

The construction of a sociotechnical surveillance network in Brazil

by Pedro Braga, André Sobral, Fernando Severo, Ricardo Jullian, and Henrique Cukierman

Abstract

Young activists in Brazil became targets of state persecution for taking part in the mass protests that took to the streets and the Web during the lead-up to the 2014 World Cup and, subsequently, during the 2016 Olympic Games. The present article is a case study tackling the growth and development of the state's Internet surveillance apparatus and how it was used to suppress young political activists. We begin this paper with a theoretical discussion on the concept of surveillance and how it is inseparable from modern capitalist society. To that end, we used science, technology and society studies as the theoretical foundation for our analysis. Further along, we describe the Brazilian political atmosphere during the mass demonstrations. Lastly, we conclude with an analysis of the personal accounts collected via interviews with the activists that were persecuted and monitored by the state.

Contents

- [1. Introduction](#)
- [2. Building a surveillance network](#)
- [3. Brazil in June of 2013](#)
- [4. The experience of persecution](#)
- [5. Final thoughts](#)

1. Introduction

Surveillance is commonly associated with the idea of an outside observer (human or technological) who scrutinises something or someone. To better understand this concept, the present article will look deeper into it, aiming to incorporate the many ways in which surveillance has been conducted, and what its implications are. This will be achieved through a case study of the protests that took place in Brazil in June of 2013.

The second section will investigate the definition of surveillance, drawing on the science, technology, and society studies (STS) literature, so as to better explore the case study. The third section will go over the events that took place in the country during the period in question. The rise of activist movements, and the responses of the emergent Brazilian state surveillance apparatuses to widespread political protests in the wake of Brazil's hosting of the 2014 FIFA World Cup, will be explored. These demonstrations, it is worth

noting, were inspired by world events such as the Occupy movement and the Arab Spring, which were organised, sometimes virally, in part, by the use of social networks (Croeser and Highfield, 2014; Morris, 2014).

The fourth section will present Tiago, an activist who is part of the Brazilian branch of the international collective called Anonymous (Olson, 2014), and who was persecuted by the police. We will explore the connection between the concepts put forward and the surveillant assemblage (Haggerty and Ericson, 2000) mobilised by the state to enable persecution. The last section will contain our conclusions regarding surveillance, STS, and the experiences faced in the country during that period.

2. Building a surveillance network

What is surveillance? According to Gary T. Marx, surveillance is not the opposite of privacy, though in many cases it “may be the means of crossing borders that protect privacy” [1]. This definition is associated with the process of gathering personal information capable of identifying an individual via electronic, chemical, or statistical methods [2].

In this concept, surveillance is evocative of dystopias such as the one found in George Orwell’s *1984*. In it, the characters are constantly monitored by a totalitarian government through the use of a telescreen — a mixture between a television and a security camera — and its presence is compulsory in every home and all public spaces. This device, which cannot be turned off, enables the regime to monitor its citizens and broadcast propaganda 24 hours a day.

According to David Lyon, Orwell’s work retains its relevance by illustrating what a form of a “surveillance society”. Lyon observes that computer systems, whether they belong to governmental or private entities, contain a range of personal information on the general populace:

Organisations of many kinds know us only as coded sequences of numbers and letters. [...] Precise details of our personal lives are collected, stored, retrieved and processed every day within huge computer databases belonging to big corporations and government departments. This is the ‘surveillance society’. [3]

In *1984*, it is impossible to know whether all the telescreens are being watched at all times, but the population *feels* constantly under watch, identical to the prisoners in a panopticon (Foucault, 2007). Similarly to *1984*, in today’s world it is not possible to know the scope of surveillance:

No one is spying on us, exactly, although for many people that is what it feels like if and when they find out just how detailed a picture of us is available. ‘They’ know things about us, but we often don’t know what they know, why they know, or with whom else they might share their knowledge. [4]

Lyon also argues that no one is being monitored directly, in the sense that there are no spies watching us through a window. We do, however, experience the feeling of intrusion when we realise how computer systems can monitor us by indiscriminately gathering data on their users, even when we attempt to resist [5] this surveillance.

Therefore, surveillance is the “toll” we must pay in order to be able to buy things with credit cards, to access smartphone applications whose functions require geolocation, and to interact with others on social media. Full participation in modern society requires submission to surveillance. In 1994, when these

technologies either did not exist or were in their infancy, Lyon was already using the passport metaphor to discuss surveillance:

Passports get us across borders, whose drivers' licences are taken more seriously than our own word for proving who we are. In much of modern life we deal with relative strangers, and to demonstrate our identity or reliability we must produce documentary evidence. Indeed, the Russian proverb above [6] should really be updated to indicate that human beings would now be defined more accurately as 'body, soul and credit card'. [7]

A striking difference between surveillance described in *1984* and surveillance found in information societies of the twenty-first century (Castells, 1996) has to do with who is doing the surveilling. In Orwell, the totalitarian regime was the only one responsible for surveillance, whereas in our world, surveillance is conducted not only by the state, but also by private entities.

One place in which surveillance is heavily used is inside factories, namely in production lines:

Hence what we now know as 'management' was developed to monitor workers and to ensure their compliance as a disciplined force. The idea of bringing workers together under one roof, in factories and workshops, has often been seen as a way of maximising technical efficiency, making full use of machinery, and so on. But it can equally well be argued that the use of factories to ensure labour discipline through the oversight of workers' activities was at least as important, if not more so. [8]

Another aspect of modern surveillance pertains to large companies and how they increasingly monitor their customers. This practice has become crucial in some cases for these corporations, influencing marketing and business decisions, which range from what services a given company will choose to provide, where it will elect to operate, and what investments will be made. Moreover:

The surveillance of both consumers and their associated consumption contributes to and is reliant upon the 'personal information economy' — a context in which the use of personally identifiable data has become a primary resource and upon which many market economies are built. The personal information economy depends upon the gathering of data through surveillance systems and then analyses this data for patterns and associations deemed to be 'of value,' continually re-evaluating corporate practices and products based on these analyses. This circular process is directed towards obtaining the maximum current and potential profitability from differing sets of consumers. [9]

In this sense, social networks play a leading role in surveillance as they gather a massive volume of information on their users. This data is systematically stored, compared, assessed, and sold, offering an overview of the users' online behaviour (Estevão, 2014). These detailed summaries can then be compared to one another, so as to define profiles and to direct advertising and consumption.

Social networks also play a crucial role in a different kind of surveillance, that of lateral (or "peer-to-peer") surveillance (Estevão, 2014). In it, social media users simultaneously monitor, and are monitored by, one

another while using the social network in question. This type of surveillance can also be used by the state, as was the case with 4chan [10] in 2013, after the Boston Marathon Bombing:

The introduction of social media into the process of searching for the suspects involved in the Boston Marathon Bombing was widely used by the US authorities, mobilizing civil society to help with national security. A noticeable role was played by communities like 4chan, which collected and spread several images of the two suspects. [11]

The 1984 metaphor is also lacking when it comes to describing the surveillance conducted by the modern state. Whereas Orwell's dystopia shows surveillance exclusively as a means to combat threats against the regime, modern states use it in a far more mundane fashion:

It was not until industrialization that states began to collect information on their citizens with any regularity, when methods became more organised, structured, rational and centralised and evolved into what we recognize as the modern bureaucratic surveillance system Migration into new urban areas, communication and transportation revolutions, growth in the electoral franchise, and an increasingly condensed workforce, all led to societies which demanded greater response and accountability from their governments. [12]

In other words, more than just being tyrants who seek to control their citizens, modern states need surveillance to keep their bureaucracies and public services functioning. A country's influence over their citizens' lives is no longer a matter of administering punishment, but an intricate system capable of fostering or disallowing life [13]. According to Weller:

Arguably, "social supervision" can also equate to the management of information on citizens in order to provide for their protection and well-being. In other words, rather than an Orwellian and sinister form of observation and monitoring, state surveillance is justified as a means which benefits the citizen through the application of social welfare. [14]

Thus, we return to our original question: what is surveillance? All the definitions presented in this paper describe the term only in part, being unable to explain a supposed totality that can fully clarify the concept. Just like Deleuze and Guattari's rhizome [15] surveillance should not be viewed as a single thing but as a multiplicity.

Inspired by the rhizome, surveillance systems are described through information flows and intentionality by Haggerty and Ericson (2000) as a "surveillant assemblage":

To speak of *the* surveillant assemblage risks fostering the impression that we are concerned with a stable entity with its own fixed boundaries. In contrast, to the extent that the surveillant assemblage exists, it does so as a potentiality, one that resides at the intersections of various media that can be connected for diverse purposes. [16]

The perception of the inherent complexity of surveillance systems has made, in the last decades, many scholars adopt the surveillant assemblage concept in their theoretical approaches (Arteaga, 2015; Romele,

et al., 2017; Nurik, 2022), such as the adoption of filming by protesters as sousveillance, a counter-surveillance protection against police abuse and how that movement led the police to adhere to the same tactics in a counter-counter-surveillance spiral (Ullrich and Knopp, 2018).

With this rhizomatic aspect in mind, we would not be able to treat the concept as a single unit. We will examine cases of repression towards political dissidents that took place in Rio de Janeiro between 2013 and 2016, which is to say, after the 2013 June Journeys (sometimes called the Brazilian Spring in English) and during the period in which the city experienced its “mega-events” [17].

