SURVEILLANCE & VIGILANTISM

Concepts, Brazilian legislation and organizations in the field

LAUT

FORD FOUNDATION

SURVEILLANCE & VIGILANTISM

Concepts, Brazilian legislation and organizations in the field

Production

LAUT CENTRO DE ANÁLISE DA LIBERDADE E DO AUTORITARISMO

We are an independent and non-partisan, inter-disciplinary research institution, committed to producing and distributing knowledge on the quality of the state of rights and democracy. Our objective is to monitor expressions of authoritarianism and the repression of freedoms to provide grounds for the mobilization of civil society and the defense of freedom.

Management

Conrado Hübner Mendes (CEO), Rafael Mafei Rabelo Queiroz (Vice-President), Adriane Sanctis (Director and Research Manager) e Carolina C.B. Cooper (Strategy and Operations Manager).

May 2022

Support

FORD FOUNDATION

This publication has been made possible due to support from the Ford Foundation

Project coordinators

Research and writing:

Anna Carolina Venturini, Pedro Ansel, Marina Slhessarenko Barreto, Yuri Marcelo Oliveira e Ana Silva Rosa

Editing

Iara Crepaldi

Translation

House of Words

Visual identity

Atonal Studio

Layout

Sergio Berkenbrock dos Santos

Citation suggestion

Venturini, A. C.; Ansel, P.; Barreto, M.S.; Oliveira, Y.M.; Rosa, A. S. (2022). *Surveillance & Vigilantism: concepts, Brazilian legislation and organizations in the field*. São Paulo. Centro de Análise da Liberdade e do Autoritarismo (LAUT)

ISBN

978-65-980829-5-6

License

CC BY SA

The content herein is licensed by Attribution 4.0 International (CC BY4.0)

Index

04 Introduction

06 Surveillance within and outside digital environments

18 Surveillance and facial recognition technologies

33 Vigilantism and digilantism

40 Organizations leading the way in Brazil and elsewhere

52 Brazilian initiatives that use surveillance to support the population

Introduction

The issue of surveillance and vigilantism has recently been increasingly more discussed both in Brazil and elsewhere, mainly due both to the developments in technology that now allow biometric data to be collected and to the increased collection of personal data. Every day we share an enormous amount of information about our habits and behavior with private companies, the owners of digital technologies such as cell phones, tablets, applications, and many others.

People are also constantly being monitored by the State. Since long before cell phones and computers existed, the State has been creating and producing records on the population, relating to when and where we were born, our annual income, and whether we use public services. Furthermore, the State can directly monitor the public through its policing, intelligence and espionage activities. But this control over our data is not always authoritative or abusive. In order for there to exist public policies that are compatible with public needs, it is necessary for a set of data collected by public entities be analyzed by researchers and specialists for the formation of public policies based upon evidence.

Surveillance and vigilantism are fundamental for our ability to consider democracy and the Rule of Law as they currently exist. In non-democratic and authoritarian systems, the power linked to the use of surveillance technologies can affect democratic development and lead to serious abuses of human rights. There exists case upon case in which opposition activists, defenders of human rights, and journalists are placed under government surveillance and have their communications read - sometimes legally, sometimes illegally.

The collection of a huge amount of data by the State also raises important questions concerning the security of its storage, the purpose of the collection, the handling of the data, and the risks of them being centralized in single database. As such, many countries have started to review their laws covering surveillance, privacy and the protection of personal data, with the aim of guaranteeing greater security to individuals and to the sharing of their data and personal information by the State and by private companies.

In addition to this, when we speak of technology, it is impossible not to also think of discrimination. Over recent years, a great number of studies have shown how automated technologies and artificial intelligence reproduce biases and stereotypes, and ultimately end up being discriminatory. The lack of diversity in the technology sector is considerable and has been widely

investigated. Many studies show the under-representation of women and minorities in the areas of technology, engineering and mathematics, be it in higher education or the workplace. And the lack of people with a varied range of identities, histories and experiences has a direct effect on the technologies that are developed. This is because the majority of these technologies depends on programming, or in other words, on someone who can develop the code (called an algorithm) which is needed for it to function. There are a growing number of organizations that depend upon algorithms to support their decision-making, but if the programming and artificial intelligence industry is made up of just one group - white men - this can lead to a bias in the system.

With this in mind, this report presents fundamental concepts on the issue and the data concerning how surveillance and vigilantism have manifested themselves in Brazil. This document also intends to offer an initial overview of the ecosystem of organizations working with these issues, both here in Brazil and elsewhere. The data presented are the result of extensive, but still not exhaustive, mapping performed by LAUT researchers based upon news and publications on the issue.

This overview has been broken down into six parts, including this introduction. The second part presents the concept of surveillance, data on draft legislation connected with the issue of protection of personal data, and landmark cases concerning the leakage of personal data of Brazilian citizens. The third part is dedicated to the matter of facial recognition, how this technology has been adopted in this country, and how it has been addressed in draft legislation relating to biometric data, artificial intelligence and facial recognition. In part four, we look at vigilantism and how it manifests itself within and outside the digital environment, including a look at cases of vigilantism that have attracted special interest from the Brazilian press. The fifth part of the report maps out those organizations in Brazil and elsewhere in the world that are working either directly or indirectly with the issue of surveillance and vigilantism. Finally, the last part provides examples of non-governmental organizations that have used digital technologies to assist the public and which have overcome, to a certain extent, the absence of the public authorities in this area or their failure to act.

Surveillance within and outside digital environments

What is surveillance? How can it affect our freedom and result in discrimination or other violations of our rights? Understanding the concept and the ways it takes shape and plays a role in our day-to-day lives.

Surveillance

This concerns the monitoring and supervision activities performed by public or private agents. In the field of public security, one example of surveillance is the patrolling performed by the police designed to guarantee the constitutional right of citizens to safety and public order. Private companies can perform surveillance activities, provided they are duly licensed by the public authorities, generally offering private security services to other organizations and individuals, under the terms of **Law nº 7,102/1983**. Civil society institutions, such as non-governmental organizations (NGOs) and councils (federal, state and municipal) can also assume the role of supervisors. Surveillance within the limits of the law should, most importantly, respect the right to privacy of those being monitored.

Digital Surveillance

Digital surveillance is related to the act of monitoring the behavior of individuals in digital environments (social networks, websites, applications and other platforms connected to the Internet). A large part of digital surveillance is made possible through the collection of so-called digital footprints, this being the information we leave behind when clicking on an advertisement or when we sign up for access to a certain online platform, for example. Much of the data produced as a result of our activities

through virtual means are called personal data, which include information that can be identified directly or indirectly, such as our social security or telephone numbers, or even our whereabouts.

It is now increasingly more common for companies operating in a wide variety of different sectors to collect our personal data. Spread out across around 440 million digital devices in use in Brazil, the data are used to map our consumer habits with the aim of developing products that are more attractive to companies' target publics. Similarly, the government also maintains constant surveillance of citizens through the processing of the personal data that circulate over the Internet. However, instead of focusing on ways of increasing its revenue as companies do, the government uses the data to enable actions such as the distribution of social benefits, drafting of public policies, and pursuit of police investigations.

Through until 2018, there was no specific law in Brazil designed to regulate the acquisition or sharing of personal data. **The General Data Protection Law (LGPD)**, from thereon, established that "*every natural person is assured ownership of her/his personal data*". Furthermore, it established a number of other legal provisions that, in theory, provide citizens with greater control over digital surveillance. *Article 5* of the LGPD also defined the different types of personal data: (a) *personal data* is "information regarding an identified or identifiable natural person"[1], (b) *sensitive personal data* is "personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organization membership, data concerning health or sex life, genetic or biometric data, when related to a natural person"1, and (c) *anonymized data* is "data related to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of the processing".

[Timeline] Legislation on the protection of personal data

The most important legal landmarks relating to the protection of personal data in Brazil.

November 2010

The Ministry of Justice opens the **First public consultation** to discuss a **draft bill of law** on the protection of personal data on the Internet. The text covers: data protection in the public and private sectors, regulations for the exchange of client information between financial institutions, and regulation of personal data protection as a policy to guarantee citizens' right to privacy and freedom. It also sets out plans for the creation of the National Council for the Protection of Personal Data.

1 According to the Brazilian Civil Code (Law 10,406/2002), a 'natural person' is any human being who is eligible for rights and duties under the civil system.

August 2011

Regulatory Framework for the Internet (Bill of Law nº 2,126/2011) is sent to the National Congress. The Bill of Law envisions principles, guarantees, rights and duties for the use of the Internet in Brazil, establishing that all those involved in the transmitting of data are required to handle them equally and without discrimination. The "Internet's Constitution", as the bill came to be called, recognizes constitutional principles such as freedom of expression, privacy and human rights in virtual environments.

November 2011

The law of Access to Information (**LAI**) — **Law nº 12,527/2011** — is sanctioned. This establishes access to public documents as a fundamental principle, allowing any Brazilian citizen to request data concerning the public authorities, at Federal, State or Municipal level, including all branches of government (Executive, Legislative and Judicial). It also ends the possibility of eternal confidentiality protecting the publication of official documents and determines that public entities pro-actively publish a minimum list of information on their activities through the Internet. It is important to highlight that, whilst the LAI regulates access to information and public documents, the law of *habeas data* (art. 5, LXXII of the CF 1988 and Law nº 9,507/1997) address access to citizens' private information collected by the State, with the intention of ensuring fundamental rights to privacy and information.

June 2012

Bill of Law nº 4,060/2012 is presented to regulate the handling of personal data, with the aim of creating specific legislation on the issue. The handling of personal data means the cross-checking of data and information regarding a person or a group in order to direct public policies, commercial or consumer decisions, or the work of a public body. This cross-checking involves the grouping of information stored in the databases of different institutions. The Bill of Law establishes as a rule that the handling of personal data should be conditional upon the permission of its owners.

December 2012

The **Carolina Dieckmann Law (Law nº 12,737/2012**), enters into effect, adding the definition of cyber-crimes performed by means of invasion of electronic devices (articles 154-A and 154-B) to the **Brazilian Penal Code**. This law came about following an episode which had enormous media repercussion: the personal computer belonging to the actor Carolina Dieckmann was hacked and intimate photos of her were released on the Internet.

August 2013

The regulatory framework on the protection of personal data is presented to the Senate, in the form of **Bill of Law nº330/13**. The **Bill of Law** covers regulations for the collection of data in Brazil, based upon the principles of human dignity, the protection of privacy, the guarantee of freedom and the inviolability of a person's image. It also establishes that personal data cannot be used with the intention of negatively affecting citizens.

April 2014

Approval of the **Regulatory Framework for the Internet**, the first Brazilian law to establish rights, guarantees, principles and duties for the **use of the Internet in the country**. Law nº **12,965** establishes that the Internet should respect the principle of neutrality of the net, or in other words, all networked information should travel equally, regardless of its content, origin, destination, service or application. It establishes freedom of expression as a basic principle for the functioning of the Internet and the "inviolability of intimacy and private life, their protection, and compensation for material or moral damages resulting from their violation" (Art. 7, item I).

January 2015

The Ministry of Justice holds another **public hearing** to discuss the protection of personal data stored in Brazil or overseas. The consultation, based upon the models of the Regulatory Framework for the Internet, seeks to provide the legal foundations for the supervision, by regular citizens, of how third parties collect and use their data. It also brings into the public debate the definition of the concepts of personal data (information that allows for the identification of individuals), anonymous data (information that does not identify its owners) and sensitive data (information that could possibly lead to discrimination on the grounds of race, religion, political persuasion, amongst other factors), as well as guidelines for protecting them.

May 2016

The House of Representatives starts the process for **Bill of Law nº 5,276/2016**. The Bill of Law is the result of the **public debate** held by the Ministry of Justice and addresses the increase in the protection of data, based upon the "guarantee of the free development of personality and human dignity".

