Evento: XXV Jornada de Pesquisa
ODS: 16 - Paz, justiça e instituições eficazes

DIGITAL CORONOPTIC: WILL THE STATE OF EXCEPTION BECOME PERMANENT?[1]

CORONÓPTICO DIGITAL: O ESTADO DE EXCEÇÃO SE TORNARÁ PERMANENTE?

Maurício Fontana Filho[2], Rodrigo Tonél[3], Janaína Machado Sturza[4]

[1] Pesquisa Institucional desenvolvida ao longo da pós-graduação em Ciências Sociais pela Universidade Passo Fundo
[2] Pós-graduando em Ciências Sociais pela Universidade Passo Fundo, UPF. Graduado em Direito pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul, UNIJUÍ. E-mail: mauricio442008@hotmail.com
[3] Mestre em Direito pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul, UNIJUÍ. Graduado em Direito pela mesma instituição. Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, CAPES. E-mail: tonelr@yahoo.com
[4] Pós-doutora em Direito pela Universidade do Vale do Rio dos Sinos, UNISINOS. Doutora em Direito pela Escola Internacional de Doutorado em Direito Tullio Ascarelli, da Universidade de Roma Tre - Itália. E-mail: janaina.sturza@unijui.edu.br

Abstract

It is an investigation on the impact of the pandemic upon the surveilling powers of the State. Its aim is on answering whether there may be an increase of vigilance and whether the State of exception created may become permanent. It starts with a positive hypothesis. Surveillance has existed for a long time, but the occurrence of a pandemic consolidates the justification of protecting the people in detriment of individual privacy. The method is the hypothetical-deductive, through which it seeks to confirm or deny an initial hypothesis using bibliographical research. An analysis on different forms of panopticon is done to better address the problem. The conclusion appoints an increase of State power legitimized by the advance of the pandemic and the fear caused by it. The new technologies seem to help build the idea of a permanent State of exception.

Keywords: Big Brother; Pandemic; Panopticon; State of exception; Surveillance.

Resumo

Trata-se de uma investigação do impacto da pandemia sobre os poderes de vigilância do Estado. Seu objetivo é responder se pode haver um aumento de vigilância e se o Estado de exceção criado pode se tornar permanente. Inicia-se com uma hipótese positiva. A vigilância existe há muito tempo, mas a ocorrência de uma pandemia consolida a justificativa de proteger as pessoas em detrimento da privacidade individual. O método é o hipotético-dedutivo, através do qual se procura confirmar ou negar uma hipótese inicial usando de pesquisa bibliográfica. Uma análise sobre diferentes formas de panóptico é realizada para melhor endereçar o problema. A conclusão indica um aumento de poder do Estado legitimado pelo avanço da pandemia e pelo medo causado por ela. As novas tecnologias parecem ajudar a construir a ideia de um Estado de exceção permanente.

Palavras-chave: Grande Irmão; Pandemia; Panóptico; Estado de exceção; Vigilância.

1 Introduction

Many people do not care very much about surveillance in the societal domain. They have trust in their State system and believe it is only a problem for criminals. Since the publication of the Snowden files in 2013 about the intense and organized spying activity of the U.S. National Security Agency (NSA), mass surveillance has become one of the most written subjects in the academy. In this context, currently the Covid-19 pandemic has added a new variable to the equation.

What is the impact of a pandemic upon the controlling power of the State? Will the State of exception become permanent? The initial hypothesis is that the State, by becoming a justifiable State of exception, progressively turns more invasive towards individual life in a permanent form, while the individual becomes more vulnerable. A pandemic justification then, afterwards, takes on a different form, but also focused on depriving people of liberty for their protection.

The methodology is the hypothetical-deductive through bibliographical research. This means that, by creating a problem, the next step is confirming or denying it by bibliographical reasoning. On the first session of the article, Jeremy Bentham's (2008) and Michel Foucault's (2013) panoptic models are briefly explored and a context is elaborated. In the end, Jeffrey H. Reiman's (1995) digital panopticon and his 4 risks of surveillance are presented. The second session is about the impact of the pandemic on the State's monitoring faculties.

Every now and then people learn from newspapers and journal articles, from documentaries and news bulletins, as well as from feature movies and television series about new developments in surveillance. That is to say, people are increasingly aware of the fact that different actors are watching them, and the effect produced continues to persist with the pandemic.