To tell this story, we took into account social agents — the state, capital, local culture, activists’ political views — as well as machinic agents — the Internet, cameras, wiretaps and cellphones, among others. How do technology and society interact within the scope of surveillance? According to Lyon, some aspects of surveillance appeared before computers, though these social and machinic technologies have a symbiotic relationship, transformed by society as they concurrently transform society:

While new technologies do indeed have a kind of self-augmenting capacity [...] this does not make them immune from sociological scrutiny. The process by which they are augmented is all-too-often a “black box”. We should open the box and analyse the contents; we may well discover some deeply social factors shaping the technologies. [18]

It is worth noting that Lyon bears detects a contradiction: it affirms that society shapes devices used in surveillance, while society is in turn shaped by technology. In other words, one is the product *and* the producer of the other, in a deeply enmeshed relationship. To understand this (re)configuration between surveillance society and the information and communications technologies (ICTs) used for social control, while also looking at outcomes from this relationship, we will use STS as a theoretical benchmark. We will delve deeper and observe how STS can provide tools to understand the creation of digital surveillance networks in Brazil.

One starting point to better understand STS is to recognize how enmeshed and inextricable the social and the technical are, and how it is not possible to determine where one ends and the other begins. Cukierman, *et al.* [19], for example, employ the “socio-technical lens” in order to face the challenge of complexity. Through this lens, society produces, designs, and shapes science, while at the same time is (re)produced, (re)designed and (re)shaped by science. The socio-technical lens breaks barriers imposed by disciplinarity. This is possible because, at the same time that it tackles the mutual configuration that takes place between society and technology, it can “likewise make us think of a configuration that belongs, at the same time, to the exact sciences as well as to the social and human sciences. This is an interdisciplinary (or even transdisciplinary) configuration *par excellence*” [20].

To understand these socio-technical configurations and reconfigurations, one possible path to follow is that of actornetwork theory (ANT). ANT explains science and technology as an output of networked relationships established between human and non-human agents, with no separation between those agents and a network’s structure, as explained by John Law:

Actor-network studies emerged in the sociology of science and technology. With others in the sociology of science, researchers argued that knowledge is a social product rather than something generated through the operation of a privileged scientific method. In particular, they argued that “knowledge” (but they generalise from knowledge to agents, social institutions, machines, and organisations) may be seen as a product or an effect of a network of heterogeneous materials [21].

Law puts quotation marks around “knowledge” to indicate that it is not simply an abstract concept: knowledge always takes material form in some way, be it as an article, a presentation given during a conference, or a patent. Knowledge can also take the form of skills incorporated by scientists and

technicians. According to Law, by recognizing this material aspect of knowledge, ANT is able to explain its origins. As per ANT, knowledge is the end product of the interpretative work done by various heterogeneous actors, human or non-human, operating together [22].

ANT uses the concept of translation, which has two meanings. According to Law, translation can mean the possibility of both equivalence and transformation [23]. Thus, translation indicates the possibility that an entity (human or non-human) may join others (whether by force or by its own volition) in order to work towards an interest that was made common via the “interpretation given by the fact-builders of their interests and that of the people they enrol” [24]. Per Latour, the act of translating plays two different roles in the building of a network of heterogeneous actors: enrolling other actors so that they may take part in the building of facts and artefacts, and controlling the behaviour of said actors so that their actions become predictable [25].

Considering the importance of the complexity of interactions between actors engaged in surveillance networks, it is important to adopt an approach that takes into consideration not only ANT but also sometimes unpredictable and *ad hoc* assemblage contributions to this debate on the resulting surveillance topography. Both ANT and assemblage thinking aim to describe the material reality as a complex configuration of heterogeneous pieces whose shaping constitute the state of the world as perceived at that moment:

Both assemblage thinking and ANT have much to say about the spatial dimensions of power and politics. That is because both approaches are concerned with why orders emerge in particular ways, how they hold together, somewhat precariously, how they reach across or mould space and how they fall apart. These aspects render assemblage thinking and ANT of particular interest not only to political geographers but indeed to anyone examining the exercise of power and politics. [26]

This approach to themes of surveillance aided by ANT and assemblage thinking is not new, being utilised in the last decade by researchers to analyse interactions between social movements, state vigilance, social media, corporate data and information policies, espionage, and many other topics (Wood and Wright, 2015; Abu-Laban, 2014; Hogue, 2016).

Let us return, then, to surveillance. How can STS studies, and ANT in particular, be used to understand it? According to Rosa Pedro, surveillance must be understood as a sociotechnical device:

The analysis we seek to undertake rejects any kind of determinism relating to technology, aligning itself with studies that see society — as well as subjectivity — as a hybrid collective woven from the complex interaction between humans and non-humans. Thus, it is necessary to comprehend the new technological surveillance devices, shining a light into their sociotechnical hybridization. [27]

By “sociotechnical hybridization”, Pedro is referring to how the social and the technical cannot be separated. She argues that surveillance can be understood as an extremely complex function, one that coordinates with (and is produced by) the interaction of several other devices. In this sense, contemplating surveillance will point toward the building of a network that produces “objects as well as subjects” [28].

The relevance of ANT in media research is widely recognized as a necessary framework for understanding the transformative power of technology beyond a passive tool, allowing researchers to better analyse how new devices restructure power dynamics in communication and surveillance:

An ANT approach has the potential to help scholars trying to grapple with the changing conditions of media in a time where humans and technology (and other entities) interact in new ways. Scholars might otherwise miss out on important insights into such changing conditions. Accounting for technology as an actor and not merely as a tool (for example, by approaching the algorithm as an enabler of journalistic practice), these two cases highlight the importance of rethinking how media and communication research draws boundaries between the assumed actors (producer/receiver, individual/society, and object/subject). (Dahlin, 2020)

Let's return to the previous framework: the surveillance network built in the context of the mega-events that took place in Rio de Janeiro. In order to describe the construction of this network, using the sociotechnical lens of STS, we must choose a starting point and follow its actors throughout their interactions. However, just like the rhizome, this network has multiple points of entry and several possible narratives. In the next section, we will explore one of these stories, encompassing mass protests against a bus fare hike in the prelude to the mega-events, as well as a revelation that Brazil's president was being monitored by foreign powers, accelerating the construction and empowerment of the Brazilian cybersecurity apparatus.

3. Brazil in June of 2013

The protests that spread throughout Brazil in June of 2013 took place in advance of the 2014 World Cup. From the moment that the country was selected to host the tournament through its announcement, the coming of the World Cup was thoroughly celebrated by Brazilians. They saw it as an expression of the country's love of soccer as well as a symbol of its social and economic progress.

However, the preparations for the event highlighted a stark contrast between a high level of quality for the infrastructure required for the games and the government's low standards when it came to essential public services, including healthcare, sewage systems, housing, and education. Still, these contradictions alone were not sufficient to explain the protests, as there are many actors involved in any given dispute as ANT demonstrates (Latour, 2005; Dahlin, 2020). The lack of funds allocated for societal needs has been a chronic problem in Brazil; the country's economic situation in 2013 was no more sluggish than usual. Moreover, the media and most Brazilian intellectuals did not acknowledge demonstrators as a legitimate part of the country's array of social movements, indicating that the right to protest was subject to validations by authorities and communicators (Lyon, 1994). For this reason, we sought out readings of the situation that expressed this lack of understanding, such as that put forward by Otaclio Neto [29]:

Should we look for the concepts of 'authorship' and 'leadership' among the protesters, we would probably not find anyone claiming these specific roles. If we take into account the role played by the Movimento Passe Livre ("Free Pass Movement") [30] in organising the first demonstrations of June 2013 in São Paulo, we would be hard pressed to deny that social movements were involved in the June Journeys. When it comes to a point where we are surprised by certain popular demonstrations that used to be common until a few decades ago, that is a sign that something important could be going on.

When recounting what happened in 2013, the activists that took part in the protests gave greater focus to

their experiences, seeking to validate an interpretation of the world that was better aligned with their interests. Communication work done by the Anonymous Rio collective [31] demonstrated the effects of the FIFA World Cup. These effects included the removal of the homeless from the streets of Rio de Janeiro [32], violations of housing rights [33], attacks on indigenous and traditional communities [34], repeated violence against reporters and activists [35], fraudulent overpricing of public infrastructure [36], sarcastic and dismissive statements by public figures and authorities [37], as well as FIFA's blatant disregard for Brazilian law [38].

The media's stance regarding protests aligned with that of authorities, starting with the dismissal of the demonstrations, remarking that they were promoted by minor groups (Haggerty and Ericson, 2000). Later, the media also criticised the protests for alleged criminal behaviour displayed by demonstrators, in reference to the destruction of public and private property as well as to a blocking of thoroughfares as a form of protest [39].

This media narrative helped to crystalize a category of "vandal" [40], which was used insistently during coverage of the protests, initially as a justification for the use of greater police repression [41] and later as a way to distinguish between legitimate and illegitimate protesters [42]. Social movements, however, do not take place in a historical vacuum: all aspects criticised by either the media or academia were simply responses developed in struggles carried out by different actors in various social contexts.

In 2013, Glenn Greenwald, then a journalist for the *Guardian*, published an article that described the contents of a series of documents leaked by Edward Snowden, a former employee of the National Security Agency (NSA), an American intelligence agency. According to the article, the United States government, together with security agencies from the United Kingdom, Canada, Australia, and New Zealand, headed a surveillance system that allowed those entities to store data on individuals, state organs, and private companies without authorization, indicating that citizen's data collection and storage has been generalised in the surveillance society (Lyon, 1994). The software used, Prism, gave the NSA access to different kinds of information, such as "search histories, e-mail contents, file, video and image transfers, voice and video calls, social media details, logins and any other data in the hands of Internet companies" [43].

