Latin American Human Rights Studies, v. 1 (2021)

The Problem of Automated Facial Recognition Technologies in Brazil: Social Countermovements and the New Frontiers of Fundamental Rights

Michel R. O. Souza[1]
Rafael A. F. Zanatta[2]

Abstract: This article analyzes the characteristics of automated facial recognition technologies and their response by civil society organizations in Brazil. We analyze two arguments in this debate: the endemic bias argument, which seeks to correct unjust and potentially racist consequences, and the endemic oppression argument, which identifies a set of facilitators of systematic violation of fundamental rights. We present the concept of countermovements to explain the possibilities of legal contestation of the dissemination of facial recognition and explain how the argument about recognition can move from the logic of bias to that of oppression, with the possibility of changing the regulation to ban this technology in certain uses.

Keywords: Facial Recognition Technology. Fundamental Rights. Social Movements. Brazil.

Introduction

The use of automated facial recognition technologies (AFRTs) has exploded worldwide in the past decade. We have witnessed the expansion of technology firms dedicated to public security and the increase of privatization of functions of the State to the private sector, such as the surveillance of public spaces

[1] Lawyer at the Brazilian Institute of Consumer Defense (Idec). He holds a BA in Law from the State University of Maringá (UEM), an MA in Law from the University of São Paulo (USP), an LL.M. in Comparative Law and Economics from the International University College of Turin (IUC), and a PhD in Law from USP.

[2] Director of Data Privacy Brasil Research Association. He is a PhD candidate at the Institute of Energy and Environment of the University of São Paulo (USP) and holds an MA in Law from USP, an LL.M. in Comparative Law and Economics from the International University College of Turin (IUC) and a BA in Law from the State University of Maringá (UEM).

and the prevention of crimes. From the economic perspective, there has been a price decrease of such technologies and a tremendous expansion of these markets.

On the other hand, automated facial recognition technologies have been strongly challenged on legal and ethical grounds. One major argument against AFRTs is the endemic problem of *bias*, which is connected to the lack of diversity of datasets trained to perform computerized activities of “recognition” and the racialized consequences in terms of activities of the police and the criminal system.

In the United States of America, the National Institute of Standards and Technology’ analyses dozens of facial recognition algorithms used by 99 developers found a variety of accuracy rates among them, higher rates of false positives in Asian and African American faces relative to those of Caucasians (EATON, 2020).

According to the “bias argument”, AFRTs are flawed and, at the current level of its technological development, should not be allowed because of their impact on systemic racism and injustice in contemporary societies, especially those that were based in slavery and profound racial discrimination, such as the USA and Brazil.

Because of the current level of errors and flaws and the impact on non-Caucasians in terms of civil liberties, AFRTs should be paused for a while. This is one of the reasons IBM[3] wrote a letter to the Congress in June 2020, suggesting the following:

> IBM no longer offers general purpose IBM facial recognition or analysis software. IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values and Principles of Trust and Transparency. We believe now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies (IBM, 2020).

[3] International Business Machines (IBM) Corporation is an American multinational technology and consulting company headquartered in Armonk, New York, with more than 350,000 employees serving clients in 170 countries. IBM produces and sells computer hardware, middleware and software, and provides hosting and consulting services in areas ranging from mainframe computers to nanotechnology.

The “bias argument” was deeply enforced after the tragic death of George Floyd and the mass global protests against racism and police abuse in the United States of America and other countries.[4]

It became clear the persistent problem of police brutality, lack of police accountability and inequality and racism in the use of power. As argued by Alex Najibi in the essay *Racial Discrimination in Face Recognition Technology*, “even if accurate, face recognition empowers a law enforcement system with a long history of racist and anti-activist surveillance and can widen pre-existing inequalities” (Najibi, 2020).

Another major argument, formulated by philosopher Evan Selinger and law professor Woodrow Hartzog, is connected to the repressive power of AFRTs and the incompatibility with a system of civil liberties in contemporary society. According to these authors, thanks to advances in artificial intelligence, proliferating photography, diminishing costs of storing big data sets in the cloud, and cheap access to AFRTs, this type of technology has become the most dangerous surveillance tool ever invented. In 2018, Selinger and Hartzog wrote an influential piece entitled *Facial Recognition Is The Perfect Tool for Oppression*, in which they claimed:

> we believe facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented. It’s the missing piece in an already dangerous surveillance infrastructure, built because that infrastructure benefits both the government and private sectors. And when technologies become so dangerous, and the harm-to-benefit ratio becomes so imbalanced, categorical bans are worth considering. The law already prohibits certain kinds of dangerous digital technologies, like spyware. Facial recognition technology is far more dangerous. (...) Surveillance conducted with facial recognition systems is *intrinsically oppressive*. The mere existence of facial recognition systems, which are often invisible, harms civil liberties, because people will act differently if they suspect they’re being surveilled. Even legislation that holds out the promise of stringent protective procedures won’t prevent chill from impeding crucial opportunities for human flourishing by dampening expressive and religious conduct (SELINGER & HARTZOG, 2018).

[4] The George Floyd protests are an ongoing series of police brutality protests that began in Minneapolis in the United States on May 26, 2020. The civil unrest and protests began as part of international responses to the killing of George Floyd, a 46-year-old African-American man who was killed during an arrest after Derek Chauvin, a Minneapolis Police Department officer, knelt on Floyd's neck for nearly eight minutes as three other officers looked on and prevented passers-by from intervening. In the course of the George Floyd protests, more than 19 people were killed and more than 14.000 people were arrested.

For them, it is not a matter of regulation and correcting the biases of AFRTs. Even if we improve those technologies and eliminate (at the best scenario) the endemic problem of racial injustice, AFRTs will still be intrinsically oppressive and incompatible with human flourishing and the exercise of fundamental human actions.

According to Hans Jonas and Hannah Arendt, by allowing such technologies to exist, we become less human and fundamentally change social behavior. We also generate "due process harms", which "might include shifting the ideal from 'presumed innocent' to 'people who have not been found guilty of a crime, yet'" (SELINGER & HARTZOG, 2018).

According to this argument - which we might call *endemic oppression* in comparison with the *endemic bias* -, "since facial recognition technology poses a unique threat, it can't be contained by measures that define appropriate and inappropriate uses and that hope to balance potential social benefit with a deterrent for bad actors"[5].

It is not a matter of imposing data protection laws and defining legal grounds for data processing. For the authors, "the future of human flourishing depends upon facial recognition technology being banned before the systems become too entrenched in our lives" (SELINGER & HARTZOG, 2018). The legal consequence of this argument is using the law to prohibit one practice, such as it has occurred with landmines.[6] It moves beyond regulation and the desired effect of changing the behavior of public and private actors that are deploying AFRTs.

Based on this conceptual distinction (the argument of *endemic bias* and the argument of *endemic oppression*), we analyze the current debate in Brazil about

[5] We use the expression endemic in the sense that it is a negative condition regularly found among a certain area. The adjective is borrowed from biology but applied in this essay as a negative condition found in one socio-technical structure, such as the Automated Facial Recognition Technologies (AFRTs).

[6] Selinger and Hartzog (2018) establish a parallel with landmines that were invented in 1937 and proved to be a highly destructive technology. They mention the *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction*, known informally as the Ottawa Treaty, the Anti-Personnel Mine Ban Convention, or often simply the Mine Ban Treaty, aims at eliminating anti-personnel landmines (AP-mines) around the world. The Convention gained 122 country signatures when it opened for signing on 3 December 1997 in Ottawa, Canada.

automated facial recognition technologies (AFRTs) and the beginning of a debate that can move from *regulation* to *total ban*.

The article is structured as follows. First, we explain the concept of Automated Facial Recognition Technologies (AFRTs) on a general level. Second, we map emerging debates about AFRTs and the differences between arguments based on *bias* and *oppression*. Third, we map the contemporary debates about facial recognition in Brazil, with a special focus on the new legislation on personal data protection and the countermovements originated by the work of Brazilian civil society.