May 2018

'House of Representatives' Bill of Law nº 53/2018 – considered as the basis for the LGPD – is approved. Its origin lies in the annexing of three other Bills of Law that address the issue of protection of personal data: **Bill of Law nº 5,276/2016**, **Bill of**

Law 4,060/2012 and **Bill of Law n° 330/2013**. A new proposal for the protection of data in Brazil is directly influenced by the recently approved **General Data Protection Regulation (LGPD)**, dated May 25, 2018, that outlined the guidelines for the **protection of data in the European Union**.

July 2018

PLC 53/2018 is **unanimously approved by the Senate**. This seeks to regulate the protection, transfer and use of personal data. It also aims to create the National Data Protection Authority (ANPD), a body connected to the Ministry of Justice that is designed to assist in the control and supervision of the circulation of data. It also addresses punishment, fines, and the suspension of the performance of the activities of companies if there have been infractions concerning the handling of data and information.

August 2018

The **LGPD** – Federal Law n° 13,709/2018 – is approved by President Michel Temer and published in the Official Gazette of the Federal Executive, stipulating a period of 18 months for it to enter into effect. This legal framework, that regulates the transfer, use and protection of personal data in Brazil, has been created in line with international parameters on data protection. It establishes Brazilian citizens' ownership of their data in both physical and digital mediums, meaning that the handling of personal and sensitive data by public and private institutions becomes conditional upon authorization by the title holders, except in cases such as compliance with a legal obligation or the creation of public policies.

It also establishes the commitment to transparency in relation to the operations performed with the title holders' personal data. In the event of non-compliance with the LGPD, administrative sanctions have been set forth including fines and the blocking of activities relating to the handling of information.

June 2019

The Biometrics and Privacy Commission is established as part of the House of Representatives' Commission for Science and Technology, Communication and Information Technology.

July 2019

A proposal for a Constitutional Amendment (**(PEC) 17/ 2019**) is presented to the Senate. The aim of this is to include the protection of personal data, including that found in digital media, in the 1988 Federal Constitution, recognizing the protection of personal information as a fundamental right in the Brazilian legal framework.

October 2019

The Federal Government issues **Decree n° 10,046/2019**, regulating the sharing of data between federal governmental organs, and creates the **Citizens' Register Base (CBC**), created using the databases of different governmental organs. The Register cross-checks data from these databases with personal information such as social security number, name, date of birth, parentage, etc. The argument for its creation is the role it will perform in the creation of better public policies.September 2020

After a series of delays, the LGPD moves into effect. The process involved in creating and finalizing the wording includes the active participation of civil society organizations and extends the reach of the data protection guidelines established by the Regulatory Framework for the Internet. With the **LGPD** now in effect, public and private institutions are required to adjust their practices concerning the storage, availability and collection of information on the Internet to the new legal regulations. Organs forming the Judiciary have also had to adopt measures to ensure that their courts bring themselves into line with the provisions of this legislation.

November 2020

The **'ANPD'** is moved into effect. This new organ forming part of the federal government assumes responsibility for the implementation, supervision and regulation of compliance with the LGPD. Amongst the main **responsibilities of the ANPD** are: promotion of cooperation with those authorities responsible for personal data protection in other countries, provision of information to the public concerning personal data protection regulations and public policies and security measures, as well as the supervision and application of sanctions in the event of non-compliance with the law. President Jair Bolsonaro chooses **three members of the military to head the ANPD**.

March 2021

Within the context of the Commission for Science and Technology, Communication and Information Technology (CCTCI), **Request 8/2021** is presented, calling for the "holding of a Public Hearing to update the discussion on the issue of facial recognition technologies for application in public security and other systems designed to ease day-to-day activities in Brazil".

May 2021

The Ministry of Justice performs a virtual public call notice to acquire the **spy software Pegasus**. This computer program, used for spying, allows access to cell phones and personal computers and the collection of data stored on them without the owners' consent. Discovered in 2016, it is a form of spyware (spying technology) supposedly intended to curb criminal and terrorist activities. Over recent years, however, the

governments of countries such as Mexico, India and Saudi Arabia have been caught using this program to hack cell phones and monitor the conversations of political opponents. The bidding process, valued at R$ 25.4 million, involves the active participation of **councilor Carlos Bolsonaro** (Republican), who visited Israel in 2019 to discuss the matter with representatives of the company responsible for supplying the technology. The organs benefiting from the process will be the Brazilian Intelligence Agency (Abin) and the Institutional Security Cabinet (GSI). The electronic bidding for the tender was ultimately **suspended by the Federal Audit Court (TCU)**.

The Director General of the Federal Police (PF) signs an agreement for the purchase and implementation of the **'ABIS' – Automated Biometric Identifi ation Solution**, that will allow for the identification of people through the collection, storage and cross-referencing of digital fingerprinting and facial recognition data. According to the PF, the ABIS system will be able to unify the data held by the Departments of Public Security (SSPs), providing state police with access to the national biometrics database. Various different entities **approached the ANPD**, arguing that the system will present a risk to individual privacy and the protection of information.

August 2022

The application of penalties moves into effect in the event of non-compliance with the LGPD, which establishes that institutions should justify the collection of personal data and request authorization for use from the owners of the information. Penalties are applied by the ANPD and vary according to the level of impact and the seriousness of the infraction of the law, with the possibility of issuing notifications or applying daily fines, simple fines of up to 2% of a company's revenue, fines involving publicity of the infraction, blocking or elimination of personal data, and suspension or even partial or total prohibition of the performance of the activities of the company in breach of the regulations.

February 2022

The National Congress enacts **Constitutional Amendment (EC) 115**, altering the Constitution to include the protection of personal data in the list of fundamental rights, and establish the exclusive authority of the Union to legislate on matters involving the protection and handling of personal information. As such, the protection of personal data officially becomes a constitutional right ("Art. 5, item LXXIX - the right to the protection of personal data, including in digital media, is assured, under the terms of the law.").

[Timeline] Cases of data leakage

Cases of data leakage that have attracted special interest from the Brazilian press

July 2007

Due to the Pan-American Games ('Pan'), the now-defunct Rio de Janeiro State Department for Security acquires the **'Guardian' telephone interception system**, allowing access to data created by voice from a telephone device - commonly referred to as 'phone tapping'. **Following the Pan Games, the system is acquired by numerous departments of the PF and by the Public Prosecutor's Offi e** (MP) in a number of states, to be used, mainly, in operations focused on fighting corruption.

June 2011

The PF investigates **a suspect of hacking the e-mail of ex-President Dilma Rousseff** by accessing medical reports and confidential documents held by the Military Supreme Court (STM) which were in the President's e-mail folders. Starting with the hacking of the Workers' Party (PT), during the Presidential race the previous year, the cyber-criminal (a person who uses programming knowledge to hack systems) had managed to access Dilma Rousseff's e-mails and copy around 600 messages. The contents were to be sold to the press and to political parties standing in opposition to the ex-head of the Executive Branch. The Federal Government announces that it is having difficulty in confirming whether the e-mails were, indeed, obtained illegally.

September 2013

The press publishes **documents leaked by Edward Snowden** revealing that the Brazilian government was the target of spying by the United States' National Security Agency (NSA). Thought to be the most extensive spying system in the world, the NSA monitored telephone numbers, e-mails and IP addresses (computer identification codes) to intercept conversations held between the Brazilian head of state and her principal advisors.

One of the pieces of software used in the surveillance job was one called "DNI selectors", capable of tracking the actions of Internet users. The documents do not state what information was intercepted nor the interest which the US had in taking such action.

December 2017

The company Netshoes reports **a mega-leakage of client data**. Faults in the cyber-security of the platform allowed virtual criminals to access and publish lists containing information on almost two million registered users. Included in the data

released were full names, products purchased, social security numbers, e-mails and dates of birth. According to the Public Prosecutor's Office of the Federal District and Territories (MPDFT), the organ responsible for investigating the case, this was one of the **biggest cases involving breach of security** ever recorded in Brazil.

April 2018

Facebook announces that **a consultation firm i legally took control of data** belonging to more than 87 million account holders, 443,000 of whom were Brazilians. With Facebook's authorization, the company Cambridge Analytica circulated a psychology test on social media, and collected data on personality traits without authorization.

The company offered the information collected illegally in support of Donald Trump's presidential campaign, highlighting which Facebook users would have profiles suitable to receive the republican candidate's banners since there was a good chance they would then post them on their social media profiles.

May 2018

The **São Paulo State Commission on Truth** reveals that rectors at the country's leading higher education institutions contributed to the military regime. According to **a document produced by the Commission, the Federal University of Santa Catarina (UFSC) and the University of São Paulo (USP) passed on information on the Ideological beliefs held by students and professors to the National Information Service (SNI)**. As well as handing over reports on students and teaching staff, the spying included members of the federal government infiltrating university circles. The commission also noted evidence of activity by spies working for the military regime in the Federal Universities of Bahia, Espírito Santo and Rio Grande do Norte, as well as PUC-SP and the University of Brasília.

February 2019

Minister Sérgio Moro's anti-crime package legally establishes the position of 'undercover police agent', the activities of which lie somewhere between a police investigation and police infiltration.

As well as having a relative degree of expertise, the undercover agent should have the ability to act without attracting attention to themselves in order to collect evidence of a crime and investigate those responsible, without interfering in the causal process of the criminal activity.

September 2019

Secret documents from the PF show that **public security agents had infi trated the meetings of social movements and protests staged in June 2013**. The names of the leaders of social movements were identified, as well as the data belonging to citizens who participated in the activities, their comments on social media and their cars. The infiltrators disguised themselves as part of the "black blocks", these being groups of protesters who generally wore black and masks, and were known for carrying out direct actions during the protests. Despite this type of activity on the part of the authorities being highly invasive and potentially violating the basic freedoms of expression and protest, **the PF told the newspapers at the time that they were "acting legally and doing their job"**.

June 2020

The press uncovers a **case of digital surveillance operated by the Brazilian Intelligence Agency (Abin)**. The central body of the Brazilian Intelligence System (SISBIN) performed a political operation, considered to be illegal, in an attempt to obtain data contained from the driving license (CNH) records of more than 76 million Brazilians. This involved the ABIN requesting that the Federal Data Processing Service (SERPRO), the country's largest public technology services company, obtain information from the National Driving License Records (Renach) database concerning vehicles, telephone numbers, addresses, parentage, telephone numbers, vehicle data and photographs belonging to driving license holders in the country, meaning almost 40% of the Brazilian population. The information was to be delivered to the Federal Government. A lawsuit filed with the **Federal Supreme Court (STF)** alleged that Abin had violated the right to privacy, protection of personal data and informational self-determination, as well as being an affront to human dignity.

July 2020

The Department of Integrated Operations (SEOPI), an organ within the Ministry of Justice and Public Security created by ex-Minister Sérgio Moro, is accused of having **monitored the personal data of 579 federal and state civil servants, and university professors listed as being antifascists** and critics of the Jair Bolsonaro government. The organ had produced a dossier containing names and, in some cases, photographs and social media addresses of those being monitored, with a report being distributed to federal and state governments. The **Sustainability Network questions the secret investigations** conducted by Seopi within the sphere of the Federal Supreme Court. The Court classifies the practice of collecting information on "civil servants with a political stance contrary to that of the government" as an "abuse of the state machine", thus **ordering the suspension** of any action of this nature by the Federal Government.

August 2020

The Sustainability Network and PSB question the interpretation that it **the Brazilan Intelligence Agency** (ABIN) has the legal power to order sensitive and confidential information to be handed over, such including documents covered by tax secrecy, COAF reports and telephone privacy, for example. **The Court decided that data and knowledge specifica ly relating to Abin can only be provided** when it is proven to be in the public interest, thus removing any possibility that such data serves personal or private interests. It also decided that it was absolutely fundamental that a formal procedure should be started, along with the existence of electronic security systems and access records, including for the purposes of establishing liability in the event of possible omissions, irregularities or abuse.