2 From Bentham's architecture to the Digital Panopticon

The monitoring system of Bentham (2008) is called the Panopticon, which means All Seeing (MANOKHA, 2018). Its objective is to guarantee the absolute publicity of the people being watched. It consists of a circular building with cells along its circumference, some of which are empty to prevent residents from communicating. "He is seen, but does not see; he is an object of information, but never a subject of communication." (FOUCAULT, 2013, p.190, our translation).

The inspector's apartment occupies the center, with each cell having its own window in order to decrease lighting expenses. The Panopticon is not a prison, but a principle of imprisonment. "Its essence, therefore, consists in the centrality of the inspector's situation, combined with the most well-known and effective devices for seeing without being seen." (BENTHAM, 2008, p.28, our translation, author's emphasis).

The fundamental principle that idealizes it is the certainty of the subject's mind that he is, without a doubt, being inspected, watched at every second of every moment (BENTHAM, 2008). "The idea was to build the prison cells in a circle around the guard post" (REIMAN, 1995, p.28) to make the watched feel as if he was being monitored at all times. If the prisoner blinked, someone would see it; if he moved, sighed, coughed or even yawned at all someone would be ready to persuade him to stop any unwanted practices.

"The very fact of general visibility – being seeable more than being seen – will be enough to produce effective social control." (REIMAN, 1995, p.28). The basic idea is that the people to be inspected should always feel as if they were under inspection, which would facilitate the reforms of their behavior, and that is the main point: change the way people behave. This disciplinary tool works even though there may be no one in the guardhouse. In this form, through fear (BENTHAM, 2008).

"No matter how different or even how opposed the purposes may be" (BENTHAM, 2008, p.19, our translation), the project can be applied to any institution, both schools, hospitals, prisons and companies. In a school, the inspector would be the teacher; in hospitals, the doctor; in penitentiaries, the director and in the Market, the contractor (BENTHAM, 2008).

Imagine an employee who believes he is under watch at all times, which motivates him to use every second of his time to meet his boss's expectations for productivity. The more constantly the people under inspection are in sight of the inspectors, the more perfectly the establishment achieves its purpose. Ideal perfection “requires that each person remains in that condition, during every moment of every time of their lives.” (BENTHAM, 2008, p.20, our translation).

It is a means of ensuring control of the mind over the mind, the few over the many. The inspector must see without being seen. This control of the mind over the mind is what Byung-Chul Han (2017) qualified as psychopolitics. The circular shape makes it possible for the inspector to have perfect vision without having to change position. The inspector's power encompasses more than an objective skill, that of inspecting, also comprising the subjective potency of fear (BENTHAM, 2008).

This power of fear works by making one believe he is seen at all times. In George Orwell's (1992) major work, Nineteen-Eighty-Four, the Big Brother figure serves as the perfect example for the watcher. The people's belief was that they were always under watch, no matter what they did, where they went or what they thought. In the case of the inspector, nobody would know for sure if he was there, but still he would be obeyed, out of fear (BENTHAM, 2008).

Everyone is kept under surveillance both in visual and audio, because of this, people begin to see themselves as being observed and therefore behave according to a set of rules. “This is comparable with the situation in organizations, which keep their members under surveillance” (TAEKKE, 2011, p.443), and the data collected about these individuals transforms them, disciplining the way they act and what they become.

Wherever we drive, we drive in the public world, and thus normally subject to unobjectionable public observation. The means by which all this is achieved is the destruction of privacy and the transfer of men to an environment of constant tension and, more precisely, eternal surveillance (REIMAN, 1995).

Not only does the panoptic machine makes one visible, but it also hides the motives, practices and ethics of the operations from the supposed viewer. “To know one is being seen without being able to see carries with it an uncertainty that becomes a source of anxiety, discomfort and terror…Who is watching? Why are they watching? What will they do?” (SIMON, 2002, p.4).

All of this is supposedly a function of the relationship of vision established by the panoptic machine. Faced with an uncertainty with whether someone is watching, the subject watches himself. “That is, he behaves as if he was being watched and so is careful not to attract the ire of the observer who he imagines is there. The inmate thus tows the line and conforms to the explicit and even implicit rules of the institution; all because he imagines he is being watched.” (SIMON, 2002, p.5).