Through the analysis of the work of civil society organizations and Parliament, we argue that, in Brazil, legal discourses focus on problems of bias and potential abuse of the use of facial recognition technologies. There is still no systematic articulation of the endemic oppression argument and a countermovement of total banning of these technologies. We argue that, depending on the consistency of the development of arguments in the future, there may be an important argumentative transition in Brazil, moving from the regulation discourse to the ban discourse.

On the other hand, this movement faces two major problems: (i) the persistence of the discourse on the public security crisis in Brazil and (ii) the Brazilian federative arrangement, which concentrates the power of economic regulation and privacy legislation in the federal executive power.

1. Understanding how Automated Facial Recognition Technologies works

Automated facial recognition technologies (AFRTs) attempt to verify individuals using their faces. It is a computerized process that detects faces, extracts distinctive features from the faces, and compares the features to those accumulated in a database.

According to the Office of the Privacy Commissioner of Canada (2013), facial recognition aims to identify or authenticate individuals by comparing their faces against a database of known faces and looking for a match. The process can be simplified as follows.

First, the computer must find the face in the image. After this, it creates a numeric representation of the face based on the relative position, size and shape of facial features. Finally, this numeric "map" of the face in the image is compared to database images of identified faces, for example, a driver's license database.

For pedagogical purposes, we can claim that AFRTs involves the following steps:

a) An image is captured;

b) The computer program takes information about the face and transforms it into digital information, such as measuring the space between eyes, the shape of the chin, and the length of the nose (*e.g.* vectorial analysis);

c) A special algorithm is used to compare the test face and others in a database;

d) The program determines if the face matches another one in the database;

There are different methodological approaches to AFRTs in computer science. Some of the most sophisticated methods use "neural networks". According to the community Deep AI, a neural network is a "computational learning system that uses a network of functions to understand and translate a data input of one form into a desired output, usually in another form" (DeepAI, 2019).

Neural networks are just one of many tools and approaches used in machine learning algorithms. The neural network itself may be used as a piece in many different machine learning algorithms to process complex data inputs into a space that computers can understand.

As explained by computer scientists, machine learning techniques called deep learning are applied in conjunction with artificial neural networks in the recognition task. Machine learning performs the search for patterns in images. The search result is knowledge acquisition, which allows the necessary adaptation of the neural network to perform the recognition of images. The search for patterns is done through training, which is carried out several times on a database with sample images.[7]

[7] According to Rodrigo Chaves, today, "convolutional neural networks achieve the most accurate results compared to other models of neural networks" (CHAVES, 2019). Convolutional neural networks are well adapted for image classification, because they use the spatial structure of the image to perform the analysis.

AFRTs are the object of study for more than three decades in computer science (BARON, 1981; SAMAL & IYENGAR, 1992; CHELLAPPA *ET AL*., 1995).[8] There is a common feeling that AFRTs are here to stay. As explained by Lila Lee-Morrison in her book *Portraits of Automated Facial Recognition*, automated facial recognition is now increasingly being implemented in more mundane and everyday scenarios, changing our perception about the governance of our existence:

> AFR systems are used in our phones, at ATM machines, in office security systems, for the manning of cash registers in convenience stores and inside toilet-paper dispensers in public bathrooms. They are also used covertly, in CCTV and police cameras. In these new contexts, successful recognition by AFR is increasingly intervening in a complex negotiation between recognition, identity and access. Alongside the expansion of AFR into everyday contexts, there is a growing realization that we are becoming reliant on machines looking at us - and, most importantly, perceiving and interpreting us - and making decisions that, ultimately, govern our existence" (LEE-MORISON, 2019, p. 15-16).

In the book *Our Biometric Future: facial recognition technology and the culture of surveillance*, Kelly Gates argues that the terrorist attack of September 11 2001 was a turning point for the deployment of facial recognition technologies: "In the post-9/11 context, the technology emerged as an already existing, reliable, and high-tech solution to the newest, most pressing problem facing the nation" (GATES, 2011, p. 2).

What we witnessed in the past twenty years is "not a unified program", but "an interdisciplinary field of research and set of technological experiments", which is "part of the broader effort to automated vision - to create machines that can not only generate images, but also analyze the content of those images" (GATES, 2011, p. 3).

[8] Helen Chan Wolf was one of the pioneers in the field. In the 1960s, Wolf worked with other scientists at the Panoramic Research on teaching computers to recognize human faces. Early computer programs used humans to coordinate a set of features from images of faces and then a computer for the recognition. Wolf joined the Artificial Intelligence group at SRI International (then Stanford Research Institute) in 1966. In 1977, she developed Parametric Correspondence, a technique for matching images to a three dimensional symbolic reference map. The work of Robert Baron is also recognized as one of the pioneering studies in the field during the 1980s. Most of the techniques used nowadays are the evolution of the basic ideas developed in the past century.

For the military, state security and law enforcement agencies, these technologies are “uniquely suited to the development of smart surveillance, monitoring systems that perform the labor of surveillance with less human input and less need to rely on the perceptual capacities and analytical skills of human beings” (GATES, 2011, p. 3). On a general level, as argued by the author, the development of ARFTs is a matter of new divisions of *perceptual labor* between humans and computers.

ARFTs can also be explained by focusing on the differences between *identification* and *analysis of expression*. The analysis of expression is linked to the effort to program computers to recognize facial expressions as they form on and move across our faces.

As explained by Gates, “while facial recognition technology treats the face as a 'blank somatic surface' to be differentiated from other faces as an index of identity, automated facial expression analysis treats the dynamic surface of the face as the site of differentiation” (GATES, 2011, p. 152). In this approach, “the dimensions and intensities of facial movements are analyzed as indices of emotion and cognition, as a means of determining what people are thinking and feeling” (GATES, 2011, p. 152).

Writing ten years ago, the author noticed that “whereas facial recognition technology has already been integrated into some real-world surveillance and identification systems, automated facial expression analysis is still in a more nascent stage of development in computer science” (GATES, 2011, p. 153). That is not the reality anymore. As it will be argued in the following sections, the recognition of expressions has become popular in Brazil and has been the subject of legal proceedings and civil society confrontations. Techniques have spread and there are several companies operating in these markets.

2. The debate about facial recognition today: the impact of global discussions in Brazil

As explained by Evgeny Morozov and Francesca Bria in their report *Rethinking Smart Cities*, the expansion of AFRTs must be understood as part of a broader neoliberal program of decentralization of traditional public functions and creation of new markets that can be occupied by new technology firms (BRIA & MOROZOV, 2019). The public security and crime crisis is also an opportunity for business and contracts with the government. This economic expansion of AFRTs is followed by a growing feeling of opposition and resistance by the academia and organizations of the civil society.

Two letters from organized civil society illustrate this growing concern in Brazil, in connection with international movements such as those launched by organizations such as Fight for the Future, Privacy International and Epic.

In 2019, during the Internet Governance Forum in Berlin, the Coalition *Direitos na Rede* published an open letter from representatives of Brazilian civil society facing threats to the democratic, free and open internet in Brazil. In this letter, they noticed:

> The use of automated facial recognition systems by police is also growing in the country. These draft laws and surveillance policies call into question democracy and the rule of law by threatening citizens' fundamental rights and freedoms, such as privacy, self-determination, freedom of expression, equality and freedom of association. In addition, research has shown that automated systems and the use of algorithms reflect and reinforce approaches and prejudices about gender, race/ethnicity, and class in society. In Brazil, according to data published by the Safety Observatory Network, 151 people were arrested through the use of facial recognition technology in five regions in 2019 — 90% of them are black. It is well known that these technologies are also flawed and should not guide public safety policies. A study by the University of Essex in the United Kingdom looked at 42 cases of facial recognition and found that only 8 were successful, less than 20%" (COALIZÃO DIREITOS NA REDE, 2019).