Per Snowden's revelations, Prism may have tracked 2.3 billion phone calls and messages, on top of all the information hosted at various services provided by Internet companies, such as Google, Microsoft, Facebook, Apple, AOL, and Yahoo, vulnerable to NSA's monitoring [44]. Several governments in Europe and Latin America were monitored, including Brazil:

The whistleblower showed, through leaked documents, that the U.S. government, more specifically the NSA, was even monitoring President Dilma Rousseff's e-mail conversations. According to Snowden's leaks, Brazil was second only to the United States when it came to the volume of interceptions and monitoring. Some of the files are part of an internal presentation by the NSA, called 'Intelligence filtering your data: Brazil and Mexico case studies' and were divulged by Greenwald. [45]

This espionage had a deep impact in Brasilia. Preliminary investigations conducted by the Armed Forces and the Ministry of Defence detected no breach of the government's strategic information systems, as reported by journalist Thiago Herdy in the newspaper *O Globo* on 14 July 2013. In that interview, then Minister of Defence Celso Amorim admitted that, even though no security breach was detected, the country's cryptography systems were vulnerable as they were dependent on foreign technologies. He also stated that the Ministry of Defence and the Ministry of Science and Technology would seek "innovative national solutions", emphasising the need for Brazil to create its own cryptographic algorithms (Herdy, 2013).

The case sent shockwaves through Brazil's Congress, so much so that, on 10 August 2013, a Congressional Investigative Commission [46] (CPI) was set up. Its goal was to investigate “the reports on the existence of an espionage system structured by the United States government, the aim of which was to monitor e-mails, phone calls, and digital data, in addition to other ways of gathering information that has been classified as privileged or is protected by the Federal Constitution”. [47]

The Brazilian non-governmental organisation *Article 19* conducted a study on the country's surveillance policy, describing how the so-called “Espionage CPI” worked:

The CPI lasted seven months, and 13 senators took part in it. According to the Commission's findings, it was not possible to determine what information may have been breached, or whether any of the espionage described by Snowden actually took place, but the Commission stressed that all the evidence gathered pointed to that being the case. The most important finding — and the one that was used to legitimise the adoption of practical measures for the development of new policies in the sector — was the discovery that there were breaches in Brazil's digital security. [48]

The CPI's final recommendations included: developing national security technologies, making greater investments in intelligence and counter-intelligence, and training professionals to work in the cybersecurity field (Brasil, 2014). According to the NGO's study, the CPI resulted in the “creation of a broad Internet-surveillance state apparatus in Brazil” [49].

Brazil's counter-surveillance network was beginning to take shape, bringing together the office of the President, Armed Forces, the country's Parliament, as well as the Ministries of Defence and of Science and Technology. All these entities worked together to make Brazil capable of monitoring its cyberspace adequately so that it could defend itself from NSA and other cyber-spies. Their specific interests were translated into a common objective, meaning that Brazilian institutions produced an equivalence capable of enlisting its peers towards a shared interest (Law, 1992; Latour, 2005).

However, translation was also treason [50], and new actors arose to shake up this network and bring its members closer to their own agendas. One such politicised “reorientation” of surveillance emerged with the mega-events, which came with a growing concern that the 2013 demonstrations would repeat in 2014, during the FIFA World Cup. The mega-events in a sense created a new enemy against which the whole cyber-surveillance apparatus would be used. The network was no longer pointed to Washington and the NSA; it would now look inwards, at Rio de Janeiro, as the surveillance assemblage began spying and sorting Brazilians. *Brasil de Fato*, on 4 August 2016:

In truth, Brazil has, for some time now, been trying to follow the mass surveillance doctrine established by the United States [51]. This doctrine arrived here before; Snowden himself showed us this in 2013. It's just that we hadn't felt it. One of the major justifications for monitoring people's lives *en masse* is the coming of the big events — the World Cup, now the Olympics. Brazil has created a cybersecurity hub, organised by the Army, which has, for some time, been persecuting those who are considered ‘dangerous’, those who are considered, at any time, an enemy of the state. [...] The problem is that, by following the U.S. doctrine, you have a series of agents that are indistinctly monitored as though they were highly dangerous, as though they were terrorists. The list includes: environmental activists, defenders of traditional and indigenous communities,

social movements — both the traditional and new activists —, freedom fighters on the Internet, students protesting against education policy [...]. (Amadeu, 2016)

With this paradigm shift, new business opportunities arose in Brazil, especially in Rio de Janeiro during the preparation for the mega-events, more specifically pertaining to the sales for surveillance equipment, as shown by Natália Viana and Gabriele Roza in their study conducted for the NGO *Agência Pública*:

The spending was indeed extraordinary. The Ministry of Justice's Special Secretariat for Large Events (SESGE) alone spent close to [360 million U.S. dollars] [52] in five years (from 2011 to 2016), not to mention the spending done by the Armed Forces, as well as by state and municipal governments. Out of this total, more than half, [195.79 million U.S. dollars] was used for Command and Control Centres (CICCs), which are public safety units that gather various police forces in the same building, later given to each state's Public Safety Department. (Viana and Roza, 2017)

The network's door was open for a new wave of non-human agents, such as new security solutions developed by various companies, to enter. For example, there was *Aeromot*, a company from the state of Rio Grande do Sul, which provided:


Thirty-five aircraft with a system that can generate images, including infrared ones, sent to ground teams, to help with air monitoring needed for the World Cup. *Polsec*, a company from the state of Minas Gerais, equipped the SESGE with, among other products, vans that could be turned into covert police vehicles, camouflaged and outfitted with monitoring and radio transmission systems. (Viana and Roza, 2017)

Brazilian companies were not the only ones to take part in these opportunities: for example, the cameras in all 12 of the 2014 World Cup host-cities' CICCs were outfitted with espionage software from the German company *Helmut Mauell* (Viana and Roza, 2017). Apart from Mauell, e-mail messages leaked by the Web site WikiLeaks [53] revealed that Brazil's Federal Police had been in discussion with, HackingTeam (HT), an Italian company that specialises in selling espionage software to governments around the world:

Basically, HT's main product is a security breach suite developed from the undivulged vulnerabilities found in operational systems [54]. Through social engineering, which is to say, when the target clicks and runs the malware, it is possible to [contaminate the operational system being monitored], extract its data, intercept audio files and videos of conversations, activate its video camera, infect other computers, discover their location and even exit the system without leaving any trace in the victim's device. [...] Using the codename "Brenda", the Brazilian Federal Police contacted HT to implement a pilot project in the beginning of 2015. [55]

If we follow the actors in this surveillance network, which was set up to provide the security for the mega-events, we will notice a technical sophistication that contrasts with the more traditional methods used in the cases that we will outline in the following section. The June 2013 protests were carried out by individuals, by their actions in the streets. By bringing our analysis down to the level of ants [56], as suggested by ANT

(Latour, 2005), getting closer to those people and seeing everything from their perspective, we will then be able to better understand not just the national context but also the materiality of the events. We will follow the story of one of the 23 people imprisoned by the Brazilian state, Tiago, a member of the Facebook page Anonymous Rio, and his experience pertaining to the events that transpired between June 2013 and the end of 2014.



4. The experience of persecution

We will follow the story of Tiago, a founding member of the Anonymous Rio Facebook page (which is no longer active), learning about his life as an activist and how he handled the consequences that derived from contesting official discourse. After joining the Anonymous Rio Web page in 2011, Tiago noticed the lack of good sources of information available to the demonstrators and felt the need to transmit the events taking place at the time, taking a more active role in the site. Tiago's workload grew with the popularity of Anonymous Rio, as it started divulging more news and following more events. The effort to produce content is often an individual endeavour. This activity was performed alongside other demands from the participants' day-to-day lives, and sometimes it had to take a backseat whenever life became too busy, as explained in Tiago's interview [57]:

At the time, all the members were granted administrator status in the group due to an ideological reason, that of horizontality. Our intention was always to divulge information and news. We always aimed to communicate what was happening in the city. [...] I imagined this would maybe happen in the long term, but *what we did was like little ants' work*. [...] But it happened so fast, in such short notice, that we didn't expect it. Even the jump from 30 thousand to 130 thousand [followers] happened in a week, it was out of control [58]. (Tiago, 2015)

The perception of the challenge that came with the work, both in its scope ("little ants' work") and in its potential (the page's reach), are recurring themes in conversations with Tiago. When asked about how the Web page contributed to the protests, Tiago acknowledged that Anonymous Rio was not the sole responsible party, and that other collectives engaged in similar projects had their hand in it as well as:

A policeman put me in a headlock, so I started shouting "I'm being arrested, I didn't commit any crime!". Someone was nearby and filmed what happened. The policeman saw it and decided to let me go, but then he went after a different person, someone who was not being filmed by anyone. Back in the day, you had protests, you had repression, people got beat up and nothing came of it, nobody heard about it. [...] Now, there's a bunch of independent versions on what happened. (Tiago, 2015)

News coverage on the streets came with contradictions relative to footage taken during the protests. Videos served as a form of protection when used to report cases of police brutality but, at the same time, they could become a source of further persecution, as the videos of protests provide evidence as act as a form of surveillance data (Lyon, 1994). Despite this risk, the use of personal social media profiles was common for a long time, both by the Web page's administration as well as comments posted in group discussions. In a certain way, it seemed to be part of the confrontation game being played, a conscious risk taken by those who had never experienced persecution and surveillance:

I didn't expect physical surveillance, but digital surveillance. As soon as we started making trouble, all they'd have to do was ask Google or Facebook for our data and they would know everything about us. [...] We talked many times about the issue of using our own personal profiles, as that was a bit easier, more practical. Often we would be on the street while something was happening, such as the police abuse against some street vendor or some protest going on that needed coverage [59], it was easier to post directly from our phones. If that ended up getting us in trouble, no problem, everything comes with a risk. (Tiago, 2015)

The participants took risks by not protecting their anonymity, but they were more concerned that the content that they had been releasing would be deemed illegal, and so they sought to avoid outwardly defending the use of violence in their Internet content. Their actions generated a guide with safety instructions for protesters. Even though it only contained tips and precautions, the guide would be used eventually by the police as part of a legal case brought against the group:

We're always careful so that nothing we wrote could be legally actionable. We ended up filtering out some photos that the police could use in some way, nothing illegal, but they took issue even with our peaceful resistance guide [60], which was twisted into a "terrorist guide" and got picked up by *Veja* magazine. In the beginning it was just us, but in 2012 they started repressing the bus fare hike protests in front of City Hall. More people, close to 100 or 150 participated, and then we started closing down the streets, making some noise and bothering them. Even back then, people were already being beaten up, getting tased, pepper sprayed, tear-gassed, even though the people protesting were very much a 'peace and love' kind of crowd. (Tiago, 2015)

The criminalization and repression of the protests was not directly related to the occurrence of violence or any kind of radicalization amongst the participants. In 2013, the police questioned two Anonymous Rio members at the Computer Crimes Unit (DRCI), as part of an investigation called Operation Firewall [61], and the suspects had their phones and banking transactions tracked.

