Contributions of the book *De Orwell al cibercontrol* to understand cyber control

Aportes da obra De Orwell al cibercontrol para entender o cibercontrole

JIANI ADRIANA BONIN[a]

University of Vale do Rio dos Sinos (Graduate Program in Communication Sciences.
São Leopoldo – RS, Brazil

ABSTRACT

In this text I systematized contributions from the book *De Orwell al cibercontrol*, by Armand Mattelart and André Vitalis to reflect on the problem of cyber control. Their contributions serve as basis to understand the phenomenon in three dimensions: a) as a new form of social control, historically managed and umbilically related to state, geopolitical and economic interests associated with the development of digital technologies; b) as a new type of exercise of power, distinct from disciplinary power; and c) as a field of contradictions, with possibilities of resistance and social protestation. Along with the restoration of these contributions I explore some complementary lines of thought for the investigation of contemporary cyber control.

Keywords: Cyber control, cyber-surveillance, Mattelart and Vitalis

[a] Professor and researcher at the Graduate Program in Communication Sciences at Unisinos. Orcid: https://orcid.org/0000-0001-8598-7411. E-mail: jianiab@gmail.com

RESUMO

Neste texto, são sistematizadas contribuições do livro *De Orwell al cibercontrol*, de Armand Mattelart e André Vitalis, para pensar a problemática do cibercontrole. São recuperados aportes para a compreensão do fenômeno em três dimensões: a) como nova forma de controle social, historicamente gestada e umbilicalmente ligada a interesses estatais, geopolíticos e econômicos associados ao desenvolvimento das tecnologias digitais; b) como nova modalidade de exercício do poder, distinta do poder disciplinar; e c) como campo de contradições, com possibilidades de resistência e de contestação social. Junto à restauração desses aportes, são exploradas algumas linhas complementares para a investigação do cibercontrole contemporâneo.

Palavras-chave: Cibercontrole, cibervigilância, Mattelart e Vitalis

DOI:http://dx.doi.org/10.11606/issn.1982-8160.v14i3p197-211

INTRODUCTION

> *To resist the rise of the whole of security is to restore the idea that control techniques cannot replace the political resolution of the fundamental problems of society* [1].
> (Mattelart & Vitalis, 2015, p. 12)

THE PROCESS OF digitalization of societies has reconfigured our communicative ecosystem, opening up new possibilities for subjects, groups, collectives and social movements from the dissemination and access to production resources and the social appropriation of digital technologies. However, it has also been accompanied by strong contradictions, such as the concentration of property and business in a small number of transnational economic groups and the constitution of cyber control, which is a renewed form of social control, whose nature and consequences need to be critically investigated.

Since the 1960s Armand Mattelart[2] has been engaged with investigating the control problem. His analyzes in this field include examining the forms of geopolitical control of systems, means, industries and communication flows in the world (Maldonado, 2015). In his recent works, he has been concerned with the examination of cyber control, an issue that acquired relevance and crucial importance with the expansion of digitalization. This paper aims to discuss cyber control drawing on Mattealrt and Vitalis' contribution in their book De Orwell al cibercontrol, in view of its relevance, topicality, and investigative richness.

The research script for this work is focused on three dimensions present in the investigative work of Mattelart and Vitalis (2015), which I consider keys to understanding cyber control: 1) its historical processes; 2) the specificities of this new form of exercising power; and 3) possibilities of appropriation and social resistance. Along with this analysis, I also explore some complementary lines of reflection from the dialogue with the work of other researchers who have been studying the theme[3].

---

[1] In the original: "Resistir al ascenso del *Todo securitario* es restaurar la idea según la cual las técnicas de control no pueden servir como sustituto de la resolución política de los problemas de fondo de la sociedad". Translation of the author.

[2] A detailed and consistent analysis of this contribution was carried out by Efendy Maldonado (2015).

[3] Mainly I consider the work of Sérgio Amadeu Silveira, Fernanda Bruno and some researchers who participated in the book *Tecnopolíticas da vigilância* (Technopolicies of surveillance), launched in 2018, the result of a seminar promoted by the *Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade* (Lavits) [Latin American Network of Studies on Surveillance, Technology and Society], operating since 2009.

