prohibited: [...]

IV – in biometric identification systems at a distance, in real time and in spaces accessible to the public, except in the following cases:

- a) instruction of a criminal investigation or proceeding, upon prior and motivated judicial authorization, when there are reasonable indications of authorship or participation in a criminal offense, the evidence cannot be made by other available means and the fact investigated does not constitute a criminal offense of lesser offensive potential;
- b) search for victims of crimes and missing persons, or in circumstances involving serious and imminent threat to the life or physical integrity of natural persons;
- c) flagrante delicto of crimes punishable by deprivation of liberty of more than two (2) years, with immediate communication to the judicial authority;
- d) recapture of escaped defendants and compliance with arrest warrants and restrictive measures ordered by the Judiciary.

The Bill teaches that these permissions must be proportional and strictly necessary to meet the public interest, safeguarding the due process of law, judicial control and the principles and rights listed in its provisions, and, where applicable, the dictates of the General Law for the Protection of Personal Data (LGPD), especially with regard to the fight against discrimination and the need for review of algorithmic inference by the responsible public agent (art. 13, Paragraph 2).

In turn, the high-risk classification covers a dozen designations and contexts of uses allowed for the invention (art. 14), which will require additional governance measures (art. 18) and the elaboration of an algorithmic impact assessment (art. 25) by the developer and/or applicator who introduces or puts the intelligent system into circulation on the market¹⁵. Among the hypotheses, there is the use of identification devices and biometric authentication for the recognition of emotions (art. 12, XI), except for those with the exclusive purpose of confirming a specific natural person.

Persons impacted by surveillance tools in the field of public security may face difficulties in exercising the rights listed by the Bill. The lack of transparency in the implementation of AI raises concerns about the distortion of precepts alluding to information about interactions with such systems (art. 5, I) and the explanation of the decisions, recommendations, or forecasts taken by them (art. 6, I).

As a result, the non-compliance with both has the effect of affecting the challenge and the request for review of the outcome offered by the algorithm (art. 6, II), equally threatened by the complexity inherent to its architecture. Despite the fact that the

¹⁵ While additional governance measures must be taken jointly by the developer and the applicator of an AI system (art. 18), the algorithmic impact assessment must be produced, alternatively, by one or the other (art. 25).

participation of human beings in the decision-making process has been preserved, the various episodes of "false positives" narrated so far show the insufficiency of the supervision exercised over the machine, which can undermine protection against direct and indirect discrimination (art. 5, III).

Despite the warnings of experts pointing out the unfeasibility of face identification solutions in view of their low success rates and the high costs for their hiring, the normative proposal chose to follow a different path to the ban.

Taken as the central inspiration of PL No. 2,338/2023, the *Artificial Intelligence Act* (AI Act) (European Union, 2024) inaugurated the regulation of artificial intelligence in the world. In its Recital No. 17, the AI Act establishes a double classification for remote biometric identification systems, which can operate: a) "in real time", when the steps of capturing biometric data, comparison with the reference database and identification occur instantaneously, almost instantaneously or without relevant delays; and b) "deferred", characterized by the existence of a considerable time interval between the capture and the subsequent stages of comparison and identification.

In "real-time" systems, the use of collected materials (e.g. images or videos from cameras) takes place "live" or "almost live". In "deferred" systems, the content to be analyzed is previously captured, for example, from "closed-circuit television cameras or private devices".

As the European legislator points out, the above species are not to be confused with biometric verification technologies, which usually use facial recognition for authentication purposes (e.g. attesting that people who try to access a service are really who they claim), given their lesser potential harm to individual fundamental rights and the active participation of the subjects who are identified throughout this process.

The latest version of the proposal under discussion qualifies the use of remote biometric identification systems "in real time" and in spaces accessible to the public for the purposes of law enforcement as a prohibited artificial intelligence practice¹⁶, only authorized for the indispensable achievement of three specific purposes.