November 2020

The **High Court of Appeal (STJ) announces** that its computer system has been the target of a cyber-attack. According to the investigation, a fault in the STJ's network security system had allowed cyber-criminals to block judges and employees from accessing the court's records. As security measures, institutional e-mails were taken off the air and those working at the court were instructed not to use their computers. The cyber-attach occurred at a time when judgment sessions were in progress, and these had to be suspended until the technical department had reestablished security.

June 2021

The Governor of Rio de Janeiro **sanctions a law that orders the inclusion of video and audio cameras on police uniforms and on aircraft** operated by the security forces. The approval raises discussions, considering that **Governor Cláudio Castro vetoed important** passages, such as those establishing deadlines for the installation of the equipment, those determining the availability of audio and video records at the time the event is recorded, with the aim of confirming the inviolability of the material, and, moreover, those guaranteeing that "any and every citizen" directly involved in the action may have access to the material.

January 2021

News of a **mega-leakage involving the data** of 223 million Brazilians is reported. **Databases** containing information such as the full names, dates of birth, social security numbers, genders and residential addresses of living and deceased persons were traded by digital criminals on the dark web (an area of the Internet where it is more difficult to track activities). The crackers also offered lists containing information such as education, National Institute of Social Security (INSS) benefits, social programs, incomes and credit ratings. A portion of the data was offered free-of-charge and 37 packages of data were being sold. The PF arrested two suspects in relation to the crime.

August 2021

The **internal network of the National Department of the Treasury** is the target of ransomeware, a virtual attack in which a computer's data is encrypted, meaning it cannot be accessed. In such cases, criminals generally demand a ransom to release the data. In a statement, the Ministry of the Economy clarified that, despite the attack, no damage to the National Treasury's systems had been identified by specialists.

December 2021

The website of the Ministry of Health (MS) suffers a **virtual attack**. The website is taken off the air and, in its place, there appears the following message from the group assuming responsibility for the attack: "the internal data of the systems have been copied and deleted. 50 TB of data are in our hands. Contact us if you wish the data to be returned". The **Covid Portal and the 'SUS Connect' Portal were also brought down** by the virtual criminals. The PF and GSI are brought in to investigate the case.

Surveillance and facial recognition technologies

In Brazil and various other countries, facial recognition technologies and their use for surveillance or combating fraud has raised intense discussions, as a result of the increase in the number of cases of algorithmic discrimination that have been causing errors and the punishment of innocent people.

Below, we set out the fundamental concepts for understanding this issue, as well as the main uses of the facial recognition technologies that we have identified in Brazil along with bills of law aimed at regulating the use of these technologies and artificial intelligence in the country.

Algorithms

Algorithms can be understood as sequences of codes (rules, instructions, operations or reasonings) that need to be followed to resolve a problem or achieve a certain objective - a kind of recipe of sorts. Algorithms structure all that is done in computers and, consequently, all that is done in the virtual world. In general, these codes are written by those responsible for developing the technology industry, companies which establish all the steps for the functioning of software and equipment such as computers, cell phones, surveillance cameras, etc. They have recently been the target of much criticism, due to the effect they have had on the quality of the public spheres and the balance of power both in the private and public sectors. Furthermore, they are open to criticism due to the lack of transparency found in their mechanisms, which reinforces the possibility of manipulation. In the private sector, for example, they enable the creation of bubbles containing the reproduction of opinions and positions (for example, the clusters of left-wing versus right-wing opinions on social media) and targeted advertising. These are, therefore, fundamental elements not only for the functioning of the surveillance systems, but also for the existence of any digital software or technology.

Algorithmic discrimination and artificial intelligence (AI)

Algorithmic discrimination occurs when there is a difference in the approach of digital content due to biases assumed by the algorithms (as a result of the way in which their codes were developed). This type of discrimination has been frequently tied to artificial intelligence, an area of research with computer science which, through computational mechanisms, seeks to build machines capable of performing tasks that normally require human intelligence, such as the resolving of everyday problems. It is important to highlight that artificial intelligence is a very broad subject, which should not be confused with **"machine learning"**, since this is just one of its features. Software with machine learning involves programs that can automatically improve in accordance with the amount of data they process.

Once programmers/developers have instructed them with materiality criteria, the AI algorithms can separate or emphasize information. The most frequent forms of **algorithmic discrimination** are racism and sexism, since studies show that the technology industry is largely made up of white men, meaning that the materiality criteria used to produce the algorithms often assume sexist and racist premises to classify information in the digital world. In 2018, the tech giant Amazon created an artificial intelligence algorithm that selected curricula for job vacancies, but the company ended up taking the technology out of circulation after realizing that there was a strong tendency towards declassifying women from the selection processes. In another case, the preference for selecting the faces of white people in photos containing white and Black people, in 2020, led the Twitter social network to discontinue the algorithm that performed automatic cuts of photographs before being posted by users.

Biometric recognition technologies

Biometrics can be defined as the analysis of physical, morphological and behavioral characteristics to provide identification of an individual, based upon the principle that such characteristics are singular and immutable over time. Biometric recognition technologies respond to automated methods to verify or recognize a person's identity based upon the gauging of their physical characteristics, including the curvature of the lips, the distance between the eyes, the format of the fingerprints and even the layout of the blood vessels that feed the retina. We do not always notice it, but our everyday lives are filled with these technologies; the most common being fingerprint reading (used to issue documents such as our ID or driving license) and facial recognition.

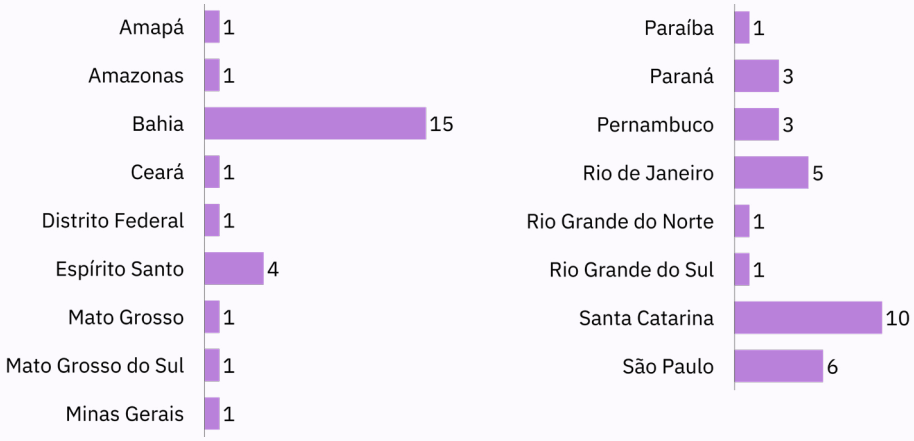
Facial recognition technologies allow a person's face to be digitalized and automatically associated with a database. Over recent years, facial recognition has been used to unblock cell phones, to allow people to gain access to buildings, to control access to schools, and to clock people into work, as well as to locate people fleeing from justice, through the use

of cameras distributed around public spaces and monitored by police authorities. These technologies have also been used on public transport, arguing that it is designed to tackle fraud. It is important to highlight that not all video-monitoring cameras installed in cities and buildings have facial recognition technology - rather just specific cameras that have only recently been installed in public and private spaces, and on public transport.

Facial recognition technologies have led to intense discussions in the field of Public Security throughout the world, due to the increase in the number of cases of **algorithmic racism** that have led to errors in the facial recognition of Black people and sent innocent people to prison. It has also been noted that they are responsible for disseminating structural racism. According to the ***O Panóptico*** project, developed by the Center for Security and Citizenship Studies (**CESeC**), around 90% of prisons in Brazil based upon these technologies target the Black population.

In a limited mapping of the scenario, based upon Brazilian news reports, we identified initiatives developed by both the government and private agents focused on the implementation of surveillance technologies based upon facial recognition in different areas. These initiatives can be found in 56 cities, in 17 states around the country. It can be seen that Bahia is the state where the highest number of these projects have been implemented (15), followed by Santa Catarina (10) and São Paulo (6).

[Graph] Distribution of the 56 initiatives by State



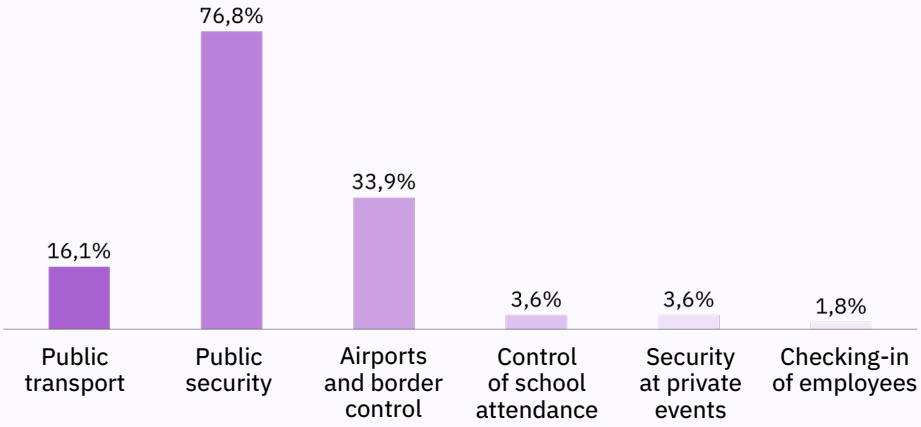
In relation to the distribution of the areas with the most implementation of facial recognition in each state, it can be seen that there are a greater number of states investing in these technologies in the areas of public security[2] and in airports and

2 In this area, the most common use is for locating people considered to be “at large” and for identifying those nsuspected of crimes. Surveillance cameras equipped with facial recognition technologies are distributed around public spaces, managing to digitize a person’s face and automatically match it to a database held by public security authorities.

border control[3]. In public security, for example, the state with the highest proportion of initiatives in this area is Bahia, with 34.9%, followed by Santa Catarina, with 23.3%. In relation to public transport[4], the state that stands out is São Paulo, with 22.2% of the initiatives, whilst the other states adopting these measures have 11.1% each. The state of São Paulo is also of note in the area of airports and border control, since there are a higher proportion of cities with this type of technology being implemented in their airports (21.1%).

If we look at the distribution of the initiatives in the different areas, we can see a predominance in the area of public security (76.8%), followed by airports and border control (33.9%), and public transport (16.1). Furthermore, we can see that facial recognition technologies are being introduced into schools to control attendance rates, for checking on employees clocking in at companies, and for security at private events such as festivals and at stadiums[5].

[Graph] Distribution of the 56 initiatives aiming to implement facial recognition technologies by area of activity



It should be noted that the first initiatives of facial recognition in Brazil were implemented in 2011 (11%), a percentage that had risen to 16% in 2016 and to 37% in 2021 and 2022.

3 Deployment to enable 100% of the boarding procedure to be conducted using facial biometrics technology, as well as identification of people suspected of committing crimes or who have received court sentences, as well as to identify the number plates of cars crossing international borders.

4 The most frequent use in this area has been to confirm the identities of people using public transport who are entitled to travel free of charge, in order to identify fraud by those illegally using travel passes.

5 See the cases concerning the *Mineirão* (Belo Horizonte, MG) and the Oktoberfest (Blumenau, SC) mentioned in the timeline below.

[Timeline] Facial recognition technologies in Brazil

Cases of actual and proposed implementation of these technologies in Brazil and questions concerning their use by researchers and civil society

April 2011

One of the fir t facial recognition systems was implemented in Brazil, in the form of a pilot project undertaken on two public transport bus service providers in the city of Ilhéus (BA). In total, 139 vehicles were equipped with the technology, with the intention of detecting possible cases of fraud involving those receiving free bus passes. The software captured the images of the faces of passengers who boarded the bus and compared them to the photographs registered in the database of people who are entitled to travel free of charge, creating material proof upon which to justify blocking the passes in the event of improper use of the benefit.