I start from the historical point of view proposed by the authors to investigate the genesis of cyber control and its development.

THE EMERGENCY OF CYBER CONTROL IN A HISTORICAL PERSPECTIVE

A relevant aspect of the contribution of Mattelart and Vitalis (2015) examined here is the adoption of a historical perspective to understand the process that leads to the constitution of cyber control. Thus, the researchers' contribution challenges views that, abdicating the historical perspective and abstracting its economic-political dimension, produce limited understandings of the phenomenon that preclude the possibilities to more effectively comprehend its political meaning, its specificities and social consequences.

In the research carried out, the researchers dedicated themselves to the construction of a genealogy of the uses and functions of the technologies of social control from a specific object: the techniques of profiling people with the objective of controlling them. This is the *profiled*, a term that comes from police or industrial language and refers to the form of indirect control of people based on the exploitation of information obtained about them. The profile is understood as a technopolitical device. To decipher it, they investigated the emergence, processes of experimentation, improvement and social expansion of such device, unveiling its articulation with state, geopolitical and market interests that engender it. The authors explored its transformations until their global expansion, driven by the mercantile motives of neoliberal hegemony and by the immense advance of national security strategies, combined with digital technologies. They sought to examine this phenomenon based on the local reality of the French state, exploring its intertwining with the global dimensions of the phenomenon. They discussed and denounced the risks to freedom, privacy and democracy introduced with this process.

The authors' view allows us to see how political and rights-based progress is accompanied by forms of control that limit their effects and how security prescribes limits to freedom. It also shows that the tensions between freedom and control have historically become more complex and derive new intensified forms during periods of economic crisis, political revolution and wars. On these occasions, we can see the use of existing means of control in a more pronounced way, as well as the creation of more effective surveillance technologies.

It is worth noting that the historical reconstruction carried out by the researchers covers a limited period, detailing these processes based on the

French reality and taking into account mainly their articulations with the European and American scenario. According to the authors, the French state was one of the first to experiment with population tracking techniques, already in the mid-19th century, based on records of delinquent and repeat offenders and the creation of a state apparatus to measure and classify crimes. This phenomenon was not confined to penal institutions, expanding to various spheres of economic activities and daily life, and according to the authors, it expresses a way of governing.

For the systematization that I proposed in this work, it is interesting to recover fundamental features of the process that were examined in detail by the researchers. The reconstruction has as starting point the context of the Industrial Revolution, in the 1850s, when an economy anchored in the international division of labor took shape. The market became the axis of a new order of social relations, demanding freedom of movement for people and goods, which is fundamental for the realization of the new economic order. Paradoxically, mechanisms to control the movement of nomads, traveling professionals, homeless people and immigrants were created and improved by the states and the police, indicating the obsession of the powers for marginalized populations. Statistics is put at the service of police controls, placing itself as a tool for social regulation, inaugurating the mathematization of mass management.

During this period, measurement, control and regulation of time started to order the social experience. In addition to the control of people, there was the continuous movement of goods. Factories become a key space for experimenting and perfecting control devices, designed to monitor workers' displacements and time their gestures aimed at developing processes to maximize income from work flows, in line with Taylorism, also fed studies focused on industrial efficiency and psychology.

Then, the processes of Taylorization of consumption were soon consolidated, fueled by mass communication and the development of the advertising industry. From the 1940s on, consumption has become a field of experimentation with polling techniques to control consumer behavior, with a view to knowing and acting on their needs. These processes preceded and fed the development of contemporary data mining strategies developed in the digital environment for the production of consumer profiles.

After the Second World War, the welfare state emerged in the European context, divided between the providential and the security role. Within its scope, protection measures were created for impoverished populations and ways of monitoring assisted populations were introduced. A bureaucratic system for the

administration and management of population data was developed, and both and private databases were improved, expanding the forms of surveillance and the possibilities for social control. Statistical techniques were put at the service of these forms of monitoring and social regulation.