This police investigation constitutes another actor, created through various successive translations. In it, the collective's conflicts were reinvented amidst intrigue, captured by virtual patrols and translated into possible connections between the actors, until it culminated in the supposed existence of a criminal organisation.

The administrators of the aforementioned Facebook page are "hackers" [62], and they invade government Web sites in order to expose confidential information, such as when they divulged the names and addresses of Military Police officers after hacking into the Rio de Janeiro State Military Polices Web site. The "Anonymous Rio" Web page itself was hacked and its administrators were accused of causing chaos in the city of Rio de Janeiro and throughout Brazil. They were also accused of having connections with foreigners, through which they coordinated terrorist activities in the country, and their data was divulged on the Internet. [63]

The legal case against Tiago was based on the fallout of a romantic infidelity scandal [64] that took place within Anonymous Rio. After discovering the affair, one of the group members took over the page and removed the others, whom she considered to have betrayed her along with her boyfriend. The information leaked during this episode was used as evidence in the police investigation:

We were only able to collect these conversations, which were captured via screenshots, because of a split within the Anonymous Rio community, as it was hacked by one of its own participants, who leaked information pertaining to the page's administrators, their political affiliations and personal goals. This 'internal dispute' made it possible for the conversations posted on the page's timeline to be exposed for any and all users visiting it to see them at any moment. [65]

Tiago did not think that this leak alone provided sufficient information to substantiate the investigation's claims, choosing to believe there was another source involved, one that had not been mentioned during the case. According to him, what led the police to secure this information was a decree from the state government, passed in the same year, created with the intent of persecuting digital activists:

The only evidence the investigation had of our participation in the Web page was the one [that resulted from the romantic infidelity affair], but I think that's the only thing they could legally use. [...] in 2013, there was a decree dealing with access to government information that got revoked. The decree established a new type of priority for access to information requests, meaning that, if there was any court order requesting information, it wouldn't have to wait, it would go straight to the communications companies. (Tiago, 2015)

Decree number 44,302 (Rio de Janeiro, 2013b), enacted by the Rio de Janeiro state government on 19 July 2013, established the creation of a Special Investigative Commission on Acts of Vandalism in Public Demonstrations (CEIV). Under the pretext of countering damage caused by protests, the government proposed a complete violation of the right to privacy:

[...] to prevent the occurrence of further acts of vandalism and punish the criminal practices that have already been perpetrated [...] the CEIV will take all the necessary measures to investigate said acts of vandalism, having the ability to request information, conduct due diligences and do whatever is needed to conduct criminal proceedings [...] the telephone companies and Internet providers will have a maximum of 24 hours to comply with the CEIV's information requests. (Rio de Janeiro, 2013b)

The decree was very open about giving full persecutory powers to its participants (Rio de Janeiro's state Public Prosecutor's Office [66], the state's Public Safety Department [67], as well as the state's Civilian [68] and Military [69] police forces), obligating phone companies and Internet providers to comply with the CEIV's information requests within 24 hours.

On 24 July 2013, the decree was modified so as to make its contents more palatable, as it had been criticised by civil rights organisations. These changes reflected the state's capabilities to access personal information, illustrating the power and political dimensions of the surveillance assemblage (Müller, 2015). The CEIV would now first have to obtain a court order to request private information pertaining to phone

calls and online interactions. The new version of the decree also removed the 24-hour deadline for the release of requested information, replacing it with a mere priority status (Rio de Janeiro, 2013c).

Tiago's suspicions about the investigation were reinforced by information obtained by the police via phone tapping, the contents of which were completely irrelevant. In the phone records, there were several conversations between the suspects, among which there could be found declarations of love, trivial day-to-day affairs, and references to politics and protests:

[...] they call each other 'my love' and agree to meet at the bus station at eight o'clock. She thinks that is too early, because she wants to get her nails done. He says he has grown a beard but that he will probably shave it. He says he is going to prepare the flash drives to do something on the rude *badernista's* [70] computer. They talk about Linux and Mandriva. She says she tagged him in her status. He says he was on Facebook chat. He lets her know he is going to do that thing on Facebook. Says he asked for a meme and will spread it every day they are in Rio. [71]

The information collected via screenshots from the Web site during virtual patrols illustrated stark inconsistencies between what was presented as evidence and legal arguments used during the investigation. The activists were accused of being financed by political parties, with the police noting that it was the only way that the suspects could afford computers, tablets, and cellphones, due to their supposed lack of employment. However, in other parts of the investigation, the police recognized one suspect as being a lawyer and another as a bartender. This argument reinforced that, in the police's view, even access to non-human actors was considered fundamental in the framing of the actions of protesters as crimes (Law, 1992). The police considered all suspects to be members of a dangerous group but presented no proof that conclusively demonstrated that the persons accused had orchestrated or carried out actual acts of vandalism:

[...] the suspects are extremely violent people, and recently a TV network employee was murdered by a firework rocket while filming the protest [72]. The members of the "BLACK BLOCS" and "ANONYMUS" [sic], who truly are criminal minds, hide behind masks and use tools from the virtual world to practise crimes. [...] the gang, which is under investigation, has been committing acts of vandalism during the demonstrations taking place in the state of Rio de Janeiro, and they have been trying to recruit more members via social media and other channels. [73]

Actual evidence was not presented to incriminate the suspects, only presumptions based on conversations and media reports. The police's accusatory stance was not limited to the suspects, but applied generally during the protests, according to Pires:

During the wave of protests that began in June of 2013, multiple illegal arrests were made and many demonstrators were imprisoned without the police presenting a specific reason or paying attention to who actually committed a crime. They simply were taken to police stations, brutalised, and charged with falsified allegations, usually of contempt, disobedience, and conspiracy to commit crimes. Charging demonstrators with these 'felonies' was so easy that they started using them as 'generic felonies', so as to give a technical facade to their

arbitrary use of authority, with little in the way of rationality to go with all the power they held. [74]

It was through this kind of indirect accusation, based on phone records and the alleged existence of a ‘gang’, that the investigation issued a search and seizure order, leading to interrogations of suspects:

On 10 July, two days before the start of the World Cup, some activists in Brasilia had their homes surveilled by men claiming to be agents of the Regional Electoral Court (TRE), who questioned them about their daily routines. After this visit, the activists went to the TRE and found that the identification badges those men had presented to them were fake, revealing another underhanded action by the police. The following day, on the eve of the World Cup, an operation by Rio de Janeiro’s DRCI detained four activists, Elisa Quadros, Tiago Rocha, Game Over [75], and Anne Josephine, and seized documents from their homes. [76]

As described by Tiago, the experience of the police raid into his home revealed that the agents responsible for the operation were expecting something different and did not know how to explain the specific charges:

On 11 June, the day before the start of the World Cup, they came with a warrant to search and seize electronic devices, digital media and bombs. I asked to read the warrant and it said “Breach of software copyright law”. [...] They searched everything in my home [...] I had to go to the police station at the time, I didn’t know if I was under arrest, it was my first experience with this kind of thing. (Tiago, 2015)

The charges found on the warrant read “breach of software copyright law” [77]. This accusation is reserved not for those who pirate computer programs but to those who are experienced in software development and coding as well as those who create channels for piracy and bypass registries, permitting the use of illegal copies of software, also known as “cracks”. Tiago pointed out that this was a strange accusation, as he noted that “all the computers I own run on Linux”. [78]

The police chose to use this specific type of allegation so that they could seize the suspects’ electronic devices, which could help to build their case. Later on, after the group’s arrest, the investigators justified this choice, stating that it was a typing error and alleging that the correct charges were those of conspiracy to commit crimes (which, by then, could be backed up with the statements taken from the group). Tiago questioned the nature of this mistake: “I said none of that was on the warrant I was shown, the police chief replied saying it was a typing error. According to him, because their police unit specialised in computer crimes, there were no other types of felonies programmed into their system”. The police recorded this “typing error” in their investigation log as “an error resulting from the fact that, in the warrant, under the item ‘CLASS’, there was the name of that law written” [79]. Tiago talked about how his arrest was carried out, his feeling of being silenced due to the charges he was facing, and the overall incompetence displayed by the authorities responsible for the investigation:

The chief of police started asking a lot of questions about me and the others who got arrested, he was clearly trying to paint us as a gang, each of us supposedly having a different role in it. [...] They asked if I knew my own name, I joked that I knew it very well. If the police unit investigating you doesn’t even know who you are, then it’s not really an investigation, it’s

clearly just a way of silencing you. [...] they threatened to arrest me just because I had kept the casing of a rubber bullet shot at me during a protest; they wanted to use that fact to press weapon charges against me. (Tiago, 2015)