August 2011

In partnership with the Police Force, **the Santa Catarina Department of Tourism**, presented plans to monitor public spaces, with the aim of combating violence against tourists through the installation of cameras connected to facial recognition systems in seven coastal towns: Balneário Camboriú, Laguna, Itapema, Navegantes, Palhoça, Bombinhas and Penha. This system is capable of capturing images in real time, analyzing the facial characteristics of the subjects, and comparing them to photos of individuals accused of crimes or who are on the run from the law, immediately alerting the police in the event of recognition.

September 2012

Bus companies began implementing **facial recognition technologies in the entire fleet of vehicles in the city of Caruaru** (PE), to detect whether student or OAP passes were actually being used by the benefit holders themselves. As well as facial recognition, it was announced that the 130 buses serving the city would be equipped with an Intelligent Transport Management System, that would provide online communication between vehicles, and there would be a monitoring unit called an Operational Control Center, which would use 3G communication and GPS navigation technologies.

September 2013

The municipal government of Cascaval (PR) signed an agreement with the ValeSim bus company and the Smart automated solutions development company, for the **installation of a facial recognition system on the fleet of 159 buses serving the municipality**. These biometric devices are aimed at preventing fraud involving those entitled to pay half price on public transport or travel free of charge. This measure was taken following a

40% increase in the use of OAP and student passes on the city's buses. In 2019, it was also **announced** that facial biometry would be expanded and fleet tracking technologies would also be implemented, these being forms of ITS (Intelligent Transport Systems).

June 2014

140 **buses serving the Limeira (SP) public transport system were equipped with a facial biometrics system**, aimed at preventing the improper use of bus passes designed for elderly passengers to travel free of charge and to provide discounts for students. The contract for installation of the system was signed between the concession operators responsible for the transportation and the technology provider company, with no cost to the municipality.

August 2016

The National Transport Confederation announced that a new surveillance system, based upon facial recognition and controlled by the Federal Revenue Service, had started operating in 14 Brazilian airports: Confins (Belo Horizonte-MG), Curitiba (PR), Florianópolis (SC), Porto Alegre (RS), Brasília (DF), Fortaleza (CE), Foz do Iguaçu (PR), Galeão (RJ), Guarulhos (SP), Viracopos (Campinas-SP), Manaus (AM), Recife (PE), Salvador (BA) and São Gonçalo do Amarante (RN). The aim was to identify passengers who pose a potential risk of practicing customs wrongdoings, crimes or infractions.

April 2017

The municipal public schools in Jaboatão (PE) started using facial recognition systems to control student attendance[6], as a cost of R$ 3,000 per school. As well as student attendance, the system would also be monitoring school lunches and whether or not students were actually pursuing their activities.

July 2017

The municipality of Macapá (AP) implemented a facial recognition system on 243 buses serving inter-municipal and urban routes, designed to prevent fraud, after the Amapá Passenger Transportation Companies Union (Setap) noted that 25% of the passengers who used half-price bus passes did not have to right to enjoy such benefit. Cameras installed in the vehicles compared the photos of passengers with the photos registered on the passes. Should different images be detected, the beneficiaries would be called for an in-person check. If fraud were to be confirmed, the benefit would be immediately blocked.

---

6 In **France** and **Sweden**, courts and data protection authorities have stated their opposition to the use of facial recognition to control access to schools and student attendance. These measures were considered to be disproportionate, since they breach the regulations governing the data protection of students who are unable to provide their free consent.

September 2017

In Cuiabá (MT), the Delegated Services Regulation Agency (Arsec) authorized public transport provider companies in the municipality **to implement facial biometrics devices at the onboard bus turnstiles**. At an average cost of R$ 5,000 each, these devices were installed on 60 buses, with the aim of reducing irregularities in the use of free or reduced rate travel by passengers.

April 2018

Municipal schools in Nova **Venécia (ES) tested facial recognition technologies amongst students**. After registering the students in the biometric recognition readers, the system was used, mainly, to eliminate the need to make calls, monitor attendance (informing the parents or guardians of the presence or absence of students via text message) and more accurately calculate the number of meals that need to be cooked on any given day, thus reducing waste.

May 2018

Blumenão Autonomous Municipal Traffic and Transport Service (SC), in partnership with the bus company, **started facial recognition system tests on the city's public transport service**. This system photographs the users of the passes that go through the turnstiles and compares them to detect whether the photographs match with the images of the beneficiaries registered in the public transport system. If any fraud is detected, the pass is blocked.

August 2018

The Personal Data Commission of the Public Prosecutor's Office of the Federal District and Territories (MPDFT) opened **a public civil inquiry to investigate the CredDefense, Certibio and Acesso Digital companies,** due to the suspected illegal sale of biometric data. During the investigations, **Certibio**, which offers digital security services through the cross-referencing of personal data and facial recognition, confirmed that it uses a database, containing the registrations of 70 million Brazilians, that belongs to the Federal Data Processing Service (Serpro). However, Serpro did not have the legal authority to perform transactions involving personal data with private companies.

October 2018

The municipal government of Cariacica (ES) tested facial recognition technology to monitor whether people captured on video-monitoring images had any restrictions pending in relation to them with the State Department of Public Security (SESP). If any restrictions were confirmed, the police would be immediately notified of the suspect's location with the possibility of arrest. However, between 2019 and 2020, no financial investment was made in this program, according to the **'*Portal da Transparência*'**.

December 2018

The Secretary of Public Security, Maurício Barbosa, and the Governor of Bahia, Rui Costa (PT), launched the project **"Police"**. The initiative implemented a system of intelligent video-monitoring to support police actions based upon the use of facial recognition technologies, identification of car number plates, and the sharing of data between police authorities. It also installed 300 facial recognition cameras at a cost to the state of more than R$ 18 million.

December 2018

The **municipal government of Campinas (SP) presented the 'Safe City' Plan, in partnership with** Huawei and the Telecommunications Research and Development Center (CPQD).

Focused on public security, this initiative aimed to install 30 surveillance cameras containing facial recognition systems to identify criminals and missing persons, as well as provide support for the management of traffic and Civil Defense activities. Six of the planned cameras were actually put into operation in the city at this time.

Decembe 2018

The **Urban Transport Companies Union of João Pessoa (Sintur-JP) announced the installation of facial biometrics** technology on 100% of the city's fleet of buses upon signing a contract with Transdata, which had already supplied technology for the fleet in Cascavel, for example.

The aim was to prevent fraud involving passengers with the right to free travel or half-price fares. Since installation of the system in 2019, Sintur has **registered** a considerable amount of fraud.

March 2019

The **fir t prison sentence following facial recognition is registered in Brazil**. During a carnival parade in Salvador (BA), traveling between the Barra and Ondina districts, cameras connected to facial recognition software, installed by the Bahia Department of Public Security (SSP-BA), identified a 19-year-old man as a suspect in a homicide investigation and alerted the police, who arrested him. The state announced that it had invested more than R$ 18 million in this type of technology.

March 2019

Campinas (SP) started testing facial recognition cameras similar to those that helped in the arrest of a fugitive from justice during the carnival in Salvador (BA). The cameras were implemented at the Central Terminal and in the center of the city.

June 2019

The **Prison Administration Department (Seap) implemented a facial recognition system in the Floramar Prison**, in Divinópolis (MG), as a means of more easily checking that the prisoners entering the prison had provided truthful information to the authorities at the time of arrest. Seap announced that the same facial recognition system would also be implemented in another 197 prisons in the state.

September 2019

The **municipal government of Vila Velha (ES) expanded** and modernized the video-monitoring system in the city with the acquisition of 200 new cameras, that were positioned strategically after the violence in the city had been mapped and analyzed. In April 2022, the **press revealed** that the municipal government had performed tests with facial recognition technologies.

October 2019

A monitoring system assisted in the arrest of three people during a large scale event in Blumenau (SC). Police were alerted after confirmation of the existence of outstanding warrants for arrest by a facial recognition system that was in operation together with cameras installed in the Vila Germânica Park, where the traditional Oktoberfest festival was taking place.

November 2019

Facial recognition systems installed in two districts of Rio de Janeiro (Copacabana and Maracanã) assisted in the arrest of 63 people in four months in the city, according to press reports. The technology, provided by the companies Oi and Huawei, was used in partnership with the Rio de Janeiro Civil and Military Police to make the arrests. The system captured images of the people's faces and compared them with 49,000 photographs of people with outstanding arrest warrants contained in the Civil Police's database. Upon identification of at least a 93% similarity between the faces, the police were alerted to approach the suspects.

December 2019

The **'Fronteira Tech' program was inaugurated in Foz de Iguaçu (PR)**, with the installation of 70 facial recognition cameras. According to the Federal Revenue Service, the purpose was to prevent criminal activity, not only by identifying suspects, but also stolen vehicles that had crossed the Amizade bridge (between Brazil and Paraguay). The federal government invested approximately R$ 5 million in the system.

February 2020

The government of **Amapá state started recording the facial biometrics of state public employees**, as a means of automating the production of time sheets. Upon being registered by the equipment, the employee's face is recognized and the location and time of the beginning of the work period is recorded. The information is directly included in the payslip, and a copy sent to the employees' emails.

February 2020

The Bahia Department of Public Security (SSP-BA) announced the arrest of 42 wanted persons during the carnival in Salvador with the help of a facial recognition system. The authority also stated that, as well as the scan performed by the system, some of the arrests were made using the 'Facecheck' application, that crosschecks the fingerprints of suspects detained by police with those held in the Department's database.

March 2020

The Federal University of Paraíba (UFPB) presented a new security system to be installed in its 'I' campus, in the district of Castelo Branco, in João Pessoa. A total of 98 cameras containing facial recognition systems were to be installed, along with an application involving a panic button that will function together with the system. Students, employees and others registered with the application can activate the system should they feel threatened on the campus, allowing them to inform the university security service of their location.

June 2020

The **Municipal government of Curitiba, Rafael Greca (União Brasil), announced that, in partnership with the 'Cidades Inteligentes' Institute (ICI), 500 video-monitoring cameras**, containing facial recognition technology and traffic radars were to be installed, thereby forming a digital security fence around the city. The equipment was installed at strategic points indicated by the crime map of the capital of Paraná, as part of the 'Digital Wall' program, which has similarities with the **'Electronic Walls'** systems installed in other cities, such as Vila Velha (ES). The system was put into operation in Curitiba in **January the following year**.

July 2020

The **'Intelligent City' project was announced by the municipal government of Macapá (AP)**. Budgeted at R$ 5 million, it includes the use of artificial intelligence and other technologies to assist in the city's development. It involves the use of machine learning algorithms integrated into video-monitoring cameras, that provide facial recognition of citizens to assist in the work of the Public Security authorities.

August 2020

Facial recognition system of the Social Defense and Public Security Department (SSPDS) helped the Ceará Civil Police arrest a man accused of being a member of a criminal organization. During the investigations, police photographed the fugitive's partner. The image was submitted to the facial recognition process on the Advanced Command Portal application (PCA), which contains more than eight million registered profiles. After locating the identified woman's residence, the Civil Police managed to arrest the accused, who was hiding there from authorities.

October 2020

The **Federal Government** performed the first test of the 'Boarding + Security' pilot project at the airport of Florianópolis (SC). Created by the National Civil Aviation Department of the Ministry of Infrastructure and developed by the Federal Data Processing Service (Serpro), this project will allow people to board aircraft using facial recognition, without the need to present any documents. After capturing images of the passengers, a unified system will check and validate their identities by means of cross-referencing of the facial biometrics with information from different government databases. A test was performed with 12 people on one flight. It is expected that all airports will be working with this system within three years.