In the following year, at the first virtual edition of the Internet Governance Forum, the same coalition of NGOs (*Direitos na Rede*) published an open letter about the rise of techno-authoritarianism, in which they argued:

> Unfortunately, initiatives such as the expedited deployment of facial recognition technologies and massive and disproportionate collection of personal data through the implementation of a centralized database have been a reality in the country during a scenario in which the Brazilian Data Protection Authority was still being discussed and

> implemented. By the end of 2019, a massive database containing biometric information and other categories of personal data of around 200 million brazilians was created by President Jair Bolsonaro. The main objectives of the database were simplifying data sharing between government departments and improving the provision of public services. This database, called Cadastro Base do Cidadão, will be operated by the Secretary of Digital Government at the Ministry of Economy and – depending on the data category – some information might not be subject to any access restrictions to Ministries and other Public Authorities" (COALIZÃO DIREITOS NA REDE, 2020).

We observe that the Brazilian letters do not directly address the issue of banning AFRTs, but are letters about "concerns", which point to the need of regulation. Differently, it was the performance of European organized civil society in 2019. At the initiative of the NGO *Quadrature du Net*, more than 80 organizations have asked for a ban on facial recognition technologies for public security purposes, in the following terms:

> Facial recognition is a uniquely invasive and dehumanizing technology, which makes possible, sooner or later, constant surveillance of the public space. It creates a society in which we are all suspects. It turns our face into a tracking device, rather than a signifier of personality, eventually reducing it to a technical object. It enables invisible control. It establishes a permanent and inescapable identification regime. It eliminates anonymity. No argument can justify the deployment of such a technology. Besides anecdotal convenience (using your face rather than passwords to log in online or unlock your phone), its only effective promises are to hand over to the State a power of total control over its population — which it will be tempted to abuse against political its opponents and certain populations. Because facial recognition for security and surveillance purposes is by essence disproportionate, it is pointless to entrust with the responsibility of case by case evaluation an authority which would, inevitably, fail to track its numerous new applications. This is why we ask you to ban any security and surveillance use of facial recognition" (APC, 2019).

More recently, with the hashtag "Reclaim your face" an european movement that brings together civil society organizations such as *Access Now, Article 19, Bits of Freedom, EDRi, Homo Digitalis* and others, was created to ask to ban biometric mass surveillance in Europe[9]. The movement asks for more transparency

[9] https://reclaimyourface.eu/.

and respect for humans, but also understands that "only a ban on biometric mass surveillance can protect us".

We will return to this discussion later (the variation between the *corrective argument* and the *complete opposition argument*), but it is important to note, right now, that the argument for a ban was not fully exposed by Brazilian civil society. So far, what has happened is a kind of construction of critical awareness on the subject, with a strong weight of the endemic bias argument.

In addition to civil society movements, a mobilizing axis has been the work of Personal Data Protection Authorities in the matter. As noticed by Ricardo Abramovay (2019), the French Data Protection Authority prohibited schools in Nice and Marseille from using AFRTs, while in the United States of America, cities like Berkeley, San Francisco and Oakland banned the use of AFRTs by police authorities. In October 2019, California enacted a 3-year moratorium on the use of facial recognition technology in police body cameras.[10]

The initiatives of highly specialized groups in digital rights were an important first step in shaping a public discourse on the subject. Recently, civil entities began a broader cultural approach, through documentaries and partnerships with the mainstream press. “Coded bias”, a documentary by Shalini Kantayya (2020), shows how Joy Buolamwini, a MIT Media Lab researcher and Algorithmic Justice League[11] founder, alerts US congressmen of the problems facial recognition and other Artificial Intelligence features that impacts our daily life, such as misidentifying women and dark-skinned faces, violating liberties, increasing racism, sexism and perpetuating inequalities.

Big tech companies, like Microsoft, Amazon and IBM, also moved to ask legislation for a responsible use of facial recognition technology. After those alerts in Congress hearings, Democrats like Alexandria Ocasio-Cortez and Republicans like Jim Jordan raised their voices and demanded federal regulation “before its use turned itself out of control” (EATON, 2020).

[10] See https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1215

[11] The Algorithmic Justice League is a digital advocacy organization based in Cambridge, Massachusetts. Founded by computer scientist Joy Buolamwini in 2016, AJL aims to raise awareness of the social implications of artificial intelligence through art and research. See https://www.ajl.org/

A few months before the pandemics of Covid-19 - and just three months after the progressive legislation of California - the case of the company Clearview AI shocked the world after the initial reports of Kashmir Hill from The New York Times.[12]

The small firm created the biggest dataset of biometric data globally (more than 3 billion images) by web scraping photos and videos that common people published online through YouTube, Flicker, Fotolog, Orkut, Facebook, Twitter and other social networking sites.[13] Clearview promises accuracy in the identification of suspects by crossing the databases of police officers with their own.

As reported by Kashmir Hill, more than 600 hundred police departments in the USA were using this technology secretly. Hundreds of them are still using the services of Clearview. While scholars in the USA recommended the ban of ClearView AI (HARTZOV, 2019), scholars in Europe considered that "the use of the Clearview app by Member States' law enforcement agencies appears to be deeply problematic with regard to the rights to privacy and data protection", considering the European Charter of Fundamental Rights and the General Data Protection Regulation (GDPR). European regulators considered a ban of AFRTs for five years in the beginning of 2020.[14] Due to the pandemics of Covid-19, the plan was cancelled. The European Commission recommends that member States should develop their own rules.[15]

In Brazil, the main critical reactions to the use of facial recognition technologies started after notorious cases of arrests of black people. In September 2019, a woman was wrongly approached by police officers in Salvador after a false positive in the system of facial recognition used by the metro (AMPARO, 2020).

[12] ClearView AI was founded by Hoan Ton That and Richard Schwartz, who worked with Rudolph Giuliani, former mayor of NYC. The company has received seed capital from Peter Thiel, one of the investors of Palantir (firm that offers support to the intelligence community of the USA).

[13] As argued by Benjamin Sobel (2020), the Clearview AI facial recognition scandal "is a monumental breach of privacy that arrived at a particularly inopportune time" in the USA, considering that the Ninth Circuit held, in the case *hiQ v. LinkedIn*, that scraping the public web probably does not violate the Computer Fraud and Abuse Act (CFAA).

[14] According to BBC, European regulators proposed that during the ban "a sound methodology for assessing the impacts of this technology and possible risk management measures could be identified and developed" (BBC, 2020).

[15] According to Christine Fisher, "the EU has been wary of the technology for years. It has considered ways to give citizens more control over their facial recognition data, and the EU's general data protection regulation (GDPR) prohibits the collection of sensitive biometric data that can be used to uniquely identify people. In a few instances, the tech has found its way into Europe, thanks to Google Photos face-grouping feature and security cameras in London's King's Cross" (FISHER, 2020).

In November 2019, as reported by the Network of Observatories of Public Security, 151 people were arrested in Brazil with the support of AFRTs, with 52% of the cases in the State of Bahia and 37% in the State of Rio de Janeiro (BARDON, 2019). 90% were black, 88% were men, with an average age of 35 and were mainly involved in drug trafficking (24%) and theft (24%).

As argued by legal scholar Thiago Amparo, problems with facial recognition are endogenous to the technology itself and must be discussed in the context of a racist society with structural inequalities - what Silvio Almeida calls "structural racism" (ALMEIDA, 2019).

Amparo claimed that "whether or not to allow facial recognition and, if so, how to do it is intrinsically linked to another question: on which shoulders does the police state lie? Information is power and, like all power, it can be racialized and must be controlled" (AMPARO, 2020).

In this sense, according to the author, the debate on the regulation of facial recognition technologies must go through a deeper discussion on anti-racism and on a fight to combat the oppression of these groups. The warning is serious, considering that on Black Awareness Day of 2020, a 40-year-old black man was beaten to death in a supermarket in Porto Alegre, by white security guards (CAMARGO, 2020). Brazil suffers from chronic problems of racism (RIBEIRO, 2019) that have an effect on the selectivity of violence by security agents.