¹⁶ The reasons for the ban are listed with unparalleled clarity in Recital 32 of the document: "The use of AI systems for the "real-time" remote biometric identification of natural persons in publicly accessible spaces for law enforcement purposes is **particularly intrusive on the rights and freedoms of the persons concerned, as it can affect the private lives of a large part of the population, give rise to a sense of constant surveillance and indirectly dissuade the exercise of freedom of assembly and other fundamental rights.** Technical inaccuracies of AI-systems designed for remote biometric identification of natural persons can lead to **biased results and have discriminatory effects.** These possible biased outcomes and discriminatory effects are particularly relevant with regard to age, ethnicity, race, gender or disability. In addition, the immediate

Art. 5 Prohibited AI practices

1. The following AI practices shall be prohibited: [...]

(h) the use of "real-time" remote biometric identification systems in publicly accessible spaces for law enforcement purposes, unless and to the extent that such use is strictly necessary for one of the following purposes:

(i) the targeted search for specific victims of abduction, trafficking in human beings or the sexual exploitation of human beings, as well as the search for missing persons;

(ii) prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a actual and present or actual and foreseeable threat of a terrorist attack;

(iii) the location or identification of a person suspected of having committed a criminal offence for the purpose of conducting a criminal investigation, prosecuting or imposing a criminal penalty for any of the offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or detention order of a maximum term of at least four years.

Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 as regards the processing of biometric data for purposes other than law enforcement.

The discipline of the Old Continent stands out by enumerating the types of crimes that give rise to the search for victims, by adding the scenarios of threats to natural persons and terrorist articulations to the list of authorized uses of the tool, and by establishing that the location or identification of suspects touches on crimes punishable by sentences of not less than four years in the affected Member State¹⁷.

According to its Recital No. 33, strictly necessary uses are based on an "important public interest" that outweighs any risks that may exist. In these exhaustive hypotheses, in addition to the scope of confirming the identity of the individual concerned, there must be a consideration of the nature of the situation that gives rise to the use of the system and the consequences arising from it for the rights and freedoms of all affected persons (article 5, paragraph 2, paragraphs "a" and "b").

Each use of biometric systems for law enforcement purposes¹⁸ does not dispense with the prior authorization of an independent judicial or administrative authority — only waived in scenarios of justified urgency, provided that it is subsequently requested within 24 hours — which must show that it was necessary and proportionate for the achievement

impact and limited opportunities for additional controls or corrections with regard to the use of such systems operating in real time entail increased risks to the rights and freedoms of the persons concerned in the context of, or affected by, law enforcement authorities." (emphasis added).

¹⁷ Also noteworthy is the important prohibition on intelligent solutions that originate or expand facial recognition databases through the random collection of images of faces from the *Internet* or closed circuit television (art. 5, paragraph e).

¹⁸ Each Member State may establish total or partial authorisations for the use of biometric identification systems remotely "in real time" and in publicly accessible spaces for law enforcement purposes, subject to the provisions of Article 5(1)(h), (2) and (3). It is even allowed that national laws provide for more restrictive rules in relation to the matter (art. 5, no. 5).

of one of the aforementioned purposes and that "it is limited to what is strictly necessary with regard to the period of time and the geographical and personal scope" (art. 5, no. 3).

All use must be notified to the national market surveillance and data protection authorities, which are responsible for preparing annual reports to be addressed to the European Commission, which will compile and publish these productions, not including sensitive operational data on law enforcement activities in them (art. 5, paragraphs 4 to 7).

Once the European diploma has come into force, it remains to be seen whether, in future votes on PL No. 2,338/2023, care will be taken in disciplining AI — especially regarding facial recognition systems, which are regulated in detail — ensuring compliance with national peculiarities in the application of the disruptive technology.

CONCLUSION

The recent expansion of facial recognition systems in Brazil, especially remote biometric identification solutions in the field of public security, generates justified concerns linked to their harmful potential in relation to historically disadvantaged individuals or groups, such as black people, women, and transgender people. Underrepresented in the datasets used during the learning of the algorithms, these segments become the target of machine errors that can result in wrongful detentions and serious human rights violations.

Unfortunately forgotten during the training of these intelligent apparatuses, the individuals who are part of these collectivities are only remembered during their questionable application, often affected by low correlation rates, as illustrated by the experiences of video surveillance in the Copacabana neighborhood in Rio de Janeiro. Add to this the possibility of remaining in loops of punishability, as they become the main recipients of consecutive AI systems (e.g. data from a young black man arrested for a minor offense being fed back into a recidivism prediction system), as Cathy O'Neil elucidates.

The short story "In the Penal Colony", by Franz Kafka, acts as an interesting parallel to these peculiar digital machines, which, like the island's torture apparatus, have an obscure functioning, capable of generating disproportionate or unreasonable sanctions, facing the growing resistance of research institutes aware of their possible losses (e.g. high costs, algorithmic discrimination, lack of fairness in public-private relations, and leaks of sensitive data).