In the post-war period, in a Cold War scenario, national security was brought to the forefront of state policies. The United States developed a military-industrial complex and later the teleinformatics systems were invented that would allow the creation of future mass surveillance devices.

Since the 1940s, the United States has developed a permanent war economy, in which information and communication technologies play a key role. Satellites, computer spy systems, geolocation technologies, drones and non-lethal weapons are part of the devices developed, tested and perfected in this sphere.

From the 1970s onwards, we had the decline of the welfare state, accompanied by crises of governance of democracy and the model of economic growth, which paved the way for neoliberalism and its policies of savage deregulation. Information technologies started to be seen by industrial societies as a way out of the crisis and, since then have spread socially, which made possible the computer revolution of control. The computerized processing of personal data was thus multiplied.

At the beginning of the 21st century, national security is once again gaining prominence in the strategies of Western states, under the pretext of combating terrorism, with the figure of the vigilant state. As of the September 11, 2001 attacks, the US government began to reinforce its security, civil and military arsenal, triggering a generalized mobilization of security in the western states, reinforced from those attended on March 11, 2004 in Madrid, July 7, 2005 in London and January 7, 2017 in Paris. The advance of security dynamics had an impact on communication processes and the circulation of people, messages and goods.

In this scenario, the war on terrorism has internationalized, becoming a common element of security policies, doctrines and strategies in various parts of the world, with Western countries at the forefront. Interagency and intersectoral synergies were strengthened and the doctrines of war began to be oriented towards the field of information, aiming to act in the capacity of understanding and action of the "enemy." For the United States, making this war operational required the restructuring of mechanisms for the collection and dissemination of information worldwide, the placement of intelligence agencies in networks and the expansion of their analytical capacity.

The interconnection of police and administrative databases has accelerated in this context, driven by the concern of public authorities to

identify potential focuses of violent or deviated behavior. The measures progressively implemented by the states established the bases for a renewed control structure, based on the increase of databases and their interconnections, on the improvement of the identification of people (especially through biometrics) and on the experimentation of automatic classification and classification methods detection.

For a long time, the construction of databases and profiles had been carried out by states. In the inter-war period, the development of the modern *advertising* and *marketing* industries led to the improvement of methods of observation and analysis of consumer behavior in order to establish profiles aimed at public awareness, together with the increase in new technologies.

With the advancement of digitalization, monopolies based on commercial exploitation of personal data have been consolidated, generally based on the provision of free public services and the participation of people in social networks. The increase in the memory capacity of digital media, as well as the deterritorialization of processing, the automation of collection, the use of algorithms and the intersection and dissemination of data have enhanced the exploitation of people's data.

The contemporary panorama of centralization of the internet around large private corporations, highlighted by Mattelart and Vitalis (2015), is also considered by other researchers, such as Fiormonte and Sordi (2019), who recognize that Gafam – Google, Apple, Facebook, Amazon, Microsoft, all American corporations – have been dominating the different facets of the network on a planetary scale. Currently under pressure from China, they have been trying to extend their penetration through artificial intelligence and the internet of things that 5G will make possible.

In terms of regulation, when examining the milestones developed by the French state and establishing relations with others in the context of the European Union and the United States, Mattelart and Vitalis (2015) find an increasingly clear desynchronization between the rhythms of the computerization processes and the legal efforts to protect their abuses. Even so, the authors consider its symbolic importance, as they formalize and specify the rights of citizens over their information in a democratic society. They also highlight the strong distinctions between the American and European regulatory model in terms of protecting people's privacy. They reflect that regulation should intervene from the conception of these automatisms, a direction set by the *privacy by design* approach, which proposes to act in the design of materials, programs and architectures in order to guarantee respect for private life.

The perspective of Shoshana Zuboff (2018) helps to complement the examination of Mattelart and Vitalis (2015) in terms of the specificity of emerging capitalism in this process. The researcher understands that the emergence of a new logic of accumulation is underway, surveillance capitalism, which has been gradually constituted from the last decade of the 20th century with digitalization and its social penetration, enabling a persistent and continuous record of data that feed the emerging logic of capitalism.