While facial recognition technologies are spreading in the private[16] and public sectors[17], the public debate on the subject has grown steadily. In 2018, the

[16] In Brazil, with less than 300 hundred dollars one person can buy today a device for access control equipped with facial recognition technology. One of these devices, for example, runs on Linux, has a processor Quad Core (1,2G), 1G of capacity for memory and 8G for storage. This simple device, quite common in commercial buildings in cities like São Paulo and Rio de Janeiro, can support a list of 2.000 unique faces and has the capacity to store 200.000 registrations. With each passing year, these technologies become cheaper, while there is an increase in the processing capacity and storage capacity of biometric data. In addition, more and more companies have emerged specialized in providing this type of service to individuals and private organizations.

[17] Besides private and commercial use, AFRTs are increasingly being used by the public sector, especially by the transport sector in Brazil. In June 2019, the public company SPTrans announced that it had successfully blocked more than 300.000 cards ("Bilhete Único") that were used unlawfully by third parties. The technology works as follows. First, the passenger is photographed by a camera positioned on the validators whenever the ticket passes. The images are sent every day, when the bus stops running, to a server, where they are analyzed by a computer program in order to identify fraud. The database is also made available to security agencies, such as the police, when requested. By identifying incompatibility between the transport user and the ticket holder, the public company is able to block the

Brazilian Institute for Consumer Defense (Idec) filed the first public civil action against the use of facial recognition technologies in the São Paulo subway.[18]

The Institute obtained an injunction that forced the shutdown of the cameras that allowed the analysis of expressions of millions of passengers. In 2019, the Federal District Public Prosecutor's Office organized public hearings on the subject and invited experts from different sectors to discuss it.

The Internet Steering Committee also brought the matter up for discussion at the Privacy Seminar, the most important meeting on the protection of personal data in Brazil. In 2020, important organized civil society reports on the subject emerged: the report on facial recognition in the public sector, organized by the Igarapé Institute and Data Privacy Brasil, and the report on ethical recommendations for the use of facial recognition in the private sector, organized by the InternetLab and Idec.[19]

These factors - lawsuits, public events and research reports - were crucial for the debate to reach a robust level of analysis, drawing the attention of intellectuals not directly connected with the regulation of new technologies.

According to Helena Martins (2020), despite the criticisms, the use of facial recognition technologies tends to increase and counts, with that, with the support of the federal government.

An example given by Martins is Ordinance No. 793, of October 24, 2019, which regulates the use of money from the National Public Security Fund for the "promotion of the implantation of video monitoring systems with facial recognition solutions, by Optical Character Recognition - OCR, use of artificial intelligence or others". In Congress, bills seek to regulate the use of technologies, as will be explained below.

ticket. In this sense, facial recognition is used for a process of validating information about the identity of the ticket holder.

[18] As noticed by Helena Martins in a piece published at Le Monde Diplomatique, "the institute started working on the theme in 2018, the year it filed a lawsuit against Via Quatro, a concessionaire for Line 4 - Yellow of the São Paulo subway, because it was collecting sound and image data from transport users without them being informed or expressing consent. Screens were installed on the yellow line embarkation and disembarkation platforms that displayed advertising and recorded, by means of cameras, the reaction of passengers. Justice considered the practice illegal and ordered the suspension of collection. In 2019, such issues were more recurrent. Bárbara Simões reports that Idec questioned the facial recognition carried out by Hering, Carrefour, Itaú, Quot, 99 and even Dataprev" (MARTINS, 2020).

[19] We will explore these reports in detail in the following section.

3. Between data protection as a fundamental right, biometrics and facial recognition: the Congress and the Supreme Court

In Brazil, the debate on the theme related to biometrics is not new in the legislature. For example, in 2012, the Bill of Law 3.558/2012 was proposed by the Deputy Armando Vergílio (PSD/GO), which attempts to jointly regulate the use of biometric systems and personal data protection. The project ended up not gaining momentum and was shelved.

However, in 2015, Deputy Armando's son, Deputy Lucas Vergílio (Solidariedade/GO), proposed again the project that had been proposed by his father. This time, the Bill of Law 12/2015 intends to regulate biometric verification systems. The project text contains ten articles, which practically give the Executive the power to regulate the matter in its details.

The project also brings more general determinations, such as the prohibition of processing unauthorized personal data, except in the case of public interest, the regulation of systems that use biometric methods of identification and signature, in addition to bringing articles on the rights of users and administrative sanctions, penalties and civil for certain cases of non-compliance with the law.

With the enactment of the Brazilian Data Protection Law (LGPD) in 2018 (Law 13.709/2018), the issue took on new shapes.[20] As the LGPD excludes its application for the data processing carried out solely for the purposes of public security, national defense, State security, or investigative and prosecuting criminal offenses, a new opportunity for discussion about biometrics has opened up.

At the beginning of President Bolsonaro's government, an entourage of approximately 20 parliamentarians from his party, PSL, traveled to China to intensify trade relations between the two countries. Coincidentally, a few months after the trip, one of the deputies of that delegation, Deputy Bibo Nunes presented a bill to regulate AFRTs. The Bill 4612/2019, proposed by Deputy Bibo Nunes, aims to regulate the

[20] For a comprehension about the struggles behind the data protection law and its main features, see Zanatta (2015), Zanatta (2017), Bioni & Zanatta (2020).

development, application and use of facial and emotional recognition technologies, and other digital technologies aimed at identifying individuals and predicting or analyzing behaviors. Another Bill, 2537/2019, proposed by the Deputy Juninho do Pneu (DEM/RJ) also tried to regulate the issue, but with a more concise text. It only intends to approve the obligation to inform consumers about the conditions of facial recognition when entering commercial establishments.

These draft bills must be understood within a dynamic legal framework. The projects formulated since 2018 began to dialogue with the General Personal Data Protection Law (Law 13.709/2018). In addition, the country has initiated legislative discussions on the applicability of new rules for the use of data in public security and limitations on public authorities by recognizing the constitutional right to the protection of personal data.

Recently, the President of the Chamber of Deputies formed a Committee of Jurists to propose a criminal data protection legislation. The Committee was chaired by the ex Minister Nefi Cordeiro and included the participation of members such as Laura Schertel Mendes, Danilo Doneda, Davi Tangerino, Heloisa Estellita, Ingo Sarlet, Jacqueline Abreu, Jorge Octávio Lavocat Galvão, Juliana Abrusio, Tércio Sampaio Ferraz Júnior and Vladimir Aras.

The text presented by the Commission included the following axes: (i) scope of application of the Law; (ii) application conditions; (iii) principiological basis; (iv) rights and obligations; (v) information security; (vi) monitoring technologies; (vii) international data transfer and; (viii) the supervisory authority.

Gustavo Rodrigues, the coordinator of Iris, a digital rights NGO based in Belo Horizonte, concluded that the initial text of the project was a “very welcome contribution to the development of a legislative solution to this matter”, bearing in mind that:

> they are collected and processed on a massive scale by the State in the scope of investigation and prosecution of criminal offenses, but this treatment is not yet supported by a norm based on the idea of informative self-determination and consistent with the LGPD from a conceptual and terminological point of view” (RODRIGUES, 2020).

Along with these bills, the debate about the insertion of data protection as a fundamental right has also grown. For that, the Constitutional Amendment Project (PEC) n. 17/2019, by 30 Senators, to include the protection of personal data among the fundamental rights and guarantees and to establish the Union's exclusive power to legislate on the protection and treatment of personal data. The PEC was presented in March 2019 and passed in the Senate in July of that same year. Since then, it is being processed in the Chamber of Deputies.