Tiago described the shock that came after the investigation as having a strong impact on his psychological well-being and on his personal relationships. Even though he was listed as a witness during the prosecution, having his home searched and being arrested had a significant effect on him:

It was a very grim moment, emotionally speaking: getting home, seeing everything [scattered across the floor], I cried at the time. [...] I couldn't clean up the mess; I looked at it, took a shower and went to sleep. No place felt safe or at ease any more. The bell would ring and I would get scared. When the sun rose, I kept waiting for them to burst into my home like they did before. I defined the feeling as having your life suspended, like someone else having control of your day-to-day affairs. You can't make any plans, because some strangers are going to come in and take you away. (Tiago, 2015)

Much of the evidence presented by the state was also based on statements taken by the police from the activists, who were officially listed as witnesses. They, too, were taken from their homes under search and seizure warrants, and were intimidated during their detention by the police. As was the case with Tiago, the police seized some articles from other suspects' homes, with the clear intent of fabricating connections between them and any possible felony or criminal liability. Among the objects seized, there were several electronic devices and hard drives, as written in the investigative record:

Among the articles taken from the places searched were several documents, flash drives, laptops, protection goggles, filled-out notebooks, memory cards, tablets, external hard drives, masks associated with the Anonymous group (Guy Fawkes masks), cartridges, pieces of explosives [80], rubber bullets, black gloves and caps, softball bats, megaphones, protection masks, black vests, pamphlets that read "There will be no World Cup", white shirts with the saying "No more corruption", petitions to include corruption in the list of heinous crimes and against Constitutional Amendment Proposal number 37 ("PEC 37"), a flag with the words "Down with Cabral" [81] (*Fora Cabral*), several stickers for "Enough is Enough Day" [82], ("*Dia do Basta*", in Portuguese), a *Carta Capital* magazine with a story on Black Blocs and street vandalism, documents on the "*Ocupa Câmara*" [83] ("Occupy City Council") movement, tags with the saying "FIFA, Go Home" [84] and other gear that will be sent to the proper forensics teams for further examination. [85]

About a month after searching the suspects' homes, the police returned with a warrant for the preventive detention of the suspects, even though they were not considered dangerous and there was no evidence to back up allegations. The choice of date and scope for this operation made it clear that it was the police's intention to silence activists and hinder their participation in demonstrations: "[...] the day before the World Cup Final, 12 July, was marked by an enormous police operation, called 'Firewall', during which more than 100 law enforcers arrested several activists" [86]. Tiago explained how, even though the police went through all this trouble to ensure the arrests of activists, they still afforded their political prisoners a somewhat special treatment:

The Polinter [87] cell was a two-by-two meter cubicle, very cold due to air conditioning, there was no water, only a pipe set up on high that poured water into the [hole in the ground used as a toilet]. Everything got wet, there was no toilet paper or any sheets, there was no bed, we had to lie on the floor. Our lawyers brought us water, fruit, and take-out meals. We were transferred to Bangu [88] in a police van with iron seats and almost no room, handcuffed to a bar. [...] When we got to Bangu [...] we formed a line and had to take off our clothes. We were treated differently: the prisoners there got beaten up for any small reason [...] we, however, went directly to our cell in a separate corridor. (Tiago, 2015)

The persecution of the activists was a way to intimidate them, even though they were treated differently from other prisoners. The cost of participating in the protests became clear by how the actual persecution was conducted: with no due process, no right to legal defence and no evidence presented, it was possible to arrest them based solely on suspicions and conflicts of interest between activists and authorities. As Tiago put it, this resulted in the lack of:

[...] that sense of freedom. I didn't get that and still don't, I don't feel free. [...] I feel like, whenever the Web page starts making waves again, something bad is going to happen, even if I'm not involved in it. I'm already being tracked, there is a criminal record with my name on it. This new stuff, with HackingTeam and the DRCI negotiating deals, there are intelligence and surveillance companies doing this, they are just trying to make it all legal, so they can do it without a court order. (Tiago, 2015)

Operation Firewall created a precedent for the persecution of several popular movements and independent media collectives. When used to repress political activism, the police and legal system can discourage political action and take a heavy emotional and psychological toll on those being persecuted, even if they are not formally convicted. The episode described in this paper demonstrates that, even before the police raided suspects' homes, an elaborate surveillance apparatus was already in use, monitoring activists' social media, phone calls, and text messages, tracking their most mundane activities in the hopes of finding any evidence of their criminal liability. The state surveillance assemblage operates by enveloping itself, constructing a spiral of vigilance that feeds off its previous actions and justifies its future investigations (Ullrich and Knopp, 2018). The mere act of monitoring and watching a suspect for a sufficiently long period seems to eventually produce the desired villain, encouraging the watchers to see illogical connections and ill intent in everyday affairs:

It becomes a vicious circle, because the longer that you look at a kid, the bigger the file gets, even if they've done nothing. And then six months later, somebody calls the [Federal Bureau of Investigation] F.B.I. and says, 'I've seen some suspicious activity in this neighbourhood,' and an agent can see that we have thick files on all of these kids. [...] but the files have shown that these kids are guilty of nothing. (Albury, 2021)

The Brazilian scenario may have its peculiarities and differences when compared to the United States' large intelligence and police apparatus, but the way surveillance works does not change that much between the two countries. As shown by investigation records presented here, mundane objects like flash drives, black clothing, and masks were converted into evidence of a crime. The protests' capacity for social and political

mobilisation became a sufficient nuisance so that it justified the use of this state apparatus. The government's frightened and disproportionate reaction in turn made people aware of the power that they have. The same principle of surveillance assemblage as a potentiality and not a fixed entity can be applied to the protesters' mobilisation capabilities (Haggerty and Ericson, 2000). This led to the discovery of how strong rhizomatic organisations can be when facing a state bureaucracy, and it became possible to detect the frailty of the state's discourse, which could no longer be sustained in light of the numerous video recordings and text created by activists [89]. Lawsuits that began in 2014 are still on-going in Brazil's justice system, creating major concern and costs for those being prosecuted.

Through its efforts to control political activism in social media, the government has shown it does not understand the particularities and potential of the Internet, seeking to classify activists as members of criminal organisations. Thus, law enforcement agents often look for hierarchical structures, distribution of roles and responsibilities, ill intent, and extensive planning. When monitoring smaller groups, authorities believe that they're capable of conducting activities deemed unusual for their size:

[...] microstructures are on some level organised or coordinated systems, the coordinating elements involved are not of the kind we associate with formal authority, complex hierarchies, rationalised procedure or deep institutional structures. In fact, the mechanisms involved may be akin to the ones we find in face-to-face situations, but at the same time they hold together arrangements at a distance and distributed systems. [90]

In any STS analysis, the Internet and its social networks need to be understood as actors, seeing as they have decisive effects on the actions of those involved, thus allowing for personal interactions and their qualities to manifest at a distance. Relationships of trust have proven to be enough to provoke action, leading people to, for example, take part in a demonstration or express a given opinion in order to support a friend, relative, or partner. Therefore, it would be possible to coordinate popular movements via informal organisations, using their members' interpersonal relationships and ideological affinities promoted in the social networks.


5. Final thoughts

The building of the legal case against 23 activists and the empowerment of the Brazilian state's repression apparatus developed simultaneously. With that in mind, we pose the following question: what have we learned from the June 2013 demonstrations, seeing as, even though the bus fare hike was eventually cancelled, we still live in a scenario where the surveillance apparatus and persecution of social movements have grown stronger? We can understand that "even though deep institutional changes are the goal of these social struggles, if we take a historical view we shall see that these changes do not occur as often and as quickly as the activists would like." [91] Having shed an initial fascination with these social movements, we can better contemplate the difficulties that activists face in their struggle.

The seemingly harmless habit of recording day-to-day life and personal connections on social media, when combined with traceable electronic records, can be used to build convincing narratives, making it easier to fabricate allegations and factoids that can incriminate individuals (Fuchs and Trottier, 2017).

However, the multitude of electronic channels used to monitor lives must not be seen as just an expansion of the state's watchful gaze. Information gathering has become ubiquitous, transforming into an embedded ambient feature, an all encompassing "Panspectral" (de Landa, 1991) of ever present vigilance capacity. We must acknowledge that the act of surveillance itself changes with the use of these new devices. ANT can help us in this matter:

Rather than an intensification of Foucault’s ‘Panopticon’, Bruno Latour (2005) instead proposes the concept of the ‘Oligopticon’ to account for the exercise of control and observation within society; and he contends that surveillance exists as an activity that cannot be ‘decoupled’ from the multiple sites and materials it is enacted through. Socio-technical ‘Oligoptica’ are further advanced as having limited optical scope, yet are distributed so they may observe small portions with great precision. [92]

These devices shift the boundaries between what we consider private and personal spaces. The new possibilities brought about by their use transforms our understanding of what should and should not be surveilled. Experiences of political persecution, such as described by Tiago, allow us a glimpse into the threats posed to our rights and freedoms. Activists and common citizens that decide to raise their voices against corporate and government authoritarianism, be it on the streets or on the networks, should take into account the profusion of new devices and actors that make up the surveillance assemblage, making their personal lives inseparable from their political actions in the eyes of the state. The popularisation of ICTs takes parts of life that previously seemed to be outside the gaze of police organs and brings them into the reach of surveillance networks, expanding the list of what may be necessary to control bodies and minds. 