March 2021

The state government of Rio de Janeiro, in partnership with the Integrated Consortium of Public Security of the Baixada Fluminense Region of Rio de Janeiro State (CISPBAF), announced a **monitoring center for surveillance of 17 municipalities within the state**. Municipalities in the **Baixada Fluminense**, as well as the cities of Itaboraí, São Gonçalo, Mangaratiba and Angra dos Reis, started having their streets monitored by cameras equipped with facial recognition software which can also read car number plates. The expected investment was of approximately R$ 15 million. The financial resources for purchase of the equipment was provided by the **Legislative Assembly of the State of Rio de Janeiro (Alerj) in 2019.**

April 2021

The Government of **180 high-definition su veillance cameras** in the city by the end of the year, with facial recognition functions and the ability to read car license plates. The first 41 cameras were purchased using federal resources, through the Infrastructure and Sanitation Financing program (Finisa), following a public call notice that was won by Motorola Solution Ltda., the company now responsible for installation and maintenance of the equipment.

May 2021

The **Federal Government started tests on a facial recognition monitoring system at Belo Horizonte (MG) airport**, part of the 'Boarding + Security' project. Tests were started in October 2020, designed to enable 100% of the boarding process to be performed using facial biometrics. The project formed part of the Federal Government's Digital Transformation Program, an initiative coordinated by the Under-secretariat for Strategic Management, Technology and Innovation (SGETI), answerable to the Executive Department of the Ministry of Infrastructure. The technology was developed by the Biomtech, Wolpac and Azul/Pacer companies.

July 2021

The Governor of Bahia Rui Costa (PT) presented an **expansion of the 'Video Policing' Project**: Itabuna, Ilhéus, Guanambi, Teixeira de Freitas, Porto Seguro, Eunápolis, Itamaraju, Valença e Barreiras, Feira de Santana, Alagoinhas, Santo Antônio de Jesus, Jequié and Vitória da Conquista were to form part of the list of 77 municipalities in the state with vehicle license-plate tracking and facial recognition systems. The project, budgeted at approximately R$ 665 million, involves the provision of services for a period of five years by a consortium made up of Oi SA and Avante SA, the companies which won the bidding process. According to **Intercept**, with the inclusion of this project, Costa is making Bahia a "laboratory of facial recognition surveillance".

August 2021

The **Leite Lopes Airport, in Ribeirão Preto (SP)**, started tests for passenger boarding using facial recognition technology, as part of the Federal Government's '100% Digital Boarding + Security' program. With the adoption of this system, passengers no longer need to present their identification documents or a boarding card to be able to travel, since the entire process will be performed using facial recognition.

August 2021

Planned targets for public security in São José (SC) aimed to expand the video-monitoring to all the city's neighborhoods, including cameras capable of performing facial recognition and the installation of totems (digital security systems) in all of the city's public squares. In February 2022, the **municipal government** reported an improvement in the locating and identification of the perpetrators of theft, robbery, burglary, assault, and the dealing or use of drugs, which was attributed to the work of the Video-Monitoring Center working with biometric identification technologies.

February 2022

The Civil Police **arrested a fugitive from justice with the help of facial recognition cameras installed in the Juazeiro (BA) Produce Market.** The Municipal Supply Authority (AMA), the organization that manages the market, alerted the police the moment that the monitoring system, made up of 53 cameras, identified a man who had a warrant out for his arrest on suspicion of homicide in the state of Pernambuco. Civil police immediately sent a team of officers to the location and arrested the suspect.

February 2022

A device involving what is called **"Hyper-Converged Infrastructure – (HCI)"** was announced as a means of combating crime in Vitória (ES). A total of 150 cameras, each equipped with facial recognition, were installed for the urban monitoring of the state capital, at a cost of R$ 15 million to the public funds. The tool will be capable of locating vehicles that are operating illegally, people with outstanding arrest warrants and crime suspects, all in real time, as well as locate persons carrying guns or dangerous objects.

March 2022

The **Municipal Government of Recife announced that a public notice would be issued for a Public-Private Partnership** aimed at installing 108 clocks containing advertising and information such as the time, air quality and temperature, as well as facial recognition surveillance **cameras**. At a public hearing, town councilors and members of civil society opposed the public notice due to concerns over violations of the right to privacy, algorithmic racism and a lack of transparency concerning the operation of the technology and purpose of the cameras. The public notice offered a 20-year service provision concession to the successful bidding company.

March 2022

The Minas Gerais Soccer Fans Court, together with the Biomtech technology company, **inaugurated facial recognition cameras at the Mineirão soccer stadium, in Belo Horizonte**. The aim was to prevent illegal acts, such as entrance without paying and involvement in fights. People caught committing an illegal act in the stadium would be registered in the biometrics facial system. By doing so, it would be possible to guarantee the implementation of measures designed to prevent persons prohibited from entering the stadium by court order from doing so, using facial recognition systems capable of identifying them when cross-referenced with the registered database. Following the adoption of this system, **three people were apprehended**.

March 2022

A court prevented the operation of the São Paulo subway system's facial recognition system, following a court decision in favor of the Civil Class Action filed by the Public Defender's Office of São Paulo and the Union, the Brazilian Consumer Defense Institute (IDEC) and civil society organizations, in August 2018. The entities alleged that the recognition system on the subway violated citizens' rights and did not respect the legal requirements for the collection of personal data set forth in the LGPD, in the Public Services Users' Code, the Child and Adolescent Statute, the Federal Constitution, and international treaties. Via Quatro, the subway operator, confirmed that the system had been installed for statistical purposes to estimate the flow of passengers.

[Timeline] National Congress Bills of Law concerning facial recognition, biometric data and artificial intelligence

Pending Bills of Law (PL) concerning issues involving the use of these technologies between 2017 and 2021

December 2017

PL 9,414 makes it obligatory to install digital fingerprinting and facial recognition on collective public transport, as a means of preventing benefit fraud (free travel and fare reductions) granted by the government to citizens for access to public transport.

March 2018

PL 9,736 makes the presence of facial recognition systems obligatory in prisons throughout the country. It includes in the Criminal Enactment Law identification by means of facial recognition methods for all those being held in prisons.December 2018

PL 11,140 establishes that, not only prisoners, but also public employees, service providers and visitors should all be identified by the biometric system to gain entry to prisons.

August 2019

PL 4,612 is intended to regulate the development and use of facial and emotional recognition technologies for the identification of people, as well as analyze or predict their behavior. This is justified by the need to regulate a new area of expanding technology.

February 2020

PL 329 aims to make electronic payment obligatory for journeys made using private transport, as well as facial or biometric registration of the passengers. This bill aims to reduce violence against drivers whose work involves digital platforms and establishes the need to identify criminal records of passengers traveling on journeys booked using applications.

February 2021

PL 572 creates the National Facial and Digital Recognition Database, made up of the facial records of minors under the age of 18, collected upon registration of their identity. It aims to make it easier to locate missing children and adolescents.

October 2021

PL 3,714 aims to make alterations to the Code of Criminal Procedure so that facial recognition by photographs is obtained, preferentially, from official organs (public authorities) and that it is used in all phases of a criminal case. This is justified by the number of errors made in decisions that use photographs as the sole and principal evidence against the defendants, often leading to unjust decisions.

March 2022

PL 745 alters Law n° 13,812/2019 concerning the National Policy on the Search for Missing Persons which created the National Missing Persons Register and altered the Child and Adolescent Statute (Law n° 8,069/1990), to deploy and regulate the use of facial recognition data involving minors. This is justified as a response to the large number of minors who go missing each year.

Vigilantism and Digilantism

We have already looked at how people are monitored by both the State and by private companies and the risks that this creates for individuals and for democracy. However, within this risk matrix we also need to include the direct activity of parastatal groups and individuals who, due to a lack of action or perhaps even with the encouragement of the government, decide to take direct action, outside the law, when they feel threatened. These groups and individuals act to resolve alleged problems involving security or employment, perhaps exacerbating particular misunderstandings about difference or the 'other'. Vulnerable groups end up being the preferred targets of this type of activity. And "taking justice into their own hands" results in physical or psychological violence against people.

Vigilante activity is recurrent in Brazil, since violence is seen as by part of the public as playing an educational role and the State's security policy ends up leaving space for groups to act outside the law and individuals feeling the need to take the law into their own hands.

Below we highlight the fundamental concepts for an understanding of the debate surrounding vigilantism, be it in the physical or virtual environment.

Vigilantism

Vigilantism is connected to the exercising of control over the lives of others through the violation of basic rights guaranteed by laws. The first fundamental point is the idea that, due to an insufficient response to social demands, negligence, or a lack of resources from the State, groups appear which independently attempt to resolve supposed problems in a manner that is, in the majority of cases, violent and outside the law. As such, vigilantism can be undertaken by individuals or organizations without any ties to the government, through the imposition of rules and punishments that are not set forth in legal provisions, or which are set forth but should be performed by the proper authorities.

The act of taking the law into one's own hands, that often takes the form of murders, lynching and other crimes, is a categoric example of vigilantism by private individuals or groups. Such groups, which use institutional violence and mechanisms to persecute and intimidate, with the aim of controlling territory or pursuing any other way of undermining the rights of citizens, such as militia groups or criminal outfits, can also be categorized as forms of vigilantism.

Vigilante actions, moreover, can stem from state authorities, such as in cases where the government does not take direct action, but rather encourages acts of violence, or intolerance or persecution of people or groups, through speeches, for example.

Digilantism (digital vigilantism)

This relates to the undertaking of vigilantism through digital mediums. **Digital vigilantism**, also referred to as 'digilantism' or 'cyber-vigilantism', occurs when information technologies connected to the Internet are used by individuals, groups or public authorities for criminal practices, such as inciting crime, invasion of privacy, or spying, or for other actions that are not necessarily crimes, but which generally cause severe damage, as is the case with virtual lynching.

Year after year, there has been a rise in the number of cases in which the victims of virtual lynching, throughout the world, lose their jobs, suffer attacks or commit suicide, after having their privacy or political opinions exposed on the Internet, sparking thousands of hate messages and death threats.

The idea of taking the law into one's own hands is a feature of digital vigilantism, generally taking form when organized groups or individuals commit crimes under the pretext of fighting other crimes, as in the case of the Anonymous group of hackers, which published a list online containing the personal date of supposed pedophiles. A failure by the public authorities to shore up the gaps in legislation, security actions and the lack of infrastructure for the supervision of virtual environments, also encourages digital vigilantism.

Types of actions that can be considered vigilantism

Below we highlight situations that can be considered vigilantism, both within and outside the virtual environment, including some examples of cases that were extensively covered in the media.

1. Cases in which groups working in parallel, such as militias, death squads and other vigilante groups practice vigilantism as a way to maintain or strengthen their control over certain territories and prevent crime. By doing so, they punish those who threaten

their power in any way (e.g. if someone complains about a charge demanded by the group) or who break the rules imposed on that territory (e.g. failure to pay a security charge, use or sale of illegal substances, or committing a crime or infraction). The punishments may vary in type and intensity, involving physical violence (a beating or public lynching), violence against property or assets (theft of a business' equipment) or even death. The violence is exercised as a means of educating or exacting revenge, in the sense that it reinforces the authority that the groups hold. In the case of death squads, these groups generally aim to punish those who are accused of committing crimes or take revenge for the death of members of the group.

- In Rio de Janeiro in the 1960s, accusations started to appear of executions performed by an organized group of police officers following the death of the famous Civil Police detective Milton Le Cocq, in 1964, during a shootout with one of the most wanted criminal suspects in the state capital at the time, Milton Moreira, known as 'Cara de Cavalo' or 'Horseface'. The death of Le Cocq led to the rise of the country's most famous death Squad, the **"*Escuderia Le Cocq*" ('Le Cocq's Shield')**. Created to avenge the detective's death, the group mobilized a great many police officers who voluntarily participated in the pursuit of the murderer, who was killed just a few days later, the victim of more than 50 bullet wounds. **The squad was active between the 1960s and 1980s, coming to an end in the 2000s.** At least 1,500 people were killed in the state of Espírito Santo alone.