The most relevant legal fact for the protection of personal data in 2020 was the judgment of Direct Actions of Unconstitutionality that questioned the federal government's attempt to share personal data from telecommunications operators to a public research agency, IBGE.[21]

The case, which became known worldwide, allowed the Supreme Court to analyze the constitutional nature of the right to the protection of personal data.[22] In a majority vote (10 votes to 1), the Court recognized that the attempt to share government data was unconstitutional due to the lack of established safeguards. The decision, however, was crucial to establishing a robust constitutional interpretation of the rights guaranteed in the LGPD. As explained by Bruno Bioni and Renato Monteiro:

> If the Brazilian Constitution's core value is the protection of human dignity, the protection it affords should go beyond the right to privacy in order to address other harmful challenges to an individual's existence, and not only harms to personality rights. Today, humanity can be hacked not only through granting access to data regarding our intimacy, or aspects of human personality that must be locked under seven keys. Recalling the work of philosopher Yuval Harari, Justice Gilmar Mendes argued that due to technological progress, any type of

[21] As described by Bioni and Monteiro: "A historic ruling of the Brazilian Supreme Court from May 07, 2020 describes the right to data protection as an autonomous right stemming from the Brazilian Constitution. By a significant majority, 10 votes to 1, the Court halted the effectiveness of the Presidential Executive Order (MP[1] 954/2020) that mandated telecom companies to share subscribers' data (e.g., name, telephone number, address) of more than 200 hundred million individuals with the Brazilian Institute of Geography and Statistics (IBGE), the country's agency responsible for performing census research. More important than the decision itself was its reasoning, which paves the way for recognizing the protection of personal data as a fundamental right, independent of the right to privacy, that already receives such recognition, in a similar fashion to the Charter of Fundamental Rights of the European Union".

[22] Direct Action of Unconstitutionality 6387, 6388, 6390 and 6393, Federal Council of the Brazilian Bar Association, Brazilian Social Democracy Party, Brazilian Socialist Party, Socialism and Liberty Party, Communist Party of Brazil v. Federal Government - Provisional Measure n. 954/2020, DJe. May 7th, 2020.

> data use that covers an extension of our individuality can pose a threat to human rights and fundamental freedoms. For this reason Justice Fux argued that just like the Charter of Fundamental Rights of the EU, the Brazilian Constitution should recognize the protection of personal data as an autonomous fundamental right, distinct from the right to privacy (BIONI & MONTEIRO, 2020).

As argued by Bruno Bioni *et al.* (2020), the decision might guide the future interpretation on this matter. The recognition of the fundamental right to the protection of personal data can guide new legislative discussions on the regulation of facial recognition technologies.

There is also the possibility that the argument surrounding the absence of safeguards and precautions may be mobilized to interrupt the operation of technologies that present failures, risks and social upheaval for population groups in Brazil.

According to the proportionality test proposed by Justice Luis Roberto Barroso, the use of personal data must be evaluated, on constitutional grounds, based on three tests: (i) the purpose of the processing is clearly specified and legitimate, (ii) the amount of data collected is limited to what is strictly necessary in relation to the purposes for which they are being processed, (iii) information security measures are adopted to avoid unauthorized third-party access.

The proportionality test can be mobilized in the future to demonstrate that a specific use is disproportionate at the constitutional level. This argument may gain strength in the coming years, especially due to the influence of decisions by other jurisdictions on the disproportionate and arbitrary use of facial recognition technologies.

The Brazilian Legislative debate on data protection, despite advancing with Bill proposals about facial recognition and Constitutional amendments on data protection as a fundamental right, remains with a real gap regarding the protection that is due for the processing of data for criminal purposes.

However, there is still no definition of who is the federative entity that can and should regulate these issues. Along with that, now the debate shall take into account that the Brazilian Supreme Court (STF) itself decided that there is a fundamental right to data protection, despite the inertia of the Brazilian government in adequately protecting citizens' rights, for example, with postponements of the LGPD term.

It is impossible to predict the dynamics of Congress on this matter. Considering the strength of the public safety bench, bills that seek to legalize and regulate the facial recognition market in public security are likely to continue. At the same time, the advancement of international activism and the fundamental right to the protection of personal data - recognized by the Supreme Court - can encourage the challenge promoted by civil society.

4. Countermovements in Brazil: understanding the dynamic nature of society and socio-technical structures

The concept of *countermovements*, strongly inspired by Karl Polanyi,[23] has been used by Mireille Hildebrandt and Julie Cohen to designate the dynamic way in which the social fabric, through its organizations and actors, reacts to processes of commodification and suppression of rights (HILDEBRANDT, 2020). As argued by Hildebrandt in her review of Cohen's seminal book *Between Truth and Power*:

> To come to terms with the systemic harms of information capitalism, we need to develop a keen eye to the precise way that legal rights, duties, immunities and powers are deployed and reconfigured to enable the move from a market to a platform economy - while also detecting the emergence of novel entitlements and disentitlements outside Hohfeld's framework. Steering clear of both technological and economic determinism, Cohen argues that the instrumentalization of legal institutions by powerful economic actors requires new types of Polanyian countermovements, to address and redress outrageous accumulation of economic power (HILDEBRANDT, 2020, p. 1).

Julie Cohen's work, which completely opposes the instrumentalization of law in defense of the lens of analyzes centered on power and the forms of contestation

[23] As explained by Gareth Dale in his book about Karl Polanyi: "as diagnosis is a prelude to prognosis, one may ask what the likely consequences of these destabilizing developments is. A countermovement is the short answer, but plotting its co-ordinates is no simple task. (...) the countermovement does make sense but as a heuristic that refers to the way in which, when the self-regulating market undermines the security of their livelihoods, human beings look to political ideas and organizations that claim to defend society against market excesses" (DALE, 2010, P. 220)

and reconstruction of law in its immersion in political economy, is central to this debate. In this perspective, Cohen presents a rich dialogue with Hildebrandt and the concept of “rights as affordance”, placing the process of social contestation as an element of codetermination of how we can be read by computers (HILDEBRANDT, 2015; COHEN, 2017). This concept is profoundly connected with countermovements.

In the Brazilian legal community, the concept of countermovements has been used to explain, for example, how, in the face of threats, such as the relaxation of the right to privacy due to the Covid-19 pandemic, organizations are able to react strategically and start legal battles with the capacity for some degree of social transformation (BIONI, ZANATTA, KELLER & FAVARO, 2020).

The concept of countermovement can be used to describe this dynamic nature of oppression and contestation, of threats to rights and restoration of those rights within contexts of affordances and sociotechnical structures mediated by computerized processes.

If, on the one hand, the digital economy has caused the expansion of the surveillance and public security markets, in the process of commodification of personality traits (in addition to the commodification of work, land and money, as Karl Polanyi had denounced), on the other hand, civil society has reacted through challenges, new legal discourses, new activism strategies and disputes over digital rights.

We describe below how this movement has occurred in Brazil in the past two years and its importance in thinking about the affirmation of fundamental rights in the face of the expansion of facial recognition technologies.

4.1. Idec/ViaQuatro Class Action

In 2018, the Brazilian consumer NGO Idec filed a class action against the public transport service concessionaire for one of São Paulo's private metro line 4 (Four - Yellow), ViaQuatro, for installing facial recognition cameras for ad purposes.

The judge in the case gave an injunction for ViaQuatro to stop collecting user data. The company followed the judge's orders and did not appeal the injunction.

The case is important because it discusses consumer data protection to consumers/metro users, biometric issues and consumer information, without having the LGPD in force, with a constitutional basis with other laws, such as the consumer law and public service users protection law.

Although the class action isn't over yet, other Civil Society Organizations are supporting the case, such as the participation of Instituto Alana (Brazilian NGO for children's rights) as *amicus curiae* and the Consumer Public Defense. Other Civil Society Organizations, the Institute for Research on Internet and Society, from Belo Horizonte, Minas Gerais, (IRIS) and Access Now, filed expert opinions in the case.

After analyzing the class action and documents from ViaQuatro' Interactive Doors System, Iris (TEOFILO *et al.,* 2019) stressed that capturing user reactions to advertisements through cameras at stations ViaQuatro violates the Federal Constitution, the rights of Consumers and Users of Public Transport, as well as the rights of protection of personal data and rights of consumers by, through the Interactive Doors service.

Iris identified problems concerning anonymization of the data and problems even if the data is anonymized, such as lack of adequacy between means and ends; lack of the duty to inform and consumer's freedom of choice and manifestly excessive advantage concerning the hidden price of the service provided.