In Yevgeny Zamyatin’s (2007) work, We, the individuals in their apartments had walls of transparent glass, this aiming at their monitoring by the State and its disciplinary program, that is, to prevent any individualities in their citizens to diversify from the wanted pattern. In this scenario, even the most intimate moments of private life were made public. Everything that was considered peculiar was taken away, and the surveillance system paid attention to the end of shaping behavior.

Making it short, “Bentham’s Panopticon involves three main assumptions: first, the omnipresence of the inspector, ensured by his total invisibility; second, universal visibility of objects of surveillance; and third, the assumption of constant observation by the watched.” (MANOKHA, 2018, p.222).

According to the Bentham Project (2020), the world center for Bentham Studies and a part of the University College London's (UCL) Faculty of Laws, many panopticons were built all over the world, or at least relative models and institutions based upon Bentham’s principle of surveillance. Some of the prisons that no longer exist reflect his ideas for the Panopticon. However, none of them conforms precisely to the detailed drawings, nor to Bentham's key principle of management: the unobserved inspection.

The panopticon was not originally Jeremy Bentham’s idea. It belonged to his brother, Samuel. When he was working in Russia with an unskilled workforce, he sat himself in the middle of his factory and arranged the workforce in a circle around his central desk as to keep an eye on what everyone was doing. When Jeremy visited Samuel in the late 1780s, he understood it and decided the centralized arrangement could be applied in a completely larger vision (MCMULLAN, 2020).

Bentham never saw a panopticon built during his lifetime. A number of prisons have since incorporated some of its elements into their design, but it was not until the 1920s that the closest thing to a panopticon prison was built, the Presidio Modelo complex in Cuba, infamous for corruption and cruelty, now abandoned (MCMULLAN, 2020).

That its design is panoptic is a claim made by many prisons such as Kilmainham Gaol, in Dublin, Ireland. Buildings designed for other purposes were also called panopticons, but only a few resemble a circular plan, like the Edinburgh panopticon, in Great Britain. In Siena, Italy, there is the Padiglione Conolly, opened in 1876, part of the now decommissioned Psychiatric Hospital San Niccolo, as well as the Santo Stefano prison, established in 1795 and closed in 1965 (BENTHAM PROJECT, 2020).

In Lisbon, Portugal, there was the Hospital Miguel Bombarda. It was designed to be a forensic prison infirmary for patients from the penitentiary and those considered dangerous. It functioned from 1896 to 2000, when closed. In Netherlands, the Lelystad Prison, built in 1995, consists of two domes with a central guard station. Haarlem, another structure, was built in the early 20th century (BENTHAM PROJECT, 2020).

In Russia, the St Petersburg panopticon was built rather as a school than a prison. In Spain's Mataró city, it was established a panopticon in 1863, while in Switzerland, Geneva, in 1825 and demolished in 1862. In the United States, there are two, the Rahway Prison, in New Jersey, and the Stateville Penitentiary, in Illinois. In Colombia, the Bogota Panoptico was built between 1874 and 1905, while it has since 1948 been transformed into a museum (BENTHAM PROJECT, 2020).

Foucault (2013, p.197, our translation) used Bentham's panopticon structure as a metaphor for mechanisms of large-scale social control, but went further, proposing that it is a mechanism for "organizing power". An (organized) power of repression that preys upon an (unorganized) individual liberty towards discipline and behavior shaping.

In this new vision of the panoptic that goes beyond the architectural arrangement, Foucault (2013) sums up the development of the big old-fashioned institutions in relation to surveillance, that is, for instance, how monasteries throughout the centuries have developed surveillance to ensure the "monks worked and behaved as demanded" (TAEKKE, 2011, p.444), which means, enclosure, partitioning, functional sites and ranks.

Every monk had to be at a special place at a particular time according to special schedules, in a certain position in a line of monks, doing specific functions and so on. Foucault (2013) brings context into the matter by signaling old practices that fit as the panopticon's monitoring bases, as "the panopticon is arranged with such ingenuity that the inmates do not know when they are under surveillance, which forces them to adopt a pattern of conformity." (TAEKKE, 2011, p.444). He finds the principle of conformity in many old customs and social institutions, long before the panopticon's invention.