About the authors

Pedro Braga is a D.Sc. candidate in systems engineering and computer science at Universidade Federal do Rio de Janeiro (UFRJ).
E-mail: pedrohcb [at] cos [dot] ufrj [dot] br

André Sobral is a D.Sc. candidate in systems engineering and computer science at Universidade Federal do Rio de Janeiro (UFRJ).
E-mail: lealsobral [at] cos [dot] ufrj [dot] br

Fernando Severo is a D.Sc. candidate in systems engineering and computer science at Universidade Federal do Rio de Janeiro (UFRJ).
E-mail: severo [at] cos [dot] ufrj [dot] br

Ricardo Jullian is a D.Sc. candidate in systems engineering and computer science at Universidade Federal do Rio de Janeiro (UFRJ).
E-mail: jullian [at] poli [dot] ufrj [dot] br

Henrique Cukierman is a professor at Universidade Federal do Rio de Janeiro (UFRJ).
E-mail: hcukier [at] cos [dot] ufrj[dot] br

Notes

- 1. Marx, 2009, p. 47.
- 2. Marx, 2009, p. 47; Arora, 2019.
- 3. Lyon, 1994, p. 3.
- 4. Lyon, 1994, p. 4.

5. Activists can adopt some measures against vigilance or at least make it more difficult and costly. For example, tools and software, such as cryptography and VPN, are intended to prevent interception of information transmitted through the Internet. Unfortunately, as discussed in this article, the surveillance assemblage is multilayered and draws upon sources of information that are not commonly available (such as security cameras and banking data).
6. Lyon opens this chapter with the following Russian proverb: “An individual in Russia was composed of three parts; a body, a soul and a passport”.
7. Lyon, 1994, p. 3.
8. Lyon, 1994, p. 25.
9. Pridmore, 2012, p. 321.
10. Launched on 1 October 2003, 4chan is a forum in which users can post images and texts anonymously, with the more recent posts appearing above older ones. It is divided into several subforums, each having its own specific content and community rules. Except for forum administrators, users do not need to register in order to post on the site. The first subforums on 4chan revolved around anime, manga, and Japanese pop culture, but the platform quickly expanded to include many other subjects, such as video games, music, politics, movies, television series, and sports.
11. Estevão, 2014, p. 162.
12. Weller, 2012, p. 57.
13. Foucault, 1978. The Chinese social credit system is an example of how technologies can be used to exert control at different levels (individual and collective). This article narrates a different level of government organisation and technological competence to illustrate how even inept actors can wield them to repress citizens.
14. Still regarding this type of surveillance, we recommend reading Paulo Feitosa’s (2010) Master’s thesis, called “O Cidadão Codificado: A Digitalização da Cidadania em Bancos de Dados de Interesse Público” (“The Coded Citizen: the Digitalization of Citizenship in Databanks of Public Interest”), at: http://objdig.ufrj.br/60/teses/coppe_m/PauloHenriqueFidelisFeitosa.pdf, accessed 16 July 2022. Weller, 2012, p. 59.
15. Deleuze and Guattari, 1987, pp. 10–36. In botany, the word “rhizome” describes plants whose shoots can branch out at any point, enabling them to function as root, branch, or thallus, no matter where they are physically located within the plant’s body. Thus, Deleuze and Guattari’s metaphor outlines a mode of knowledge in which no proposition or assertion is more elementary than the other. In other words, there is no root, nor is there a path that can be traced from it. On the contrary, there are multiple points of entry and multiple final destinations.
16. Haggerty and Ericson, 2000, p. 609.
17. By “mega-events”, we refer to the 2014 World Cup, 2013 World Youth Day, and 2016 Olympic Games. All these massive events were held in Rio de Janeiro, acting as catalysts for deep changes in the city’s urban and political landscape.
18. Lyon, 1994, p. 11.
19. Cukierman, *et al.*, 2007, p. 203.
20. *Ibid.*

21. Law, 1992, p. 381.

22. *Ibid.*

23. Law, 1992, p. 381.

24. Latour, 2012, p. 178.

25. *Ibid.*

26. Müller, 2015, p. 27.

27. Pedro, 2005, p. 3.

28. Pedro, 2005, p. 41.

29. Neto, 2013, p. 22.

30. “The MPL (‘Free Pass Movement’) is a left-wing movement that has always engaged with its counterparts, such as the Landless Workers Movement (‘Movimento dos Sem Terra’, in Portuguese) and urban movements for better housing. It has found support among intellectuals and in certain parts of the progressive blogosphere, with its main point of reference being the Web site tarifazero.org. Though, in some ways, the MPL represents a break with some institutional aspects of formal democracy, in other ways it carries on the left’s tradition of social struggle, seeking to transform society”. (Judensnaider, *et al.*, 2013, p. 19).

31. Anonymous Rio is an activist collective which operates mostly on social media, mainly Facebook. Anonymous Rio’s page can be found at <https://www.facebook.com/anonymousrio?fref=ts>, accessed 16 July 2022.

32. There was another instance of this kind of social cleansing, the goal of which was to create a more tourist-friendly appearance: http://www.olhardireto.com.br/copa/noticias/exibir.asp?noticia=Sociologo_critica_limpeza_social_durante_Copa_e_cobra_criacao_de_poiiticas_publicas&edt=7&id=6619, accessed 16 July 2022.

33. The public works needed to host the World Cup resulted in the eviction and removal of thousands of families: <http://www.cartacapital.com.br/sociedade/pesquisadora-faz-mapa-da-expulsao-de-moradores-por-obras-da-copa-em-curitiba>, accessed 16 July 2022.

34. The development of public works needed to host the World Cup threatened the Indigenous Peoples Museum in Rio de Janeiro, which came close to being turned into a parking lot: <http://www.ebc.com.br/noticias/brasil/2013/12/concluida-desocupacao-do-antigo-museu-do-indio>, accessed 16 July 2022.

35. Reporters were injured while covering protests, with police violence against media professionals appearing intentional: <http://terradedireitos.org.br/en/news/terra-de-direitos-in-the-media/brazil-police-in-spotlight-as-world-cup-looms/14843>, accessed 16 July 2022.

36. Cases of embezzlement in public works associated with the World Cup: <http://esportes.terra.com.br/futebol/copa-2014/jornal-mais-carro-da-copa-estadio-do-df-tem-desvios-de-r-212-mi,bc00d316aab7c310VgnVCM5000009ccceb0aRCRD.html>, accessed 16 July 2022.

37. Ronaldo, a famous former soccer player, noted that “you can’t host a World Cup by building hospitals”: <http://www1.folha.uol.com.br/esporte/folhanacopa/2013/06/1297590-ronaldo-usa-web-e-se-defende-da-afirmacao-de-que-nao-se-faz-copa-com-hospital.shtml>, accessed 16 July 2022.

38. FIFA's impositions were unconstitutional and massively skewed in favour of corporations: <https://www.viomundo.com.br/denuncias/exigencias-da-fifa-para-a-copa-violam-direitos-dos-brasileiros.html>, accessed 16 July 2022.

39. Judensnaider, *et al.*, 2013, p. 33.

40. A vandal was a term used to designate a member of a specific Germanic tribe from antiquity. The term was appropriated by the Romans, who gave it a meaning similar to "barbarian", someone who was not Roman or not civilised. It is an ethnocentric appropriation of the Other, used as a way to dismiss those who do not accept the rules of a political game.

41. "The depiction of the protests as acts of violence, rage and lack of self-control is disseminated in order to call for more repression. The rest of the news coverage reinforces the editorial's message, emphasising the 'marks of vandalism' of the previous protest, the criminal liability of those involved and the arrests made, in addition to spotlighting the police officers injured during the last demonstration". (Judensnaider, *et al.*, 2013, p. 85)

42. Resende, 2015, p. 122.

43. Article 19, 2016, p. 6.

44. *Ibid.*

45. Article 19, 2016, p. 6.

46. "The goal of the CPIs [...] is to conduct investigations of interest to public life and to the constitutional, legal, economic or social order of the Country. They have investigative powers equivalent to those held by judicial authorities, including the power to appoint due diligences, conduct hearings for indicted individuals, examine witnesses, request documents and information from public organs and entities, request audiences with State Representatives and Ministers, receive statements and testimonies from federal, state and municipal authorities, and to request the services of any authority, including the police". From the Brazilian Congress Web site, at <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito>, accessed 16 July 2022.

47. Brasil, 2014, p. 5.

48. Article 19, 2016, p. 7.

49. *Ibid.*

50. This is a reference to an old Italian saying, a word play on the similarity between *traduttore* ("translator") and *traditore* ("traitor"). It means that no translation can really capture the exact meaning of the original so, in a sense, every translator ends up "betraying" the original a little.

51. This is a reference to the post 11 September establishment of a robust surveillance apparatus in the United States (Guzik, 2009).

52. Conversion of 1.17 billion Brazilian real, using exchange rate as of 31 December 2016.

53. These e-mail messages were released on 8 July 2015; see <https://wikileaks.org/hackingteam/emails/>, accessed 16 July 2022.

54. According to its "Technicians' Guide. Hacking Team Remote Control System (RCS)", the company's main product has payloads for infecting Android, BlackBerry, iOS, Symbian, and Windows Mobile smartphones, as well as Windows and Mac OS personal computers. See

<https://theintercept.com/document/2014/10/30/hacking-team-rcs-9-technicians-guide/>, accessed 24 July 2022.

55. Article 19, 2016, p. 38.

56. Latour explains the origin of the ants' metaphor: "Alas, the historical name is 'actor-network-theory', a name that is so awkward, so confusing, so meaningless that it deserves to be kept. [...] until someone pointed out to me that the acronym A.N.T. was perfectly fit for a blind, myopic, workaholic, trail-sniffing, and collective traveller. An ant writing for other ants, this fits my project very well!" (Latour, 2005, p. 9).