Iris also concluded that "it is crucial that the decision on the case takes into account the pillars of protection against automated treatment and those concerning self-determination, both within the framework of constitutional and consumer rights, and the logic of existing sparse data protection rules, such as the Internet Bill of Rights".

Access Now, a global civil society organization dedicated to defending and extending the digital rights of users at risk, agrees with Iris expert opinion and concluded that Digital Interactive Doors system illegally collects, stores, and processes sensitive biometric data about passersby.

Access Now shows two additional concerns. One that the facial categorization system "makes invalid inferences about the private emotional life of passersby, and makes decision about what advertisement to show them based on these invalid inferences", that subjects users to "invasive surveillance and judgement of their inner emotional life, and had no opportunity to opt out of or to deny consent to such processing of their data and did not receive clear information about the system".

The second concern is that gender categorization by the DID system forcibly assigns gender systematically undermining "the rights of non-binary and trans people who do not conform to the binary conception of gender which underlies its functioning" (ARROYO & LEUFER, 2020).

4.2. The DPU/Metro probation case

The other case also included Sao Paulo's Metro. The Metro started in 2019 a contracting process for the revitalization of the metro security system, with the forecast that this system will use AFRTs. Again, Idec asked for information about a bidding of facial recognition cameras for the Metro's public lines.

After not receiving enough information about the AFRTs used in the case, Idec, together with Sao Paulo's and Brazil's Public Defensor Office and NGOs Intervozes, Article 19 Brazil and Human Rights Lawyers Collective (CADHu), filed an action for proof production that wanted to know how passengers' biometric data will be collected and treated by facial recognition systems.

Among the questions that are to be responded are: the way users' personal data will be collected and processed by the Metro; the databases used as reference; the protocols implemented in case a suspect is identified; the trust and security specifications used and the measures implemented to avoid data leaks. In summary, the action seeks consistent information about how the initiative responds to the principles.

Metro answered with the documents. However, the organizations' analysis is that Metro did not take into account the risks that facial recognition has, and did not have an impact assessment about it, concluding that the technology is expensive, inefficient and dangerous.

4.3. The Senacon fine in the sanctioning administrative process in a shopping mall

In August 2020, the Brazilian National Consumers' Secretary of the Ministry of Justice (Senacon) applied a fine to the Brazilian clothing retailer Hering has been convicted for the use of facial recognition technologies without consumer consent.

The case started with Idec’s notifying the company in 2019 to obtain further information after acknowledging the implementation of facial recognition cameras in one of its stores in São Paulo. After that, the Secretariat opened an administrative sanctioning process.

In addition to notifying the company to receive further clarification, the NGO Idec also acted as a third party interested in the process, having submitted statements and opinions to assist Senacon in judging the case.

The technology was used to analyze consumers' reactions and outline a profile of them, regardless of the lack of clear and adequate information and the absence of consumers' consent. The legal basis is the Brazilian Constitution, Consumer Defense Code and Civil Code. The company was convicted by Senacon for abusive practices, violation of the right to information and to the personality rights and now have to pay a fine to the Diffuse Rights Defense Fund (FDDD).

4.4. Reports and critiques from social movements in Brazil

As argued before, since 2018, metro, stores, airlines, churches, universities, police departments and even social security are using AFRTs in Brazil. Along with this exponential growth, organized civil society and academia have turned their attention to discussing the limits for the use of technology, as well as systematizing the places where technology is used and individual cases of injustice and discrimination.

In summary, we can list the reactions in three fields that intertwine: (i) production of knowledge and alert to the population; (ii) monitoring of cases of injustice linked to facial recognition; (iii) judicial and administrative sanction cases.

In middle 2019, Pablo Nunes and Bruno Sousa, from the Center for the Study of Security and Citizenship (CESeC), from Cândido Mendes University, created "O Panoptico"[24], a project to monitor the adoption of facial recognition systems by public security authorities in Brazil. Recently, the Panoptico Project adopted a focus on revealing adoption cases in Brazilian states and municipalities, in addition to presenting the role of governments and companies in financing and offering this technology.

It also aims to communicate comprehensively in social media[25] about the risks of using facial recognition and its biases for the black population. In early 2021, Nunes published a long essay entitled "The Algorithm and the Racism of Everyday Life", in which he called for something different than the correction of bias. For him, AFRTs should be paused because of major structural problems of police violence that are directly reinforced by the use of these technologies:

> Without any kind of control, with the active participation of the federal government in the financing of this type of use of technology by the police, we are moving towards having a facial recognition camera on every street and corner of the country. A brake on this process is necessary so that we can deeply discuss the risks and potentials of this technology for the population, especially the black population, which has once again been the preferred victim of the "exempt" algorithms" (NUNES, 2021).

Scholars like Ana Carolina Lima and Tarcizio Silva created AqualtuneLab[26], a collective dedicated to inserting the topic of race in discussions on topics involving the use of technology, such as its functions in the legal system (public

[24] https://opanoptico.com.br/sobre/
[25] https://twitter.com/opanopticobr
[26] https://aqualtunelab.com.br/

and private surveillance), data protection policies, biometric identification, security in internet, mobile apps and social media.

Recently, Coding Rights (2021) published the report *Facial recognition technologies in the verification of trans identities* (SILVA & VARON, 2021). Coding Rights also produced *From Devices To Bodies*, a series of mini-documentaries in partnership with Heinrich Böll Brazil, that brings important conversations with women and non-binary people, researchers who aim to broaden debates about the implementation of biotechnologies and digital technologies that work based on the collection of data about the bodies.

The second episode, "Facial recognition: race, gender and territory", discussed the AFRT in the political context, with a conversation between the researcher Mariah Rafaela Silva and computer scientist Nina Da Hora with Joy Buolamwini, from Algorithmic Justice League. The episode explores the accurate problem, that an automated system reproduces the racial bias and reinforces a series of social stereotypes. But Buolamwini goes further:

> Even if they were completely accurate they can still be abused, they can be used for mass surveillance. So if you are in an area that people are protesting knowing that police will use facial recognition some people will choose to stay home instead. Some of the protection that comes from being anonymous in the crowd will go away. Which literally can lead to authoritarian ways of tracking you. (CODING RIGHTS, 2021)

The emerging movement to contest and challenge AFRTs in Brazil is connected to regional efforts to produce knowledge and mobilize social change. Vladimir Garay, from Derechos Digitales (2019), published the report *Mal de Ojo - Reconocimiento facial en América Latina*, in an excerpt from the 2019 edition of Latin America in a Glimpse.

The report demonstrates that the adoption of this type of technology occurs throughout Latin America and is not only a Brazilian characteristic. In the same way, the reaction to this type of technology has been with knowledge production and with lawsuits, for example, as happened in the city of Buenos Aires, in Argentina, contested by the Asociación por los Derechos Civiles (ADC)[27], and in Asunción, in Paraguay, questioned by the NGO TEDIC[28].

We focus on analyzing these movements, academics, and legal actions in the next section.

4.5. Discussion about the cases: countermovements, affordances and fundamental rights

As noted in the previous topic, there has recently been an increase in the debate and contestation of the use of facial recognition technologies in Brazil. Civil society organizations have brought and elaborated more arguments focused on the endemic oppression side of the argument, as explained in the introduction.

The questions raised about the immense potential of discrimination brought by the use of automated facial recognition have been taking shape in the discourse of Brazilian organizations. In this sense, both the race argument and the gender argument have been better presented, especially in the last year (AMPARO, 2020; NUNES, 2021; SILVA & VARON, 2021). The recent growth of research organizations and institutions with a focus on racial and gender themes has certainly contributed to the debate gaining strength.

It is notable that, after George Floyd's global protests and the retreat of technology companies in offering facial recognition technologies, the Brazilian debate has become racialized. This is extremely positive for a discursive change that goes beyond the restricted field of consumer rights.

Gradually, social movements are mobilizing the argument of endemic oppression, noting how the simple use of this type of technology changes architectures and our ability to enjoy fundamental rights. Despite not having an explicit dialogue with the philosophy of technology - such as Evan Selinger, Julie Cohen and Mireille Hildebrandt -, civil entities may be transitioning from a corrective speech toward an opposition speech.