- **The Death Squad is established in São Paulo in the 1960s, following the military coup,** and starts operating more forcefully, and together with the State, in the execution of "suspects" and "bandits". Between 1968 and 1969, the squad in São Paulo started operating as an independent group and acting as part of the political repression of the dictatorship. In the book "***Rota 66 - A História da Polícia que Mata", the journalist Caco Barcellos highlights that the group known as the 'Rondas Ostensivas Tobias de Aguiar"*** **(ROTA) assumed a role of social cleansing through exterminations** in the state of São Paulo. The 'ROTA', and its continued operations in police forces after the end of the dictatorship, represent the "institutionalization" of the Death Squad due to its violence and number of deaths.

- In the early hours of July 23, 1993, eight boys are shot to death by a group of police officers near the Candelária Church, in the center of Rio de Janeiro. The armed police officers Marcus Vinicius Emannuel Borges Vargas, Nelson Oliveira dos Santos, Marco Aurélio Dias de Alcântara and Arlindo Afonso Lisboa Júnior are convicted for the crime, known as the "Candelária Massacre". The massacre was performed as revenge against the children living on the streets in the vicinity of Candelária who, the previous day, had thrown stones at a police vehicle driven by Marcus Vinicius, in protest against the arrest of Nilton and Ruço, two boys who lived there.

- On August 29, 1993, 22 people are killed in the district of Vigário Geral, in the North Zone of Rio de Janeiro, one month after the Candelária Massacre. Those responsible for the crime were members of a group known as the "*Cavalos Corredores*" ("Running Horses") - due to their habit of violently entering favelas, running around like wild horses and shooting at random. The group consists of police officers from the 9th Military Police Battalion of Rocha Miranda, also in the North Zone. The massacre is a reprisal by the group for the murder of a police officer, allegedly committed by drug dealers from the Vigário Geral favela. None of the twenty-two people killed had anything to do with drug dealing.

- Between August 19 and 22, 2004, ten people living on the streets near the Praça da Sé main city square in São Paulo, are killed by blows to the head, by a group of armed police officers and private security guards, aimed at silencing possible witnesses to the group's involvement with drug dealing.

- In 2005, 30 people are shot by armed police officers in the cities of Nova Iguaçu and Queimados, in the Baixada Fluminense region of Rio de Janeiro state, in retaliation for the arrest of police officers from the 15th Military Police Battalion of Duque de Caxias. Dissatisfied with the approach being taken by the battalion's new commanding officer, the police officers shoot at random in different locations of the cities on March 31, 2005, killing 29 people.

2. Another act considered to be vigilantism worthy of mention is that of lynching. These types of group actions designed to punish those accused of crimes or violations have occurred throughout history. Whilst in the case of militia groups, death squads, or other vigilante groups, surveillance is undertaken to prevent crime, "typical" lynchings" are the result of a sudden, spontaneous or irrational decision by the lynchers. Lynchings are often based upon decisions taken in the heat of the moment, fueled by hate or fear, with the accusers almost always remaining anonymous. The lynchers feel no need to have to present any proof upon which to base their suspicions and the victim has neither the time or opportunity to prove their innocence. It is a judgment without a neutral judge or the possibility of appeal. Social media has also performed a role in the spreading of rumors and photos of alleged crimes, contributing to lynchings taking place - both physically and online. We can highlight cases in which people are accused of a crime and are the target of violence, such as beatings (in some cases to death) or binding victims to posts, amongst other acts.

    - Three brutal murders shocked the country in 1990, in a case that came to be known as the **Matupá Massacre.** When the police arrived at a house in the city of Matupá (MT), following reports of a break-in, the three men who had broken in took a family hostage. During negotiations to free the hostages lasting more than 15 hours, the neighbors gathered around the house to watch the events unfold. After the criminals had given themselves up to the police and released the hostages, the townspeople caught them and took them to the main square in the town, where they were shot, hung and burned alive. The images were recorded

by the amateur filmmaker Leno Durrewald, and released to the media, leading to national repercussions. In total, **18 defendants** accused of the crime went to trial by jury.

- In 2014, **an adolescent is beaten and bond to a pole with a bicycle chain in the district of Flamengo, in the South Zone of Rio de Janeiro**, after being accused by residents of being a **known thief** in the region.

- In 2015, **a man is tied to a post and beaten to death by a group of residents**, after being suspected of the attempted robbery of a bar in São Luis, Maranhão.

- In 2020, during the first months of the Covid-19 pandemic in Brazil, the States started to set up emergency hospitals due to the increased number of cases and hospitalizations. In the midst of a crisis involving certain governors and a tendency to negate the seriousness of the situation, President Bolsonaro asks his supporters to "find a way" to get into the emergency hospitals and film whether the hospital beds are actually occupied or not. This triggered a **series of hospital invasions**, despite the risk of contagion.

3. The cases of violence and justice at the hands of the people place not only Brazilians in their sights. Cases of violence against immigrants and refugees have become increasingly recurrent. They arise directly from what can be called xenophobia, a feeling of hostility towards a person or persons due to their nationality.

   - In 2010, Haiti is destroyed by an extremely heavy earthquake. The catastrophe and the ensuing economic crisis led thousands of Haitians to migrate to other countries, and Brazil is one of the main destinations. However, Brazilian cities do not have sufficient shelter to house the immigrants and refugees in situations of vulnerability. During the years that followed, there were numerous violent attacks against Haitians. In 2015, **six Haitians** are **shot** in the center of São Paulo. From the information provided by '***Missão Paz***' and by the victims, they were on the steps of a church which offered aid to immigrants, in the São Paulo district of Glicério, when one of those responsible for the attack drove past in a car, with three other people and, before shooting, shouted: "Haitians, you stole our jobs!"

   - A similar situation involving Venezuelan immigrants occurred in Roraima. The Brazilian town of Pacaraima, on the border with Venezuela, **started receiving thousands of refugees in 2016**. In August 2018, following the hold up of a store, a fire to **the tents and belongings of Venezuelan refugees**, accusing them of the rise in violence in the town. Videos show Brazilians shouting "set it on fire" and carrying pieces of wood and rocks. In March 2021, the Federal Police storm a refugee camp in Pacaraima and take 55 Venezuelan women and children away for deportation. In August, an investigation by the press revealed that the Army had created a detention area in Boa Vista, where indigenous Venezuelans were being illegally held and tortured.

4. We should also draw attention to cases of vigilantism that occur online, which have different names and affect the lives of those affected in different ways. Vigilante actions on the Internet can include (a) publicly accusing someone of guilt (blaming); (b) attacks designed to uncover people (debunking); (c) public shaming; (d) digital lynchings that involve persecution and attacks designed to destroy someone's reputation, which can impact their lives outside social media; (e) the search for and publication of a person's private data (addresses, car license plates, social media information and other data) and use of these data for blackmail, threats, extortion or virtual humiliation; and (f) other cases that involve death threats and other forms of harassment and psychological violence. Very often, online vigilantism and intimidation is not taken seriously. Professor Danielle Citron, of the University of Maryland (US), **performed a study on reactions to hate crimes in the cyber-environment** and found that many death and rape threats on the Internet are considered 'inoffensive'[7].

   - This is the case with Débora Diniz, a professor at the University of Brasília (UnB), who left Brazil with her family in **September 2018**, due to Internet harassment, virtual lynching and death threats, following advice from the Government's **Program for the Protection of Defenders of Human Rights**. She is an activist for women's reproductive rights who has been an active voice in the public sphere beyond academic circles **for more than 20 years**. There has been a marked increase in attacks since May 2018, especially after a public hearing was held within the sphere of the Federal Supreme Court in August concerning the decriminalization of abortion during the first months of pregnancy. The threats, however, **were not restricted** to the professor and her family, but were also directed to her students, colleagues and the UnB Rector. Even in self-imposed exile, Débora Diniz says she feels threatened and receives aggressive e-mails.

   - Another famous case of online harassment involves the Federal University of Ceará professor and feminist blogger Lola Aronovitch. Since 2008, Lola has been posting the "Write Lola, Write" blog, which has a feminist perspective and covers a range of issues. **For more than a decade misogynistic trolls have targeted it, making hate attacks on social media,** and she and her family regularly receive threats to their lives. She has filed numerous police reports, but the Women's Protection Police Department in her city says it does not have the resources to perform the investigations, since it involves complex activities, such as breaking the confidentiality of a site hosted overseas. Furthermore, the Federal Police Department says that investigation of this type of crime does not fall under its jurisdiction. The professor is also the target of 'doxing', that is, illegal publication of personal data on the Internet.

7 Citron, D. (2014). Hate Crimes in Cyberspace. Cambridge, MA: Harvard University Press.

- In March 2021, the **YouTuber Felipe Neto** is notified by the Rio de Janeiro Civil Police to make a statement in an investigation into an accusation filed against him of libel and violation of the National Security Law (LSN) - revoked in August that same year - due to his accusation against President Bolsonaro of genocide. In September 2020, the Federal Deputy José Medeiros (Podemos - MT), along with politicians aligned with the opposition, also requested the opening of an inquiry to investigate the YouTuber of participation in a political act declared to be 'anti-fascist'. According to Neto, "since the first day of the government", he has constantly been receiving threats, with the requests for the opening of an inquiry being just the surface of the "full on persecution" that he has suffered. After an interview with the New York Times newspaper, in 2020, in which he accused President Jair Bolsonaro of terrible handling of the pandemic, the YouTuber is accused of pedophilia on social media, something for which he has also been accused on other occasions. The social influencer is also accused of corruption of minors due to the audiovisual content he produces.

Organizations leading the way in Brazil and elsewhere

The study sought to map civil society organizations that work with the issue of surveillance and vigilantism, either directly or indirectly. The first stage of the system involved research and information collected on Internet search engines (Google, etc.) and in publications, using key words[8] linked to the issue of surveillance and vigilantism. Following this, the study listed the organizations that published the discovered documents or are listed in them. Next there was a preliminary investigation that was, admittedly, non-exhaustive, since it was limited to those organizations that publish materials in the two languages used in the study (Portuguese and English).

We identified 48 organizations with head offices in 17 countries on five continents (**see list on page 51**) (see list on page 51). We were unable to identify any organizations located in Oceania. The map below shows the locations of the host countries.

8 Key words in Portuguese used included: *relatório, pesquisa, estudo + vigilância, vigilância estatal, vigilantismo, vigilantismo digital, reconhecimento facial, viés de reconhecimento facial, inteligência artificia , proteção de dados, proteção de dados pessoais, direito digital, dados biométricos, biometria, tecnoautoritarismo, monitoramento, tecnologias espiãs, softwares de espionagem, espionagem, Pegasus, viés algorítmico and racismo algorítmico, amongst others.* Translations of the same words in English were also used: *report, research study + surveillance, state surveillance, vigilantism, digital vigilantism, facial recognition, facial recognition bias, artificial in elligence, data protection, digital rights, personal data protection, biometric data, biometrics, techno-authoritarianism, monitoring, spy technologies, spying software, spying, Pegasus, algorithmic bias*, and *algorithmic racism*, amongst others.