Reimans (1995) focus on the digital panopticon, which is an informational tool to control individuals. It harms individual freedom with too much publicity characterized "under four headings: First, the risk of extrinsic loss of freedom; second, the risk of intrinsic loss of freedom; third, symbolic risks; and, fourth, the risk of psychopolitical metamorphosis." (REIMAN, 1995, p.34, our emphasis).

> By extrinsic loss of freedom, I mean all those ways in which lack of privacy makes people vulnerable to having their behavior controlled by others.

> Most obviously, this refers to the fact that people who want to do unpopular or unconventional actions may be subject to social pressure in the form of denial of certain benefits, jobs or promotions or membership in formal or informal groups, or even blackmail, if their actions are known to others. (REIMAN, 1995, p.35).

By intrinsic loss of freedom, the denial of privacy limits people's freedom directly, independently of the ways in which it makes them susceptible to social pressure or penalties. In other words, privacy is not just a means of protecting freedom; it is itself constitutive of freedom (REIMAN, 1995). “When you know you are being observed, you naturally identify with the outside observer's viewpoint, and add that alongside your own viewpoint on your action.” (REIMAN, 1995, p.38).

This double vision makes people act differently, whether the act is making love or driving. “The targets of the panopticon know and feel the eye of the guard on them, making their actions different than if they were done in private.” (REIMAN, 1995, p.38). Their repertoire of possible actions diminishes as they lose the choices whose intrinsic nature depends on privacy.

Both Orwell’s (1992) and Zamyatin’s (2007) citizens on their respective works are submissive and afraid to oppose the dominant party that watches them. In addition, they have embraced themselves on the party’s traditions and customs, values and practices, molding their behavior towards the State’s will as much as in accord to society’s expectations.

The third risk of surveillance is the symbolic. The panopticon symbolizes a kind of draining of the individual sovereignty away and outside of people into a single center. (REIMAN, 1995). People become its data to observe at will, while people’s outsides belong inside the system rather than to their own. “I have called this a symbolic risk because it affects us as a kind of message, a message inscribed in an institutional structure.” (REIMAN, 1995, p.39).

People are not deprived of their self-ownership in the way slaves permanently or prisoners temporarily are. Rather, the arrangement of the institution broadcasts an image of them and to them as beings lacking the authority to withdraw themselves from its view (REIMAN, 1995). “It conveys the loss of self-ownership to us by announcing that our every move is fitting data for observation by others. As a symbolic message, it insults rather than injures.” (REIMAN, 1995, p.39).

By the use of symbols people come to acquire their self-conceptions. “They shape the way we identify ourselves to ourselves and to one another, and thus they shape our identities themselves.” (REIMAN, 1995, p.40). Growing up in the informational panopticon, people are less likely to acquire selves that think of themselves as owning themselves. They tend to say mine with less authority and yours with less respect (REIMAN, 1995), just like in Zamyatin (2007) the I is a natural vice, while the We is a virtue, which explains pretty much the title of his book.

The fourth and last is the risk of psychopolitical metamorphosis. “People who are shaped to act in ways that are publicly acceptable will tend to act in safe ways, to hold and express and manifest the most widely-accepted views, indeed, the lowest-common denominator of conventionality.” (REIMAN, 1995, p.41). Reiman (1995) uses the example of the pressure television sponsors exercise against anything unconventional, in their fear of offending any segment of the purchasing population.

People willingly change their behavior in order as to get the sponsors they need, but this also applies towards surveillance. Being watched impacts the way people live their lives, which means they change the ways they are, adapting themselves to a seen life. Because of monitoring, people “will tend to act in ways that are publicly acceptable.” (REIMAN, 1995, p.41).

In Orwell (1992), the generality of people punished have a conscience of having done something wrong. The context would make them accept the punishment as a deserving response to whatever they had done. “To say that people who suffer this loss will be easy to oppress doesn't say enough” (REIMAN, 1995, p.42), they would welcome oppression as a friend, and the reason is that their social context of oppression normalized the situation through time.