[27] https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/
[28] https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/

This discursive transition (which is only a hypothesis by now) can also be potentially coupled with a change in the theoretical level, in the sense of understanding the right to codetermine how we can be read by computers.[29] This right to "have a voice" before socio-technical arrangements finds a deep dialogue with the theory of law formulated by Mireille Hildebrandt, who advocates for a new role for privacy by design (HILDEBRANDT & O'HARA, 2020).

As argued by Prof. Julie Cohen, fundamental rights are made available partly by the (i) content and institutional structure of the applicable legal regime, partly by (ii) patterns of resource distribution that enable people to attain capabilities to enjoy fundamental freedoms, and partly by (iii) the constraints and affordances of the physical environment. The relevant constraints and affordances include both those directly affecting human behavior in physical space and those governing flows of information (COHEN, 2017, p. 85).

In order to properly address the problem of affordances and sociotechnical architectures, Hildebrandt and Cohen agree to develop a discourse of "rights-conceived-as-affordances", which cannot simply be subsumed into capabilities discourse.[30] This idea of "affordance" is central as it places architecture and socio-technical systems as determinants of how we can enjoy our fundamental rights, opening up the possibility of new power arrangements so that these arrangements are not defined in an imposing, authoritarian way and without multisectoral discussions.

What Brazilian civil entities seem to seek is, in a way, this type of voice and capacity for codetermination, engaging in the public debate about the possibility that our generation - and future generations - can enjoy fundamental rights.

[29] See Cohen: "Although we cannot entirely escape the constitutive force-fields generated by our technologies - and hence it would be intellectually dishonest to speak of a right to 'determine' our own legibility to other human and non-human actors - we can and should expect to have a say. That expectation in turn can be translated into more concrete requirements relating to transparency, choice parameters, and other operational matters" (COHEN, 2017, P. 87).

[30] In Cohen's words: "To define a right in terms of capability is to specify a minimum threshold (of material wellbeing, literacy, or some other good) below which people cannot as a practical matter enjoy the civil and political rights they are presumed to possess. By contrast, if we are concerned with architecture, the conversation becomes one about ways that enjoyment of fundamental rights is informed by systematic tolerances and prohibitions. Matters requiring attention include both the actions that are required - e.g., presenting a credential to gain access to a particular space - and the range of actions that are permitted - e.g., the ability to gain access using a credential that is authenticated but anonymized, or to move about that space without generating granular, identity-liked traces" (COHEN, 2017, P. 86).

It will be interesting to observe, in the coming years, the correlation of forces generated by these countermovements, the new tactics used to judicialize cases involving facial recognition and the mobilization of speeches about the inability to enjoy civil liberties and fundamental rights due to certain socio-technical configurations involving the use of AFRTs.

Conclusion

In this article, we identified two types of arguments mobilized against the expansion of automated facial recognition technologies (AFRTs). The first argument, which we called *endemic bias*, maintains that technologies have problems with database training, selectivity in the use of data collection sites and problems related to the impacts generated on the black population, which has suffered systematic violence.

The second argument, which we called *endemic oppression*, holds that facial recognition technologies erode due process, reverse the presumption of innocence, disable the full exercise of civil liberties and are incompatible with the values of a democratic society founded on freedoms. We used the expression “endemic” because we believe that it denotes the characteristic of a *negative condition*, something undesirable and intrinsic.

In Brazil, civil society movements gained more strength and voice based on the argument of endemic bias. The main criticism today is of a corrective nature: these technologies cannot continue to operate in this way, with this type of consequence for the black population, due to false positives and problems of system accuracy.

However, we observe that there is a potential transition to the argument of endemic oppression, which can take the form of a banning legal action. This argument is more complex and sophisticated, as it demands the demonstration that this type of socio-technical arrangement is incompatible with the exercise of fundamental rights.

There are several political and legal factors that may influence the direction of the regulation of facial recognition technologies in the coming years in Brazil. An important focus of analysis will be the understanding of countermovements and the argumentative construction of civil society in fundamental rights, as we demonstrated in this article.

References

ABRAMOVAY, Ricardo. Movimento por banir uso de reconhecimento facial cresce no mundo. *Folha de São Paulo, São Paulo*, December 14 2019. Available at: <https://www1.folha.uol.com.br/ilustrissima/2019/12/movimento-por-banir-uso-de-reconhecimento-facial-cresce-no-mundo.shtml>

ALMEIDA, Silvio. *Racismo Estrutural*. São Paulo: Editora Jandaíra, 2019.

APC (2019). *Joint letter: Ban security and surveillance facial recognition*, December 19 2019. Available at: <https://www.apc.org/en/pubs/joint-letter-ban-security-and-surveillance-facial-recognition>.

AMPARO, Thiago. Polícia algorítmica, *Folha de São Paulo*, São Paulo, January 27 2020. Available at <https://www1.folha.uol.com.br/colunas/thiago-amparo/2020/01/policia-algoritmica.shtml>.

ARROYO, Veronica; LEUFER, Daniel. *Access now expert opinion in the IDEC vs. ViaQuatro case.* Available at: https://www.accessnow.org/cms/assets/uploads/2020/06/Expert_Opinion_Brazil_Facial_Categorization.pdf.

ARTICLE 19. *Emotional Entanglement: China's emotion recognition market and its implications for human rights*. Available at: <https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf.>

BARON, Robert. J. Mechanisms of human facial recognition. *International Journal of Man-Machine Studies*. Available at: <https://doi.org/10.1016/S0020-7373(81)80001-6>.

FACIAL recognition: EU considers ban of up to five years. *BBC News*, 2020. Available at: <https://www.bbc.com/news/technology-51148501>.

BIONI, Bruno; ZANATTA, Rafael. Direito e economia política dos dados: um guia introdutório. *In*: DOWBOR, Ladislau. *Sociedade Vigiada*. São Paulo: Autonomia Literária, 2020.

BIONI, Bruno; MONTEIRO, Renato Leite. A Landmark ruling in Brazil: paving the way for considering data protection as an autonomous fundamental rights**.** *Future of Privacy Forum*, June 9 2020. Available at: <https://fpf.org/blog/a-landmark-ruling-in-brazil-paving-the-way-for-considering-data-protection-as-an-autonomous-fundamental-right/>.

BIONI, Bruno; MONTEIRO, Renato; ZANATTA, Rafael; RIELLI, Mariana. A Landmark Ruling from the Brazilian Supreme Court: Data Protection as an Autonomous Fundamental Right and Informational Due Process. *European Data Protection Law Review*, Volume 6, Issue 4 (2020) pp. 615 – 624. DOI: <https://doi.org/10.21552/edpl/2020/4/21>.

BRIA, Francesca; EVGENY, Morozov. *A cidade inteligente: Tecnologias urbanas e democracia*. São Paulo: Ubu Editora, 2020.

CAMARGO, Cristina. Homem negro morre após ser espancado por seguranças do Carrefour em Porto Alegre. *Folha de São Paulo*, São Paulo, November 20 2020. Available at: <https://www1.folha.uol.com.br/cotidiano/2020/11/homem-negro-morre-apos-ser-espancado-por-segurancas-do-carrefour-em-porto-alegre.shtml>.

CHELLAPPA, R.; WILSON, C. L.; SIROHEY, S. Human and machine recognition of faces: A survey. *Proceedings of the IEEE*. v. 83, issue 5, 1995. DOI: 10.1109/5.381842.

COALIZÃO DIREITOS NA REDE. *Open letter from representatives of Brazilian civil society facing threats to the democratic, free and open internet in Brazil*. November 19 2019. Available at: <https://direitosnarede.org.br/2019/11/27/igf-2019-open-letter/>

COALIZÃO DIREITOS NA REDE. *Open letter from Brazilian civil society on the occasion of the 15th edition of the United Nations Internet Governance Forum*. November 15 2020. Available at: <https://direitosnarede.org.br/2020/11/17/open-letter-from-brazilian-civil-society-on-the-occasion-of-the-15th-edition-of-the-united-nations-internet-governance-forum/>.