57. Tiago was interviewed by the authors of this paper as part of the research completed for two different Master's theses, at <https://www.cos.ufrj.br/index.php/pt-BR/publicacoes-pesquisa/details/15/2692> and https://www.researchgate.net/publication/325694844_Uma_proposta_de_extensao_inspirada_na_Pesquisa-Acao_para_atuar_no_combate_a_Vigilancia_Digital_do_Rio_de_Janeiro, accessed 16 July 2022.

58. The sudden growth in the number of followers of the Facebook page Anonymous Rio, which increased fourfold, is a matter that requires further discussion. The Web site's own dashboard presented this surge as organic. In other words, this would mean that the page's members did not pay to expand its reach and that this increase in followers could be ascribed to how the protests became more popular and intense. A different, though less likely, explanation for this phenomenon is that the page's reach grew due to indirect funding or due to a change in Facebook's own policies and algorithms, aiming to serve the interests of a third party. For instance, through political manipulation it is possible to pay fees so that one type of content will show up more frequently to certain users, even if the content creators are not the ones directly funding this publicity.

59. Examples of videos and images by protesters showing police violence are available at <https://www.youtube.com/watch?v=iDo3C4wTd4k> and on other sites, <https://rioonwatch.org/?p=16651>, accessed 24 July 2022.

60. The "Guide for peaceful resistance" was less than five pages long and provided a set of simple instructions on how to dress, how to deal with tear-gas bombs, and how to behave when being approached by the police. The newspaper described it harshly: <http://oglobo.globo.com/rio/anonymous-divulga-manual-de-enfrentamento-em-protestos-10318885>. The newspaper *O Globo* quoted police colonel Milton Corrêa da Costa: "The way I see it, the page's contents shows we're dealing with a criminal organization that uses the Internet to teach and disseminate tactics and techniques for aggressive disobedience, which result in vandalism against the police while it is trying to restore public order. It is a dangerous circulation of practices used in guerilla and urban terrorism and for assaulting lawful authorities. It is an online crime, the perpetrators of which must be identified and punished by the law." It is possible to draw one's own conclusions by accessing the "Guide's" contents at https://pt.scribd.com/document/104388906/Manual-de-Acao-Direta-Acervo-Civone-Medeiros-de-Desobediencia-Civil-Insurgencias-e-Subversao?fbclid=IwAR0tfZERkey371aVYSiX4E0WgeYabwPn8Xz1VKk3yF7QVBmeyHNEZgFJ_A0, accessed 16 July 2022.

61. "Operation Firewall" refers to an element within computer networks, either software or hardware, providing security to a specific network.

62. By "hackers", we refer to individuals who seek to obtain unsanctioned access to computer networks or systems.

63. Rio de Janeiro, 2013a, attachment 1, p. 9.

64. The characterization of political activism as a planned and rational course of action could be challenged by the occurrence of romantic relationships between the participants. Emotional bonds kept the group together, but they also fueled personal conflicts, as was the case of the information exposed publicly on the Anonymous Rio page, which the police investigation reported as evidence "leaked by hackers".

65. Rio de Janeiro, 2013a, attachment 1, p. 107.

66. A permanent institution of the Brazilian state, in charge of prosecuting criminal cases in the public sphere. In the context of the CEIV, the Public Prosecutor's Office branch in question was that of the state of Rio de Janeiro.

67. An organ of the state of Rio de Janeiro's executive branch, responsible for managing the state's public safety issues and for regulating civilian and military police forces.

68. In Brazil, the Civilian Police fall within the purview of the states, playing the role of judiciary police in each of Brazil's federative constituents.

69. The Military Police consist of state gendarmeries responsible for the ostensible policing of the civilian population, playing a role that, in other countries, would normally be fulfilled by civilian police forces.

70. By "rude *badernista*", Tiago is referring to a member of the media activism collective "*O Badernista*" ("The Hooligan"). In its Facebook page, the collective sarcastically describes itself as "[...] the newspaper of the masked vandals funded by the PT (*Partido dos Trabalhadores*", Brazil's Workers Party) to put an end to peaceful and orderly demonstrations". Source: <https://www.facebook.com/badernistajornal/about>, accessed 16 July 2022.

71. Rio de Janeiro, 2013a, attachment 3, p. 35.

72. The police's repression of protests led to an escalation of violence, including stone throwing, fireworks, and other improvised weapons. See <https://www.wsj.com/articles/SB10001424052702304558804579374733557963374>, accessed 16 July 2022.

73. Rio de Janeiro, 2013a, attachment 2, p. 124.

74. Pires, 2015, p. 69.

75. An alias used by an activist online and adopted by the press.

76. Reys, 2014, p. 47.

77. The full content of the law pertaining to this allegation can be found at http://www.planalto.gov.br/ccivil_03/leis/L9609.htm, accessed 16 July 2022..

78. By "Linux", Tiago is referring to the open-source operating system GNU/Linux, freely distributed over the Internet. There were no crimes against intellectual property as suggested by the police.

79. Rio de Janeiro, 2013a, attachment 3, p. 230.

80. Unwary readers may interpret the term "pieces of explosives" as being a reference to bombs in the process of being assembled. However, photos taken of the seized gear indicate that the phrase was referring to the scraps of tear gas cylinders that the suspects collected as trophies, as well as the rubber bullets mentioned earlier.

81. This was a popular slogan used against former Rio de Janeiro State governor (2007–2014) Sérgio Cabral, arrested on corruption charges in 2016; see, for example, <https://www.nytimes.com/2016/11/18/world/americas/sergio-cabral-rio-governor-corruption.html>, accessed 16 July 2022.

82. "Dia do Basta" is a Brazilian social movement, made up mostly of middle-class right-wingers. Its aim is

to “bring back ethics and values to Brazil’s legislative, executive and judicial branches, in all levels of public administration”. Source: <https://diadobasta.blogspot.com/p/carta-aberta.html>, accessed 16 July 2022.

83. “Ocupa Câmara” was a movement to invade Rio de Janeiro’s City Council, following the example of Occupy Wall Street. Source: <https://www.occupy.com/article/what-brazil-protests-mean-dialogue-global-revolt> accessed 16 July 2022.

84. “FIFA, Go Home” was a slogan used in protests against Brazil’s hosting of the 2014 World Cup. Source: <https://www.aljazeera.com/features/2013/8/1/brazil-protesters-keep-up-the-pressure>, accessed 16 July 2022.

85. Rio de Janeiro, 2013a, attachment 3, p. 301.

86. Reys, 2014, p. 48.

87. The Interstate Civilian Police Forces Service. Tiago was referring to temporary cells found in the Service’s HQ in Rio de Janeiro, located in the neighbourhood of Benfica, on the north side of the city. These cells are used to hold detainees until they are transferred to a correctional facility.

88. “Bangu” is a popular name for the Gericinó Penitentiary Complex, formerly called the Bangu Penitentiary Complex, located on the west side of Rio de Janeiro.

89. Source: <https://www.aljazeera.com/features/2013/6/30/police-violence-under-review-in-brazil>, accessed 16 July 2022. Links to videos: <https://www.youtube.com/watch?v=LKj80fWHVEo> and <https://www.youtube.com/watch?v=AV7h71qQNcs>, accessed 16 July 2022.

90. Cetina, 2005, p. 215.

91. Torinelli, 2015, p. 206.

92. Berry, 2021, p. 820.

References

Y. Abu-Laban, 2015. “Gendering surveillance studies: The empirical and normative promise of feminist methodology,” *Surveillance & Society*, volume 13, number 1, pp. 44–56.
doi: <https://doi.org/10.24908/ss.v13i1.5163>, accessed 25 July 2022.

T. Albury, 2021. “‘I helped destroy people’,” *New York Times* (1 September), at <https://www.nytimes.com/2021/09/01/magazine/fbi-terrorism-terry-albury.html>, accessed 16 July 2022.

S. Amadeu, 2016. “‘Vigilância em massa é inversão dos princípios democráticos’, afirma pesquisador: Sérgio Amadeu, professor da UFABC, fala sobre combate ao terrorismo no contexto das Olimpíadas: depoimento. Interview with Rafael Tatemoto,” *Jornal Brasil de Fato, São Paulo*, (4 August), at <https://www.brasildefato.com.br/2016/08/04/vigilancia-em-massa-e-inversao-dos-principios-democraticos-afirma-pesquisador/>, accessed 16 July 2022.

P. Arora, 2019. “Benign dataveillance? Examining novel data-driven governance systems in India and China,” *First Monday*, volume 24, number 4, at <https://firstmonday.org/article/view/9840/7745>, accessed 25 July 2022.
doi: <https://doi.org/10.5210/fm.v24i4.9840>, accessed 21 July 2022.

N. Arteaga, 2015. “Doing surveillance studies in Latin America: Social sorting in contexts of violence,” *Surveillance & Society*, volume 13, number 1, pp. 78–90.

doi: <https://doi.org/10.24908/ss.v13i1.5159>, accessed 25 July 2022.

Article 19, 2016. “Da Cibersegurana à Ciberguerra: O Desenvolvimento De Políticas de Vigilância No Brasil,” at <https://www.article19.org/data/files/medialibrary/38291/Da-Ciberseguranc%CC%A7a-a%CC%80-Ciberguerra.pdf>, accessed 16 July 2022.

C.R. Berry, 2021. “Under surveillance: An actor network theory ethnography of users experiences of electronic monitoring,” *European Journal of Criminology*, volume 18, number 6, pp. 817–835.
doi: <https://doi.org/10.1177/1477370819882890>, accessed 25 July 2022.

Brasil, 2014. “Journal of the Federal Senate. Year LXIX — Sup. ‘C’ to № 51 — 17 April 2014,” at <http://www.senado.leg.br/atividade/rotinas/materia/getTexto.asp?t=149208&c=PDF&tp=1>, accessed 16 July 2022.