They would not have to be oppressed, since there would not exist anything in them tempted to drift from the beaten path or able to see beyond it. “The art of such people will be insipid decoration” (REIMAN, 1995, p.42), they would not be people anymore, as the digital panopticon would have taken every data from them and imposed every value. In the end, they would turn into panoptic extensions.

3 Surveillance, pandemic and the Coronopticon

These models and panoptic theorizations go far beyond political theory, as an era of constant data collection has taught. The Snowden files on the NSA has brought information to the public as well as impelled an intense number of academic research on the matter of surveillance (FRIEDERSDORF, 2020). Although much has changed since Bentham (2008), not the fact that the interface of the computer screen, the camera lens and the telemarketer “remain critical components for understanding the character of contemporary informed surveillance” (SIMON, 2002, p.18).

With the pandemic spreading worldwide, new forms of panopticons have made themselves felt, as people, during these times of crisis, are willing to renounce their freedoms for security, embracing States of exception. The cell phones play a huge part in this (ECONOMIST BRIEFING, 2020).

The panopticon is a way to watch and discipline citizens. However, there is no need of a round building to watch people anymore, not with monitoring electronic communications from a central location. In many ways, the watchtower at the heart of the panopticon is a precursor to the cameras, purposely-visible machines with human eyes hidden from view, stuck onto most of today’s time buildings and electronic devices (MCMULLAN, 2020).

A person buys a new phone, whatever the brand; he opens the box, presses the call button, the cell phone connects to the Internet and, without doing anything else the most sophisticated surveillance machine of his routine has started. It does not matter if he is going to download Facebook, activate a Google account, or give all access permissions to any weird flashlight or antivirus applications. Before taking any action, the new phone has already started sharing details of his life (COLOMÉ, 2019).

Bart Simon (2002, p.16) uses the term “Superpanopticism” to describe today’s digital surveillance of data. The diagram of superpanopticism is not a diagram of surveillance in the traditional sense, as no one is watching people and they do not perceive themselves as being watched. People simply go about their business while their database selves are assembled, scrutinized and evaluated. However, this is done with much more detail than in past modern times (SIMON, 2002).

The factory-preinstalled software is the perfect feature of cell phones to know its future activity, like where it is, what it downloads, what messages it sends, what music files it keeps. The most serious element in this is the scale, as there are hundreds of millions of cell phone devices. People’s personal information is sent to a wide network of destinations, which changes according to the phone (COLOMÉ, 2019).

A cell phone can have more than 100 pre-installed applications and hundreds of other libraries, which are third party services included in its code, many of which specialize in user surveillance and advertising. A cell phone is not just the product of its manufacturer as several companies are involved in its production chain. It is impossible to determine the definitive control of all the software placed there, and who has privileged access to the user's data. The result is an uncontrolled system, where no one is currently able to take responsibility for whatever happens to people's most intimate information (COLOMÉ, 2019).

The mechanism for assembling the do it yourself mini-panopticons, portable and personal furniture is commercially supplied. People, voluntarily, have the responsibility to choose and acquire these mechanisms, assemble them and put to work. Monitoring devices come from the purchase of cell phones and computers and by subscribing to social networks and information sharing websites. A kind of voluntary monitoring in an era of digital surveillance (BAUMAN, 2013).

Hence, the voluntary bondage of Étienne de Boétie (2017) takes a digital sense, as voluntary bondage to technology. A guard with his gun in hand shaped the panopticon of the past, but more recently, it has been the computer technicians and database specialists; they are the "data processing engineers" (BAUMAN, 2013, p.74, our translation) that guard the panopticon. Moreover, with the pandemic, they guard the coronopticon.

However, what is it that organizations are actually monitoring? Is it attitude, behavior, efficiency, quality or quantity of executed tasks? The answer is that it can be any one of these parameters, or in fact all of them that the management measures when they work with the results of surveillance (TAEKKE, 2011). "It is a matter of which decisions are made in specific organizations about what is monitored and how it is measured with which consequences." (TAEKKE, 2011, p.444).

In 2018, the NSA obtained 14 court orders for information gathering purposes, but the amount of information was of 434 million call detail records involving 19 million phone numbers. It was not until the Edward Snowden leaks that the scale of NSA operations became known. This makes the system more panoptic post-Snowden, when people are aware of it. Although the emphasis has not been on correcting behavior, but on providing security, namely from terrorists. In this way, a panoptic society is accepted as long as terrorists exist (FRIEDERSDORF, 2020).