CODING RIGHTS. Reconhecimento Facial: raça, gênero e território. *From Devices To Bodies. Webseries*. 2021. Available at: <https://www.youtube.com/watch?v=omP93gEuQfI>.

COHEN, Julie E. Affording fundamental rights: A provocation inspired by Mireille Hildebrandt. *Critical Analysis of Law*, v. 4, n. 1, 2017.

COHEN, Julie E.. Turning privacy inside out. *Theoretical inquiries in law*, v. 20, n. 1, 2019.

DALE, Gareth. *Karl Polanyi: The limits of the market*. Cambridge: Polity Press, 2010.

DEEPAI. *Neural Network***.** Maio 17 2019. Available at: <https://deepai.org/machine-learning-glossary-and-terms/neural-network>.

DERECHOS DIGITALES. *Mal de Ojo*. Available at: <https://www.derechosdigitales.org/wp-content/uploads/glimpse-cap-rec-facial.pdf>.

EATON, Sabrina. *Facial surveillance alarms Congress; Republicans and Democrats pledge action*. Jan 15 2020. Available at: <https://www.cleveland.com/open/2020/01/facial-surveillance-alarms-congress-republicans-and-democrats-pledge-action.html>.

GATES, Kelly A. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: NYU Press, 2011.

GRABER, Christopher B. *Artificial intelligence, affordances and fundamental rights*. In Life and the Law in the Era of Data-Driven Agency. Cheltenham: Edward Elgar Publishing, 2020.

HILDEBRANDT, Mireille. *Countermovements to Reinstate Countervailing Powers***.** Jotwell: J. Things We Like, (July 17, 2020) (reviewing Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (2019)), Available at: <https://cyber.jotwell.com/countermovements-to-reinstate-countervailing-powers/>.

HILDEBRANDT, Mireille; O'HARA, Kieron. *Introduction: Life and the law in the era of data-driven agency*. In Life and the Law in the Era of Data-Driven Agency. Cheltenham: Edward Elgar Publishing, 2020.

IBM. *IBM CEO's Letter to Congress on Racial Justice Reform*. June 8 2020. Available at: <https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/>.

IDEC. *Reconhecimento facial Dataprev INSS*, Idec Notícias. Available at: <https://idec.org.br/noticia/idec-notifica-dataprev-por-licitacao-para-uso-de-reconhecimento-facial>.

INSTITUTO IGARAPÉ. *Videomonitoramento - Webreport*. Available at: <https://igarape.org.br/videomonitoramento-webreport/>.

INSTITUTO IGARAPÉ AND DATA PRIVACY BR RESEARCH. *Regulação do Reconhecimento Facial no setor público: avaliação de experiências internacionais*. Available at: <https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf>.

INTERVOZES**.** *Reconhecimento facial no Carnaval: riscos tecnológicos nada divertidos*. Available at: <https://www.cartacapital.com.br/blogs/intervozes/reconhecimento-facial-no-carnaval-riscos-tecnologicos-nada-divertidos/>.

JAIN, Anil K.; ROSS, Arun A.; NANDAKUMAR, Karthik. *Introduction to Biometrics***.** Boston: Springer, 2011.

JASSERAND, C. Legal nature of biometric data: From generic personal data to sensitive data. *European Data Protection Law Review*. v. 2, issue 3, 2016. DOI https://doi.org/10.21552/EDPL/2016/3/6

KANTAYYA, Shalini. *Coded Bias*. Documentary. Available at: <https://www.codedbias.com/>.

LEE-MORRISON, Lila. *Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face*. Bielefeld: Transcript Verlag, 2019.

MARTINS, Helena. Reconhecimento facial: a banalização de uma tecnologia controversa, *Le Monde Diplomatique Brasil***.** April 22 2020. Available at: <https://diplomatique.org.br/reconhecimento-facial-a-banalizacao-de-uma-tecnologia-controversa/>.

NAJIBI, Alex. Racial Discrimination in Face Recognition Technology. *Harvard University Blog, Science Policy and Social Justice Edition*. October 24 2020. Available at: <http://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>.

NUNES, Pablo. O algoritmo e racismo nosso de cada dia, *Revista Piauí*, January 02 2021. Available at: <https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia>.

REZENDE, Isadora N. Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*, v. 11, issue 3, 2020.

RIBEIRO, Djamila. *Pequeno manual antirracista*. São Paulo: Companhia das Letras, 2019.

RODRIGUES, Gustavo. *LGPD penal: um remédio contra o solucionismo tecnológico na segurança pública?.* Available at: <https://irisbh.com.br/lgpd-penal-um-remedio-contra-o-solucionismo-tecnologico-na-seguranca-publica/>.

SAMAL, A.; IYENGAR, P. A. *Automatic recognition and analysis of human faces and facial expressions: A survey. Pattern Recognition*, 25(1), 65–77. Available at: <https://doi.org/10.1016/0031-3203(92)90007-6>.

SELINGER, Evan; HARTZOG, Woodrow**.** *Facial Recognition Is the Perfect Tool for Oppression***.** Medium. Available at: <https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66>.

SELINGER, Evan; HARTZOG, Woodrow. The inconsentability of facial surveillance. *Loyola Law Review*, vol. 66, 101-122.

SILVA, Mariah Rafaela; VARON, Joana. *Reconhecimento facial no setor público e identidade trans: tecnopolíticas de controle e ameaça à diversidade de gênero em suas interseccionalidades de raça, classe e território*. Available at: <https://codingrights.org/docs/rec-facial-id-trans.pdf>.

SOBEL, Benjamin. A New Common Law of Web Scraping (SSRN Scholarly Paper ID 3581844). *Social Science Research Network*. Available at: <https://doi.org/10.2139/ssrn.3581844>.

TEOFILO, Davi; KURTZ, Lahis; PORTO JR., Odélio; VIEIRA, Victor Barbieri Rodrigues. *Parecer do IRIS na Ação civil Pública IDEC vs. Via Quatro. Parecer sobre a atividade de detecção facial de usuários da Linha Quatro Amarela de metrô de São Paulo, objeto do processo nº 1090663-42.2018.8.26.0100 da 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo, ação interposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) contra a Concessionária da linha 4 do metrô de São Paulo S.A. (ViaQuatro).* Setembro de 2019. Belo Horizonte: IRIS. Available at: <http://bit.ly/340ZN53>. English version: <https://irisbh.com.br/wp-content/uploads/2019/12/Public-Civil-Action-IDEC-vs.-ViaQuatro-IRIS-opinion.pdf>.

TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora Raad. *Reconhecimento Facial: laissez-faire, regular ou banir? Migalhas da vulnerabilidade*. Avaliable at: <https://migalhas.uol.com.br/coluna/migalhas-de-vulnerabilidade/330766/reconhecimento-facial--laissez-faire--regular-ou-banir.>.

SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico. Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. *InternetLab/IDEC*, São Paulo. Available at: <https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf>.

UN HIGH COMMISSIONER FOR HUMAN RIGHTS (OHCHR). *New technologies must serve, not hinder, right to peaceful protest, Bachelet tells States*. Available at: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=E>.

ZANATTA, Rafael A. F. Proteção de dados pessoais entre leis, códigos e programação: Os limites do Marco Civil da Internet. *In* LUCCA, N. De; FILHO, Simião A; LIMA, C. R. *Direito & Internet III – Tomo I: Marco Civil da Internet (Lei 12.965/2014)*. São Paulo: Quartier Latin, 2015.

ZANATTA, Rafael A. F. A nova batalha em torno da proteção dos dados pessoais no Brasil: o que defendem diferentes atores?. *In*: *Comitê Gestor da Internet, Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros*. São Paulo: Comitê Gestor da Internet no Brasil, 2017.

ZANATTA, Rafael A; BIONI, Bruno; KELLER, Clara I; FAVARO, Iasmine. Os Dados e o Vírus. *Revista Brasileira de Direitos Fundamentais & Justiça*, 14(1), 231-256.