It is up to scholars of the subject, factually elevated to the position of the Traveler, to explore the intricacies of this inhospitable digital colony, characterized by an uninterrupted surveillance that becomes feasible by the pseudo-spontaneous concession of data by users, now converted into commodities — but with different prices for black citizens, as Deivison Faustino and Walter Lippold well remember.

Although the advanced European regulation around artificial intelligence has not adopted the path of banning facial recognition technologies at a distance and in public spaces for law enforcement purposes, the document stands out for clarifying in detail what are their permitted and prohibited uses and clearly categorizing the various existing analysis tools.

In future debates in the Chamber of Deputies aimed at optimizing the current wording of PL No. 2,338/2023, reflections on the positive aspects of the foreign proposal and the potential negative facets of surveillance tools are indispensable.

REFERENCES

1. BEIGUELMAN, Giselle. **Image Politics**: Surveillance and Resistance in the Datasphere. 2. ed. São Paulo: Ubu Editora, 2023.
2. BRAZIL. **Bill No. 2,338**, of December 10, 2024. It provides for the development, promotion and ethical and responsible use of artificial intelligence based on the centrality of the human person. Available at: <https://legis.senado.leg.br/sdleggetter/documento?dm=9881643&ts=1735605226813&disposition=inline>. Accessed on: 28 jan. 2025.
3. BUOLAMWINI, Joy; GEBRU, Timnit. **Gender Shades**: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Fairness, Accountability, and Transparency. Proceedings of Machine Learning Research 81:1–15 (2018). Available at: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. Accessed on: 14 Feb. 2024.
4. OPEN LETTER: PCR's facial recognition policy threatens the rights of all citizens. **IP.rec**, Recife, 18 nov. 2021. Available at: <https://ip.rec.br/blog/carta-aberta-politica-de-reconhecimento-facial-da-pcr-ameaca-direitos-de-todos-os-cidadaos-e-cidadas/>. Accessed on: 15 Feb. 2024.
5. CEBRIAN, Fabiana S. P. Faraco *et al.* **Technological Radar No. 2**: Biometrics and Facial Recognition. ANPD: Brasília/DF, 2024. Available at: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/radar-tecnologico-biometria-anpd-1.pdf>. Accessed on: 20 Aug. 2024.
6. COELHO, Henrique; NASCIMENTO, Rafael; ALVES, Raoni. Woman arrested after facial recognition is released; An arrest warrant had already been served. **G1**, Rio de Janeiro, 4 jan. 2024. Available at: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/01/04/mulher-presa-apos-reconhecimento-facial-e-solta-mandado-de-prisao-ja-tinha-sido-cumprido.ghtml>. Accessed on: 12 jan. 2024.
7. FAUSTINO, Deivison. **Digital colonialism** [electronic resource]: by a hacker-fanonian critique / Deivison Faustino, Walter Lippold. 1. ed. São Paulo: Boitempo, 2023.
8. PHOTO of movie star Michael B. Jordan appears on wanted list by Ceará police. **G1 CE**, [S.l.], 7 jan. 2022. Available at: <https://g1.globo.com/ce/ceara/noticia/2022/01/07/astro-do-cinema-michael-b-jordan-aparece-em-lista-de-procurados-pela-policia-do-ceara.ghtml>. Accessed on: 22 Aug. 2024.
9. FRANÇANETTO, Milton Pereira de; EHRHARDT JR., Mark. **The Risks of Algorithmic Discrimination in the Use of Artificial Intelligence Applications in the Brazilian Scenario**. Luso Brasileira Legal Journal-, v. 3, 2022. Available at: https://www.cidp.pt/revistas/rjlb/2022/3/2022_03_1271_1318.pdf. Accessed on: 14 Feb. 2024.