In the private space of personal browsing people do not feel exposed, they do not feel like their body of data is under surveillance because they do not know where that body begins or ends. People live so much of their lives online, share so much data, but feel nowhere near as much attachment for their data as they do for their biological bodies. People's data, however, is under surveillance, not only by the government, but also by corporations that make money capitalizing on it (MCMULLAN, 2020).

During the pandemic of Covid-19, on the other hand, a new level of surveillance has being achieved. Governments are imposing new digital surveillance tools to track and monitor individuals. Many citizens have welcomed tracking technology intended to bolster defenses against the new coronavirus. Authorities in Asia, where the virus first emerged, have led the way in surveillance impositions (LIN; MARTIN, 2020).

Many governments did not seek permission from individuals before tracking their cell phones to identify suspected coronavirus patients. South Korea, China and Taiwan, after initial outbreaks, obtained early successes in flattening infection curves to their use of tracking programs. In Europe and the U.S, there are monitoring initiatives on citizen movement by tapping telecommunications data (LIN; MARTIN, 2020).

The most acquired monitoring tools in use fall into three categories, very distinct from one another. The first is documentation, by using technology to say where people are, where they have been or what their disease status is. The second one is modelling, by gathering data that helps explain how the disease spreads. Additionally, the third is a new form of contact tracing that identifies people who have had contact with known infected (ECONOMIST BRIEFING, 2020).

When it comes to documentation, most of the action is done while in quarantine by replacing phone calls and home visits with virtual checking-up. Hong Kong uses WhatsApp, while South

Korea has a customized application that sounds an alarm and alerts officials if people stray away from home. Taiwan uses a different approach, tracking quarantined people's phones through data from cell-phone masts. If it detects someone out of bounds, it texts them and alerts the authorities (ECONOMIST BRIEFING, 2020).

"Over the years, social media like Facebook have developed complex strategies in order to exercise better surveillance over its users." (ROMELE et al, 2017, p.214). Even deleting one's own profile does not guarantee Facebook would stop making use of the information gathered as it is on their policies that the information associated with a person's account would be kept, unless Facebook no longer needed the data to provide products and services (ROMELE et al, 2017).

Phone companies know roughly where all their mobile customers are from and where they have been, this accomplished from natural tracking devices. Moreover, because people pay to offer advertisements, internet companies such as Bytedance, Facebook, Google and Tencent gather much data about what their billions of users are doing and where (ECONOMIST BRIEFING, 2020).

In Turkey, the people are accustomed to an intrusive and increasingly authoritarian central government. Any misgivings have also been tempered by a feeling the State should be taking stronger measures to control the outbreak. The virus-tracking applications aim at tracking the virus, but they track people too. South Korea's health authorities monitor the movement of people and then later retrace the steps of those diagnosed with the virus by using GPS phone tracking, credit card records, surveillance video and interviews with patients (FAHIM et al, 2020).

At least 27 countries are using data from cell phone companies to track the movements of its citizens. The monitoring has raised fewer objections in countries that have been more successful at battling the virus, like Singapore, and provoked a much louder debate in Europe and the United States, a difference reflected in the numbers of people who voluntarily download tracking applications (FAHIM et al, 2020).

In South Korea, fines for breaking quarantine and leaving the house without a phone are expensive and often accompanied by the threat of prison (ECONOMIST BRIEFING, 2020). China's Health Check application works through portals of online payment, such as Alipay and WeChat. These take self-reported data about places visited and symptoms to generate an identifying code displayed in green, orange or red, corresponding to free movement and send the information to the government (KUO, 2020).

Governments can use the same data to check how their policies are performing at a district or city level. In Germany, Deutsche Telekom has provided data to the government's public-health agency. The British government follows the same pattern as they can simply require the information they need through the Investigatory Powers Act of 2016, which gives power to take whatever data it wishes from any company within its jurisdiction, and to do so in secret (ECONOMIST BRIEFING, 2020).

Over the last few months, Chinese citizens have had to adjust to a new level of government intrusion. Getting into one's apartment compound or workplace required scanning a personal code, writing down the name and ID number, temperature and recent travel history. Operators track people's movements while social media platforms like WeChat and Weibo have hotlines for people to report others who may be sick. Some cities are offering people rewards for informing on sick neighbors (KUO, 2020).