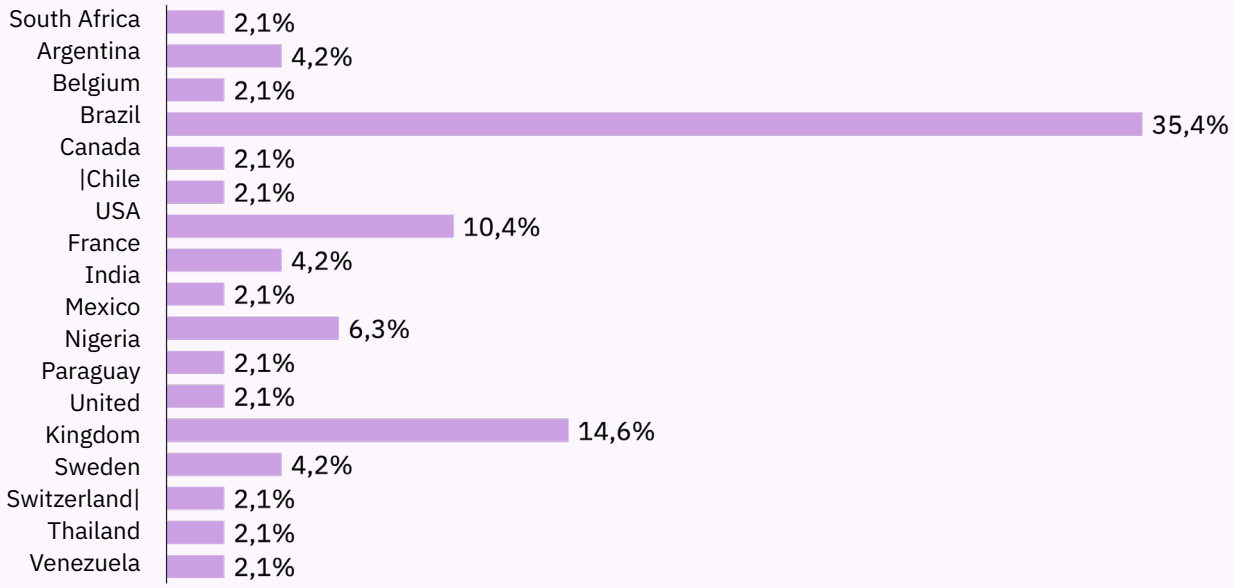
[Map] Countries in which the organizations have head offices

Key: nº number of head offices of organizations present in the country.

An analysis of the distribution of the organizations across the 17 countries shows that the highest percentage of organizations is to be found in Brazil (35.4%), followed by the United Kingdom (14.4%) and the United States (10.4%). This could be related to a number of different factors connected to the history of our country, such as the period of military dictatorship and the "**authoritarian debris**"[9], and the need to protect the individual rights and personal data that are the target of state and private surveillance.

9 The expression "*entulho autoritário*", or "authoritarian rubble", was first used in 1979 by the opposition to the military president João Baptista Figueiredo, to refer to the chaotic Brazilian legal system following the repeal of institutional acts and decrees of exemption imposed by the dictatorship. Despite the repeal of the institutional acts, laws and institutions remained in the legal system with the authoritarian leaning of the military dictatorship. This is the case with **National Security Law**, that has been used in recent years to justify the arrest of people who protest against the federal government.

[Graph] Distribution of the organizations according to host-country



In relation to the founding years of the mapped organizations, it is possible to note a certain distribution over the last century (1920-2020). There are organizations that have existed for more than 100 years and others that have been created more recently.

One fact of special note is that more than 35% of them have been created since 2014, with a concentration in 2018 (12.5%). This could be explained by the increasingly rapid appearance of new technologies and surveillance mechanisms developed by the State and large corporations over recent decades.

By using publications released recently by these organizations, we have mapped the main themes these organizations have been working with and which are either directly or indirectly connected to surveillance, vigilantism and discriminatory practices.

By analyzing the 48 organizations, we have been able to note that 93% of them have performed research or worked with matters connected to surveillance by the State, while 77% are focused on issues related to freedom, privacy and the protection of personal data.

Another issue that has been addressed in great detail by these organizations (62%) is the monitoring or civil society by the State and by private agents, which sometimes results in cases of violence against activists, journalists, human rights defenders, those protesting against authoritarian regimes or civil society in general. As well as addressing the monitoring of civil society, there are some organizations that work in different ways to protect those operating in defense of human rights (37.5%). This can

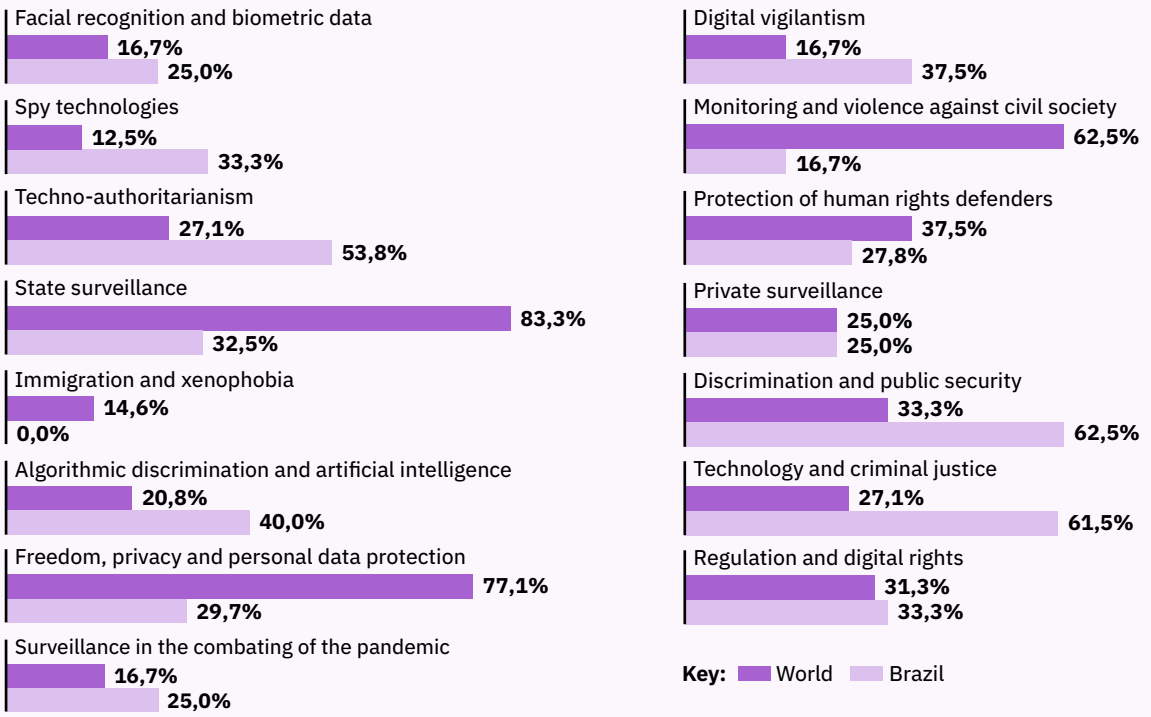
be added to the issue of techno-authoritarianism[10], that has been addressed by 27% of the mapped organizations, and to the acquisition of spy software (such as Pegasus) by different States (12.5%).

Furthermore, as we noted in item 3 of this report, the debate is growing in relation to the issues surrounding algorithmic discrimination and the use of artificial intelligence (20.8%), facial recognition technologies (16.7%) and how their use could result in cases of discrimination in the area of public security (33%) and affect court decisions in the criminal sphere (27%).

Finally, we have seen a notable rise in the discussions concerning digital rights and the regulation of new technologies (31%), with the aim of protecting citizens' freedom, privacy and personal data.

If we look at the distribution of the issues solely amongst Brazilian organizations, we can see that discrimination in the area of public security is the most highly addressed issue (62.5%), followed by the debate surrounding technology and criminal justice (61.5%) and techno-authoritarianism (53.8%). Also worthy of note is the discussion surrounding algorithmic discrimination and artificial intelligence (40%), and digital vigilantism (37.5%).

[Graph] Distribution of organizations according to the main issues analyzed



10 For more information on this issue, see: **https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/.**

The organizations, where they are, and the areas in which they operate

South Africa

Civicus (1993)

Areas of activity: freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of human rights defenders | techno-authoritarianism | state surveillance

Access the site ↗

Argentina

Asociación por los Derechos Civiles – ADC (1995)

Areas of activity: algorithmic discrimination and artificial intelligence | freedoms, privacy and personal data protection | monitoring and violence against civil society | state surveillance

Access the site ↗

Consejo Latinoamericano en Ciencias Sociales – CLACSO (1967)

Areas of activity: monitoring and violence against civil society | surveillance in the combating of the pandemic | digital surveillance

Access the site ↗

Belgium

Protection Internacional (PI) – (1998)

Areas of activity: monitoring and violence against civil | protection of human rights defenders | state surveillance

Access the site ↗

Brazil

Centro de Análise da Liberdade e do Autoritarismo – LAUT (2020)

Areas of activity: discrimination and public security | freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of human rights defenders | regulation and digital rights | techno-authoritarianism | technology and criminal justice | state surveillance

Access the site ↗

Coalizão de Direitos na Rede (2016)

Areas of activity: algorithmic discrimination and artificial intelligence | freedoms, privacy and personal data protection | regulation and digital rights | techno-authoritarianism | spy technologies | state surveillance | private surveillance | digital surveillance

Access the site ↗

Coding Rights (2015)

Areas of activity: freedoms, privacy and personal data protection | techno-authoritarianism | state surveillance

Access the site ↗

Conectas Direitos Humanos (2001)

Areas of activity: algorithmic discrimination and artificial intelligence | discrimination and public security | freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of human rights defenders | regulation and digital rights | techno-authoritarianism | spy technologies | technology and criminal justice | state surveillance

Access the site ↗

Data Privacy Brasil (2018)

Areas of activity: algorithmic discrimination and artificial intelligence | freedoms, privacy and personal data protection | regulation and digital rights | techno-authoritarianism | state surveillance | surveillance in combating the pandemic | digital surveillance

Access the site ↗

Datalabe (2016)

Areas of activity: discrimination and public security | state surveillance

Access the site ↗

Fiquem Sabendo (2018)

Areas of activity: discrimination and public security | freedoms, privacy and personal data protection | technology and criminal justice | state surveillance

Access the site ↗

Iniciativa Direito à memória e Justiça Racial – IDMJR (2018)

Areas of activity: discrimination and public security | technology and criminal justice | state surveillance

Access the site ↗

Iniciativa Negra (2015)

Areas of activity: discrimination and public security | state surveillance

Access the site ↗

Instituto de Defesa do Direito de Defesa – IDDD (2000)

Areas of activity: discrimination and public security | freedoms, privacy and personal data protection | state surveillance | surveillance in combating the pandemic

Access the site ↗

Instituto Igarapé (2011)

Areas of activity: discrimination and public security| freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of human rights defenders | facial recognition and biometric data | techno-authoritarianism | technology and criminal justice | state surveillance | private surveillance

Access the site ↗

InternetLab (2014)

Access the site: freedoms, privacy and personal data protection | techno-authoritarianism| state surveillance| private surveillance

Access the site ↗

Instituto Vero (2020)

Areas of activity: freedoms, privacy and personal data protection | regulation and digital rights | digital vigilantism

Access the site ↗

Justiça Global (1999)

Areas of activity: discrimination and public security | monitoring and violence against civil society | protection of human rights defenders | technology and criminal justice

Access the site ↗

Observatório de Favelas (2001)

Areas of activity: monitoring and violence against civil | protection of human rights defenders | state surveillance

Access the site ↗

O Panóptico (2018)

Areas of activity: algorithmic discrimination and artificial intelligence | discrimination and public security | freedoms, privacy and personal data protection | facial recognition and biometric data | technology and criminal justice

Access the site ↗

Canada

The Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto (2001)

Areas of activity: algorithmic discrimination and artificial intelligence | immigration and xenophobia | freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of human rights defenders | regulation and digital rights | techno-authoritarianism | spy technologies | state surveillance | surveillance in the combating of the pandemic | private surveillance | digital surveillance

Access the site ↗

Chile

Derechos digitales (2005)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | technology and criminal justice | state surveillance

Access the site ↗

USA

American Civil Liberties Union – ACLU (1920)

Access the site: algorithmic discrimination and artificial intelligence | discrimination and public security | immigration and xenophobia | freedoms, privacy and personal data protection |facial recognition and biometric data | state surveillance | private surveillance

Access the site ↗

The Advocates for Human Rights (1983)

Access the site: immigration and xenophobia | freedoms, privacy and personal data protection | state surveillance

Access the site ↗

The Association for Women's Rights in Development – AWID (1982)

Access the site: freedoms, privacy and personal data protection | protection of human rights defenders