M. Castells, 1996. *The rise of the network society*. Malden, Mass.: Blackwell.

K.K. Cetina, 2005. “Complex global microstructures: The new terrorist societies,” *Theory, Culture & Society*, volume 22, number 5, pp. 213–234.
doi: <https://doi.org/10.1177/0263276405057200>, accessed 25 July 2022.

S. Croeser and T. Highfield, 2014. “Occupy Oakland and# oo: Uses of Twitter within the Occupy movement,” *First Monday*, volume 19, number 3, at <https://firstmonday.org/article/view/4827/3846>, accessed 16 July 2022.
doi: <https://doi.org/10.5210/fm.v19i3.4827>, accessed 25 July 2022.

H.L. Cukierman, C. Teixeira, and R. Prikladnicki, 2007. “Um olhar sociotécnico sobre a engenharia de software,” *Revista de Informática Teórica e Aplicada*, volume 14, number 2, pp. 199–219.
doi: <https://doi.org/10.22456/2175-2745.5696>, accessed 25 July 2022.

E. Dahlin, 2020. “Approaching media as socio-technical assemblages in a datafied age,” *First Monday*, volume 25, number 4, at <https://firstmonday.org/article/view/10341/9408>, accessed 25 July 2022.
doi: <https://doi.org/10.5210/fm.v25i4.10341>, accessed 16 July 2022.

M. de Landa, 1991. *War in the age of intelligent machines*. New York: Zone Books.

G. Deleuze and F. Guattari, 1987. *A thousand plateaus: Capitalism and schizophrenia*. Translation and foreword by B. Massumi. Minneapolis: University of Minnesota Press.

T.V. Estevão, 2014. “O novo paradigma da vigilância na sociedade contemporânea — ‘who watches the watchers’,” *Observatório*, volume 8, number 2, pp. 155–169.

M. Foucault, 2007. “Discipline and punish: The birth of the prison,” In: B.B. Lawrence and A. Karim (editors). *On violence: A reader*. Durham, N.C.: Duke University Press, pp. 444–471.
doi: <https://doi.org/10.1215/9780822390169-018>, accessed 25 July 2022.

C. Fuchs and D. Trottier, 2017. “Internet surveillance after Snowden: A critical empirical study of computer experts attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden,” *Journal of Information, Communication and Ethics in Society*, volume 15, number 4, pp. 412–444.
doi: <https://doi.org/10.1108/JICES-01-2016-0004>, accessed 25 July 2022.

K. Guzik, 2009. “Discrimination by design: Predictive data mining as security practice in the United States’ ‘war on terrorism’,” *Surveillance & Society*, volume 7, number 1, pp. 3–20.
doi: <https://doi.org/10.24908/ss.v7i1.3304>, accessed 25 July 2022.

K.D. Haggerty and R.V. Ericson, 2000. "The surveillant assemblage," *British Journal of Sociology*, volume 51, number 4, pp. 605–622.

doi: <https://doi.org/10.1080/00071310020015280>, accessed 25 July 2022.

T. Herdy, 2013. "Governo brasileiro não vê indícios de invasão nos sistemas: Ministério da Defesa e Forças Armadas investigam espionagem de dados estratégicos pelos EUA," *O Globo* (14 July), at

<http://oglobo.globo.com/mundo/governo-brasileiro-nao-ve-indicios-de-invasao-nos-sistemas-9033959>, accessed 16 July 2022.

S. Hogue, 2016. "Performing, translating, fashioning: Spectatorship in the surveillant world," *Surveillance & Society*, volume 14, number 2, pp. 168–183.

doi: <https://doi.org/10.24908/ss.v14i2.6016>, accessed 25 July 2022.

E. Judensnaider, L. Lima, M. Pomar, and P. Ortellado, 2013. *Vinte centavos: a luta contra o aumento*. São Paulo: Veneta.

B. Latour, 2012. *Reagregando o social: Uma introdução a teoria do ator-rede*. Salvador: EDUFBA.

B. Latour, 2005. *Reassembling the social: An introduction to actor-network-theory*. Oxford: Oxford University Press.

J. Law, 1992. Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity, *Systems Practice*, volume 5, number 4, pp. 379–393.

doi: <https://doi.org/10.1007/BF01059830>, accessed 25 July 2022.

D. Lyon, 1994. *The electronic eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.

G.T. Marx, 2009. "Surveillance and technology: Context and distinctions," In: G.J. Leckie and J. Buschman (editors). *Information technology in librarianship: New critical approaches*. Westport, Conn.: Libraries Unlimited, pp. 47–59.

L. Morris, 2014. "Contextualizing the power of social media: Technology, communication and the Libya Crisis," *First Monday*, volume 19, number 12, at <https://firstmonday.org/article/view/5318/4166>, accessed 25 July 2022.

doi: <https://doi.org/10.5210/fm.v19i12.5318>, accessed 16 July 2022.

M. Müller, 2015. "Assemblages and actornetworks: Rethinking sociomaterial power, politics and space," *Geography Compass*, volume 9, number 1, pp. 27–41.

doi: <https://doi.org/10.1111/gec3.12192>, accessed 25 July 2022.

O.G.D.S. Neto, 2013. "Brasil, 2013: reflexões e metáforas," In: C.M. de Sousa and A. de Azevedo Souza (editors). *Jornadas de junho: Repercussões e leituras*. Campina Grande: EDUEPB, pp. 22–27.

C.L. Nurik, 2022. "Facebook and the surveillance assemblage: Policing Black Lives Matter activists & suppressing dissent," *Surveillance & Society*, volume 20, number 1, pp. 30–46.

doi: <https://doi.org/10.24908/ss.v20i1.13398>, accessed 25 July 2022.

P. Olson, 2014. *Nós Somos Anonymous: Por dentro do mundo dos hackers*. São Paulo: Editora Novo Século.

R.M.L.R. Pedro, 2005. "Tecnologias de vigilância: Um estudo psicossocial a partir da análise de controvérsias," *Anais do XXIX Encontro Anual da ANPOCS*, pp. 1–32.

G.M. Pires, 2015. "A palavra do poder que engole o poder das palavras," In: D.G. Borges and V. Cei

(editors). *Brasil em crise: o legado das jornadas de junho*. Vila Velha: Praia Editora.

J. Pridmore, 2012. "Consumer surveillance: Context, perspectives and concerns in the personal information economy," In: K. Ball, K.D. Haggerty, and D. Lyon (editors). *Routledge handbook of surveillance studies*, London: Routledge, pp. 321–329.

doi: <https://doi.org/10.4324/9780203814949>, accessed 25 July 2022.

P.E. da Rocha Resende, 2015. "A tática black bloc e a liberação anárquica do dissenso," In: D.G. Borges and V. Cei (editors). *Brasil em crise: o legado das jornadas de junho*. Vila Velha: Praia Editora.

J.P. Reys, 2014. "Um panorama dos dias quentes de junho de 2013 e além, 8/2014," In: M. Borba, N. Felizi, and J.P. Reys (editors). *Brasil em movimento: Reflexes a partir dos protestos de junho*. Rio de Janeiro: Rocco.

Rio de Janeiro, 2013a. "Process 218-01646/2013. Report on the virtual patrol conducted by the DRCI".

Rio de Janeiro, 2013b. "Decree Nº 44302 of 19 July 2013," at <https://www legisweb.com.br/legislacao/?id=256720>, accessed 16 July 2022.

Rio de Janeiro, 2013c. "Decree Nº 44305 of 24 July 2013," at <https://www legisweb.com.br/legislacao/?id=256823>, accessed 16 July 2022.

A. Romele, F. Gallino, C. Emmenegger, and D. Gorgone, 2017. "Panopticism is not enough: Social media as technologies of voluntary servitude," *Surveillance & Society*, volume 15, number 2, pp. 204–221. doi: <https://doi.org/10.24908/ss.v15i2.6021>, accessed 25 July 2022.

N. da Rocha Tiago, 2015. "Personal interviews," Rio de Janeiro.

M.C. Torinelli, 2015. "A máscara e a multidão: enquadramentos dos Anonymous nas manifestações de junho de 2013 no Brasil," at <http://dspace.c3sl.ufpr.br/dspace/bitstream/handle/1884/38194/R%20-%20D%20-%20MICHELE%20CAROLINE%20TORINELLI.pdf?sequence=3&isAllowed=y>, accessed 16 July 2022.

P. Ullrich and P. Knopp, 2018. "Protesters' reactions to video surveillance of demonstrations: Counter-moves, security cultures, and the spiral of surveillance and counter-surveillance," *Surveillance & Society*, volume 16, number 2, pp. 183–202. doi: <https://doi.org/10.24908/ss.v16i2.6823>, accessed 25 July 2022.

N. Viana and G. Roza, 2017. "Loja de souvenirs tecnológicos: Um guia para as compras da vigilância" (31 January), at <http://apublica.org/vigilancia/loja-de-souvenirs-tecnologicos/>, accessed 16 July 2022.

T. Weller, 2012. *The information state: A historical perspective on surveillance*. London: Routledge.

D.M. Wood and S. Wright, 2015. "Before and after Snowden," *Surveillance & Society*, volume 13, number 2, pp. 132–138. doi: <https://doi.org/10.24908/ss.v13i2.5710>, accessed 25 July 2022.

Editorial history

Received 14 December 2021; revised 23 June 2022; revised 17 July 2022; revised 24 July 2022; accepted 24 July 2022.



This paper is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).

The construction of a sociotechnical surveillance network in Brazil

by Pedro Braga, André Sobral, Fernando Severo, Ricardo Jullian, and Henrique Cukierman.

First Monday, volume 27, number 8 (August 2022).

doi: <https://dx.doi.org/10.5210/fm.v27i8.12410>