Chinese companies are rolling out facial recognition technology that can detect elevated temperatures in a crowd or flag citizens not wearing a facemask. Many applications use citizen personal health information to track people as well (KUO, 2020). Countries are learning how to use surveillance technology to address the pandemic problem, but some are more incisive in its use than others are, such as Singapore, South Korea, China, Israel (ECONOMIST BRIEFING, 2020).

> With the more recent rise of biometrics and facial recognition technologies, as well as with the growth of social networks comprising hundreds of millions of users, the extent of the data on individuals possessed by governmental and, in particular commercial entities, has become gigantic. (MANOKHA, 2018, p.227).

The use of data becomes most controversial when it moves beyond modelling and informing policy to the direct tracking of individuals in order to see from whom they got the disease. Such contact tracing is the same used for modern counter-terrorism tactics. The technology to track and trace already exists and is being used by governments all around the world, but now there is a rational justification: saving human lives from the pandemic (ECONOMIST BRIEFING, 2020).

The justification for quarantine tends to be based upon the idea of protecting the people against the invisible virus. However, this may be a permanent situation as new viruses could possibly appear and install themselves among societies. This reasoning is useful for a State of exception to legitimize and build its actions with public support (LACERDA, 2020). Many people are willing to renounce their freedoms voluntarily, but if pandemic and epidemic situations would last longer, they could forget what it means to have privacy (KUO, 2020).

Surveillance used as an alternative to deal with a pandemic is not the full potential of it. This type of governing also applies to a completely new sphere of subjects, like for controlling the Media. Because this method has been used before, citizens tend to accept it with more ease as it becomes normal. Not every Chinese person defends an invasive government. Those that do not do tend to claim a State capable of monitoring every step of its citizens is a threat to their privacy (KUO, 2020).

However, a threat to privacy is only worrisome as long as it is valuable to someone (REIMAN, 1995). By this, the fact that most Chinese and Asian people in general do not favor privacy comes up. It is a completely different culture, with their own values. For this reason, “in Asia, pandemics are fought not only by epidemiologists and virologists, but also by computer experts and macrodata.” (LACERDA, 2020, p.81, our translation).

Privacy is “the counter-discourse of surveillance: if surveillance is the possibility to exercise control over the subjects, privacy is the ability that the subjects have to seclude themselves or withhold information about themselves.” (ROMELE et al, 2017, p.212). The expanded digital surveillance of the Chinese State is as culturally accepted as effective against pandemics. It is a State of permanent exception, but it seems to work very well. Why then not accept it as a government model? (LACERDA, 2020).

This is a critic proposed by Marcos Lacerda (2020, p.81, our translation): “why not consider that this model of digital bio political governance can be exported and become a desirable model of global governance”, especially in the face of the daily tragedy experienced by Europe and the Americas on the pandemic? Perhaps following China’s surveillance impositions would be adequate, he suggests. It all depends on how much people value their privacy and how much afraid of an unsure future they are.

This pandemic provides more reason for the government to surveil the public. As the major events of the 2008 Olympics held in Beijing and the Shanghai Expo in 2010 created circumstances of permanent surveillance, so does the coronavirus. Lacerda’s (2020, p.83, our translation) idea of context calls upon these circumstances that change people’s minds on accepting or opposing governmental surveillance as “social consequences of the virus”.

4 Final considerations

In a matter of months, tens of millions of people in dozens of countries were placed under surveillance. Governments, private companies and researchers observe the health, habits and movements of citizens, very often without their consent. It is a massive effort, aimed at enforcing quarantine rules and tracing the spread of the coronavirus. The techniques of mass surveillance tend to become more evident and intensified as natural justifications are constructed, like protecting the people from terrorism and diseases.

Because of the pandemic, surveillance seems to be unavoidable. State authorities, in addition to locking down entire cities, have implemented security measures in the name of containing the coronavirus outbreak. From top officials to local community workers, those enforcing the rules repeat it is only a corollary of these times of exception, proposing soon things would return to normality.