Access the site ↗

Eletronic Frontier Foundation (1990)

Access the site: freedoms, privacy and personal data protection | state surveillance | private surveillance

Access the site ↗

Human rights watch (1978)

Access the site: algorithmic discrimination and artificial intelligence | discrimination and public security | immigration and xenophobia | freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of defenders of human rights | facial recognition and biometric data | regulation and digital rights | techno-authoritarianism | spy technologies | technology and criminal justice | state surveillance | surveillance in the combating of the pandemic | private surveillance | digital surveillancel

Access the site ↗

France

International Federation for Human Rights – FIDH (1992)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of human rights defenders | regulation and digital rights | techno-authoritarianism | spy technologies | technology and criminal justice | state surveillance | private surveillance

Access the site ↗

TRIAL International (2002)

Access the site: immigration and xenophobia | monitoring and violence against civil society | state surveillance | private surveillance

Access the site ↗

India

India Civil Watch – ICWI (2018)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of human rights defenders | state surveillance

Access the site ↗

Mexico

Centro de Derechos Humanos Fray Bartolomé de Las Casas (1989)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | state surveillance

Access the site ↗

Observatorio Contra a Tortura (2019)

Access the site: freedoms, privacy and personal data protection | state surveillance

Access the site ↗

Red en Defesa de los Derechos Digitales (2015)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | facial recognition and biometric data | regulation and digital rights | state surveillance

Access the site ↗

Nigeria

Global Rights (1978)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | state surveillance

Access the site ↗

Paraguay

TEDIC – Technology, Education, Development, Investigation, Communication (2012)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | facial recognition and biometric data | regulation and digital rights | state surveillance | surveillance in combating the pandemic

Access the site ↗

United Kingdom

Anistia Internacional (1961)

Access the site: algorithmic discrimination and artificial intelligence | discrimination and public security | immigration and xenophobia | freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of defenders of human rights | facial recognition and biometric data | regulation and digital rights | techno-authoritarianism | spy technologies | technology and criminal justice | state surveillance | surveillance in the combating of the pandemic | private surveillance | digital surveillance

Access the site ↗

Artigo 19 – Article 19 (1987)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of human rights defenders

Access the site ↗

Big Brother Watch (2009)

Access the site: algorithmic discrimination and artificial intelligence | discrimination and public security | freedoms, privacy and personal data protection | monitoring and violence against civil society | facial recognition and biometric data | regulation and digital rights | techno-authoritarianism spy technologies | technology and criminal justice | state surveillancel

Access the site ↗

Global Partners Digital (2014)

Access the site: freedoms, privacy and personal data protection | protection of human rights defenders| regulation and digital rights | state surveillance | private surveillance

Access the site ↗

Minority Rights Group Internatoinal – MRG (1969)

Access the site: monitoring and violence against civil society

Access the site ↗

International Bar Association – IBA (1947)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of human rights defenders | regulation and digital rights | techno-authoritarianism | state surveillance | private surveillance | digital vigilantism

Access the site ↗

Privacy International (1990)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | state surveillance

Access the site ↗

Sweden

Civil Rights Defenders (1982)

Access the site: discrimination and public security| freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of human rights defenders | regulation and digital rights | state surveillance | surveillance in the combating of the pandemic

Access the site ↗

Varieties of Democracy – V-Dem (2014)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | state surveillance

Access the site ↗

Switzerland

MENA Rights (2018)

Access the site: immigration and xenophobia | monitoring and violence against civil society | state surveillance

Access the site ↗

Thailand

Assistance Association for Political Prisoners – AAPP (2000)

Access the site: discrimination and public security| freedoms, privacy and personal data protection | monitoring and violence against civil society | protection of human rights defenders | state surveillance

Access the site ↗

Venezuela

Comité de Familiares de Víctimas de Caracazo – COFAVIC (1989)

Access the site: freedoms, privacy and personal data protection | monitoring and violence against civil society | state surveillance

Access the site ↗

Brazilian initiatives that use surveillance to support the population

The vacuum created by the State's failure to act in resolving the problems that exist and the failure to formulate public policies has frequently opened the way for actions of surveillance and vigilantism. As we have seen above, organized groups or individuals have taken advantage of regulation that is either weak and ineffective or simply non-existent to mediate in the future of the public, going above the laws that should ensure integrity, dignity and life in a democratic state of law.

However, the hard work of some individuals and civil society organizations shows us that surveillance can be used to fill the gaps left by the public authorities in a positive manner and with the aim of helping those in vulnerable situations.

Through initiatives that bring together digital technologies with the protection of fundamental rights, applications and other digital platforms have been developed to help the public with social needs that the State fails to see or seems incapable of resolving. Below, we highlight some of the non-governmental organizations and technological tools that have been created to remedy this failing on the part of the state and provide support for the public.

Fogo Cruzado

Lack of public security is a recurring problem, brought about, largely, by the inability of the State to deal with violence in society. Just as serious as the lack of security is the lack, or inaccuracy, of the provision of information to the public about where and how the violence occurs. Finding herself annoyed with the failings of the authorities, the journalist Cecília Oliveira decided to create the **Fogo Cruzado** platform. Between the

end of 2015 and the beginning of 2016, the journalist collected data on shootouts in the city of Rio de Janeiro from her social media networks. Realizing that what she was doing had potential, she then had the idea of transforming it into a digital platform.

Talking to the 'Revoar' podcast, Oliveira explained that "*covering public security, I realized how much information is missing to be able to provide broader coverage, which would provide us with more in-depth analyses that would be closer to the reality. Then, at the end of 2015, I remembered that I'd seen a cover of the 'Voz das Comunidades' newspaper, from the Complexo do Alemão (favela), which highlighted an importan headline: the Complexo do Alemão had reached 100 days without a shootout. But this wasn't being covered by the mainstream press. It was being covered piecemeal, as if these were isolated events, you could say. And at that time, I was looking for information on victims of stray bullets to be able to write an article. But there wasn't enough*".

This was how the '*Fogo Cruzado*' application came into being, officially going on air in September 2016, one month before the start of the Rio de Janeiro Olympic Games. The app monitors information on armed conflicts uploaded by users, partners, media vehicles, and police authority information channels, and then, once the information has been checked, the exact locations of the conflicts are published. Shootouts put not only people's lives at risk, but also have an enormous impact on the daily routines of the public, since many of these events result in the closure of roads, schools and hospitals, alterations to the routes taken by buses, and many other things that affect the daily lives of thousands of people. *Fogo Cruzado* not only helps with this surveillance of the occurrence of shootouts, but also draws attention to these impacts and helps people to organize their daily routines, informing them about road, hospital and subway station closures, rerouted bus lines, and other useful information. At present the collaborative mapping of armed violence also extends to the Greater Metropolitan area of Recife (PE). As well as providing a public information service, these projects are also providing the groundwork for a bill of law designed to allow school principals to be able to independently suspend classes if shootouts occur, whilst they also contribute to institutions related to public security, providing support for the development of strategies that can make public spaces safer.

PenhaS

Brazil is 5th in the ranking of countries with the highest incidence of femicide. Here in Brazil, a **woman is the victim of violence every two minutes**, and **nine out of every ten women** do not trust the official bodies established to provide services specifically for women. This is a dangerous combination that shows the weakness of the public authorities in their provision of support for the victims of this type of violence. The concerns over the sad reality in Brazil, the result of the development of different forms of violence against women in the country, led the **Az Mina Institute to launch the PenhaS application on Women's Day, 2019**. With its name having been inspired by the Maria da Penha Law, this is a form of hotline to which cases of violence against

women can be reported and to provide shelter for these victims. It was developed after listening to specialists and women of different ages, races and social classes who shared their experience about the day-to-day experiences they are forced to endure. The application ensures the caller's complete anonymity. Amongst the features of the app, we should highlight the sharing of information on women's rights, maps showing the locations of women's police precincts throughout Brazil, and the help provided in forwarding women who are the victims of violence to the closest unit providing social support services. The platform includes a panic button which alerts people chosen by the users in case of emergency, as well as allowing a recording of the sound at the location whilst the violence is taking place, thereby allowing the victims to provide evidence against the aggressors.

Serenata de amor

Transparency in public spending is a fundamental component of democracy. The public can only demand more efficient management of funds from the State if it understands how public money is being spent. The Access to Information Law (LAI) establishes that information on the public administration must be published, except in cases of confidential information. Even so, a great deal of information relating to the municipal, state and federal administrations does not reach the public, above all that which relates to the expenditure of public financial resources. Within this context, the ***Serenata de Amor Operation*** was created in 2016. The brainchild of the programmer Irio Musskopf, this project uses data science and machine learning to inspect public spending and share the information, quite simply, with anyone who has access to the Internet.

The initiative works as follows: a robot named **'Rosie'**, an artificial intelligence device developed by Musskopf together with other programmers, analyzes the amounts reimbursed by the Quota for the Exercising of Parliamentary Activity (CEAP) to federal representatives and senators spent in the exercising of their office and identifies patterns of suspicious expenditures. The financial activities monitored are passed on to the "jarbas dashboard", a site where reimbursements to members of parliament can be easily accessed. The "*serenata de amor*" platform has already managed to identify more than 8,000 suspicious reimbursements. Of these, the project reported 626 reimbursements for irregular expenditures involving 216 different congressmen and more than R$ 378,000.

Cocôzap

Basic sanitation is a right that is guaranteed by the Constitution, an infrastructure service that, just like many others, is understood as being essential to guaranteeing dignity and quality of life to the public. Lack of this service can be linked to a series of health risks and an increase in the mortality rate due to contact with waste and the

consumption of untreated water. It is the State's legal duty to guarantee basic sanitation to all citizens (art. 23, item IX, of the **Federal Constitution**), but, as we all know, in practice, this does not happen, as is the case in the 'Maré' favela complex, a district which is home to 140,000 residents in the North Zone of the city of Rio de Janeiro (RJ). To draw the public authorities' attention to the lack of basic sanitation in Maré, the **Data Labe** data laboratory, created the **Cocôzap** project, which maps out the occurrence and participation by the residents in relation to basic sanitation in favelas. The project's staff, along with the '*Casa Fluminense*' and the Maré Development Networks Association, have been working on Cocôzap since 2018, to establish a form of hotline to hold debates, and make accusations and proposals concerning basic sanitation, water supply and garbage collection in Maré through a WhatsApp number.

The system involves a cell phone number containing the WhatsApp platform receiving photos, videos and explanations of the situation involving waste and garbage in Maré, in order to identify the difficulties being faced by the residents in accessing these services that should be provided by the public authorities. A database is being produced with the intention of constructing diagnoses to support and be compared with the official indicators concerning these services. The aim of the project is to pressure the authorities to establish more effective public policies and solutions, based on evidence collected by those who daily experience the effects of the lack of basic services that ought to be guaranteed by the State.

Defezap

The violence caused by direct actions by the State kills thousands of Brazilians every year. Data published in the most recent edition of the **Annual Yearbook of Brazilian Public Security** show that, between 2013 and 2020, the number of deaths as a result of police interventions throughout the country increased over seven consecutive years, culminating in 6,416 deaths in the most recent year recorded, or in other words, more than 17 people per day, in 2020 alone, 99% of whom were men, with the majority being Black men (79%). Of the total number of deaths resulting from police interventions in the country, almost 20% are concentrated in **Rio de Janeiro**. It was this scenario of an explosion in police violence that influenced the **NOSSAS** non-profit organization to create **Defezap** in 2016. This is a form of hotline designed to allow citizens to report violence committed by the State in the metropolitan region of Rio de Janeiro. By means of a WhatsApp number, the Rio population has gained an important ally in the anonymous and safe reporting of any type of violence perpetrated by agents of the State.

2020

Production

LAUT

CENTRO DE ANÁLISE
DA LIBERDADE E
DO AUTORITARISMO

laut.org.br

@Laut_br

@laut-org

@Laut.org

@Laut_br

Support

FORD
FOUNDATION