10. HAN, Byung-Chul. **Infocracy**: digitalization and the crisis of democracy. Petrópolis, RJ: Vozes, 2022.
11. KAFKA, Franz. **In the Penal Colony** - illustrations by Lourenço Mutarelli; translation by Petê Rissatti. Rio de Janeiro: Editora Antofágica, 2020, p. 27.
12. LISBOA, Vinícius. Cameras of the City Hall of Rio in Lapa will have facial recognition. **Agência Brasil**, Rio de Janeiro, 19 Jan. 2024. Available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2024-01/cameras-da-prefeitura-do-rio-na-lapa-terao-reconhecimento-facial#:~:text=O%20sistema%20de%20videomonitoramento%20da,milh%C3%B5es%2C%20entre%20equipamentos%20e%20softwares>. Accessed on: 20 jan. 2024.
13. MARTINS, Helena. The adoption of vigilante technologies without debate. **O Povo**, Fortaleza, 16 Apr. 2024. Available at: <https://mais.opovo.com.br/jornal/opinioao/2024/04/16/helena-martins-a-adocao-de-tecnologias-vigilantistas-sem-debate.html>. Accessed on: 18 Aug. 2024.
14. MARTINS, Helena *et al.* **From the construction of a surveillance infrastructure to the introduction of facial recognition in Ceará** [electronic book]. Rio de Janeiro : CESeC, 2024. Available at: <https://drive.google.com/file/d/1sVRHlIdEVbFMDvaqkPpW29hdv3eTSEYc/view>. Accessed on: 19 Aug. 2024.
15. 'FEAR, frustrated and embarrassed', says man mistakenly detained in stadium after facial recognition system error. **G1**, [S./], 21 Apr. 2024. Available at: <https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml>. Accessed on: 22 Aug. 2024.
16. Monitoring METHODOLOGY. **The Panopticon**, [S./], 2024. Available at: <https://docs.google.com/document/d/1CM4P68Npyr6zR2myvjo1ulqJtpdoqOuPam8TiFah7yl/edit>. Accessed on: 14 Feb. 2024.
17. NUNES, Dierle. Regulation of artificial intelligence and use of subliminal techniques. **Conjur**, [S./], 26 set. 2023. Available at: <https://www.conjur.com.br/2023-set-26/dierle-nunes-regulacao-ia-uso-tecnicas-subliminares/>. Accessed on: 14 Feb. 2024.
18. NUNES, Pablo. **A Rio of selective eyes** [electronic book]: use of facial recognition by the Rio de Janeiro police. Rio de Janeiro : CESeC, 2022.
19. O'NEIL, Cathy. **Algorithms of mass destruction** : how big data increases inequality and threatens democracy / Cathy O'Neil; translated by Rafael Abraham. -- 1st ed. -- Santo André, SP: Editora Rua do Sabão, 2020.
20. PIMENTEL, Alexandre Freire. **Treaty on Technological Law and Process** – (Vol. 01) – Algorithmic Surveillance and Neocolonization; The Digital Control of the Masses and Risks and Attacks on Democracy (Including the episode of January 8, 2023). Publius Publium: Recife, 2023.

21. RECIFE wins the first of 108 digital clocks. **Recife City Hall**, Recife, 18 nov. 2022. Available at: <https://www2.recife.pe.gov.br/noticias/29/12/2022/recife-ganha-o-primeiro-de-108-relogios-eletronicos-digitais>. Accessed on: 15 Feb. 2024.
22. RIBEIRO, Aline. I lived to tell it: 'They mistook me twice for a fugitive at the same party', says young man targeted by facial recognition. **O Globo**, São Paulo, 5 jan. 2023. Available at: <https://oglobo.globo.com/brasil/noticia/2024/01/05/vivi-para-contar-me-confundiram-duas-vezes-com-uma-foragida-na-mesma-festa-diz-jovem-alvo-de-reconhecimento-facial.ghtml>. Accessed on: 12 jan. 2024.
23. SALEME, Isabelle. Two of the four arrested for facial recognition in Rio de Janeiro are released. **CNN Brasil**, [S./], 5 jan. 2024. Available at: <https://www.cnnbrasil.com.br/nacional/dois-dos-quatro-presos-por-reconhecimento-facial-no-rio-de-janeiro-sao-liberados/>. Accessed on: 12 jan. 2024.
24. SILVA, Heloísa Helena. Facial recognition algorithms and discrimination against transgender people. **Internet and Society Magazine**, v. 2, n.2, Dec/2021, p. 47-66. Available at: <https://revista.internetlab.org.br/wp-content/uploads/2022/03/Algoritmos-de-reconhecimento-facial-e-as-discriminacoes-contra-pessoas-transexuais.pdf>. Accessed on: 14 Feb. 2024.
25. EUROPEAN UNION. **Regulation (EU) 2024/1689 of the European Parliament and of the Council** of 13 June 2024 creating harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Brussels, 13 June 2024. Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689. Accessed on: 22 Aug. 2024.