However, monitoring were already everywhere even before the pandemic. Most countries used to disturb their citizens in a minor or major degree with surveillance. The pandemic has just made more obvious and justifiable the use of monitoring devices. The question is how many of these new measures are here to stay. Intrusive surveillance is already becoming the new normal as people accept it willingly, in some countries.

The set of actions associated with pandemic prevention and treatment policies could extend itself ad infinitum, and with it generate a permanent State of exception alongside new forms of socialization, with the moral justification of protecting biological life. The impact of the pandemic is that people are so afraid they willingly renounce privacy over a sense of security.

Bibliographical references

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Rio de Janeiro: Zahar, 2013.

BENTHAM, Jeremy. **O panóptico**. 2. Ed. Belo Horizonte: Autêntica Editora, 2008.

BENTHAM PROJECT, 2020. Available at:<https://www.ucl.ac.uk/bentham-project/>. Access in: 12 Jul. 2020.

COLOMÉ, Jordi Pérez. **Como você é espionado por seu celular Android sem saber**, 2019. Available at:<https://brasil.elpais.com/brasil/2019/03/17/tecnologia/1552777491_649804.html>. Access in: 16 Jul. 2020.

ECONOMIST BRIEFING. **Countries are using apps and data networks to keep tabs on the pandemic**, 2020. Available at:<https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic>. Access in: 12 Jul. 2020.

FAHIM, Kareem; KIM, Min Joo; HENDRIX, Steve. **Cellphone monitoring is spreading with the coronavirus**: so is an uneasy tolerance of surveillance, 2020. Available at:<https://www.washingtonpost.com/world/cellphone-monitoring-is-spreading-with-the-coronavirus-so-is-an-uneasy-tolerance-of-surveillance/2020/05/02/56f14466-7b55-11ea-a311-adb1344719a9_story.html>. Access in: 13 Jul. 2020.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 41.Ed. Petrópolis: Vozes, 2013.

FRIEDERSDORF, Conor. **The Costs of Spying**, 2020. Available at:<https://www.theatlantic.com/

ideas/archive/2020/02/costs-spying/607177/>. Access in: 13 Jul. 2020.

HAN, Byung-Chul. **Psychopolitics**: Neoliberalism and New Technologies of Power. New York: Verso, 2017.

KUO, Lily. **'The new normal'**: China's excessive coronavirus public monitoring could be here to stay, 2020. Available at:<https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay>. Access in: 16 Jul. 2020.

LA BOÉTIE, Étienne De. **Discurso sobre a servidão voluntária**. São Paulo: Edipro, 2017.

LACERDA, M. Governança na pandemia: a ciência como regulação moral e os problemas da biopolítica. **Simbiótica Revista Eletrônica**, v. 7, n. 1, p. 69-86, 2020.

LIN, Liza; MARTIN, Timothy W. **How Coronavirus Is Eroding Privacy**, 2020. Available at:<https://www.wsj.com/articles/coronavirus-paves-way-for-new-age-of-digital-surveillance-11586963028>. Access in: 16 Jul. 2020.

MANOKHA, Ivan. Surveillance, Panopticism, and Self-Discipline in the Digital Age. **Surveillance & Society**, v.16, n.2, p.219-237, 2018.

MCMULLAN, Thomas. **What does the panopticon mean in the age of digital surveillance?**, 2020. Available at:<https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham>. Access in: 13 Jul. 2020.

ORWELL, George. **Nineteen Eighty-Four**. London: Everyman's library, 1992.

REIMAN, Jeffrey H. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. **Santa Clara High Technology Law Journal**, v.11, n.1, p.27-43, 1995.

ROMELE, Alberto; EMMENEGGER, Camilla; GALLINO, Francesco; GORGONE, Daniele. Panopticism is not Enough: Social Media as Technologies of Voluntary Servitude. **Surveillance & Society**, v.15, n.2, p.204-221, 2017.

SIMON, Bart. The Return of Panopticism: Supervision, Subjection and the New Surveillance. **Surveillance & Society**, v.3, n.1, p.1-20, 2002.

TAEKKE, Jesper. Digital panopticism and organizational power. **Surveillance & Society**, v.8, n.4, p.441-454, 2011.

ZAMYATIN, Yevgeny. **We**. London: Vintage, 2007.

Parecer CEUA: 3.069.588