The methods of producing data from the daily extraction of information and the ways in which they acquire value reflect other characteristics of this logic, based on formal indifference and the absence of structural reciprocities in the relationship of companies with their "users." People are the sources of data extraction and the ultimate targets of the actions that such data produce. The obscurity of these practices is another face of indifference. Another aspect of this process is the need to improve standards, which leads to continuous experiments.

Reconfigurations in power structures take place in this emerging logic. Power becomes linked to ownership of the means of behavioral modification. False conscience is also produced by the hidden facts of the commercialized modification of behavior. In this new form of power, the contract and the rule of law are put under scrutiny. In the view of Zuboff (2018), surveillance work does not lead to the corrosion of privacy rights, but to their redistribution. These rights are being concentrated on private and public surveillance actors. Thus, the logic of accumulation includes not only capital and surveillance assets, but also rights.

It is not possible to finalize the considerations on this axis of reflection without mentioning the recent scenario in which there is an intensification of its logics: the crisis triggered by the global expansion of covid-19, which convulses the set of social relations on the planet. In the context of the pandemic, the need for physical distance associated with the reorientation of activities towards the digital world has exponentially benefited corporations that have their business models based on the exploitation of people's data. In addition, several states have started to apply digital surveillance strategies in order to control the spread of the disease. South Korea, Singapore, China as well as Taiwan and Hong Kong have developed cyber-surveillance systems from smartphone applications with the purpose of digitally tracking citizens with the disease or who have been present in contagious areas. The model, based on the massive use of data and associated with video protection systems, has also been adopted in countries such as Germany, the United Kingdom, France and Spain. Data from mobile phone and internet providers

have been used by states to prevent the spread of the disease and monitor people infected. Internet giants Google and Apple have also partnered with the purpose of tracking those infected with the disease and have been developing technologies to alert people when they get close to someone who has tested positive for the new coronavirus. In this process, the risks of the possibility that the exception measures adopted may remain in the future are deepened, particularly those related to cyber surveillance and biocontrol (Ramonet, 2020).

THE NEW FORM OF GOVERNMENT INITIATED BY CYBER CONTROL

In the work we are examining, Mattelart and Vitalis (2015) reflect on the new form of government inaugurated by cyber control. To understand their specificities, they relate and distinguish this form of government with that constituted in disciplinary society. Based on Deleuze's reflections on the *control society*, researchers seek to draw distinctions that express the transition from one type of regime to another.

Disciplinary society, active for more than three centuries in Foucault's perspective (1975 cited by Mattelart & Vitalis, 2015) and established after the Renaissance, according to Elias (1973 cited by Mattelart & Vitalis, 2015), is characterized by inscribing the social normalization within the individual. It is marked by the visibility of its architecture and its disciplinary devices. This disciplinary visibility leads to behavior control. The subject participates in its normalization through self-restraint and self-control. In the cyber control society, technologies are generally characterized by invisibility and automation. Its effectiveness is even based on invisibility. The individual is apparently free, but is permanently watched. He/she is the object of information and, in the event of a deviant behavior, decisions are made and immediately applied.

The contemporary surveillance system is also marked by fluidity, mobility and connectivity, characteristics driven by communication and information technologies and networks. This digital environment facilitates communication, at the same time as it constitutes a scenario of permanent control. The contents can be transmitted instantly, stored and processed anywhere on the planet. In addition, control devices are now deterritorialized.

In these processes, a new form of government emerges based on prediction and, above all, on prevention of behaviors through the application of algorithms to massive amounts of data for the elaboration of profiles and structuring the field of possible actions of individuals. Its uses include risk reduction and

intervention through the automatic detection of abnormal behaviors before the criminal acts take place and the prediction of people's needs and desires based on the treatment of their data to perform consumption. This anticipatory bias and its immediacy are distinctive features of cyber-surveillance in relation to other forms of control. It is worth considering that, although a new form of government is established, this does not mean that the discipline does not continue to operate and that new information and communication technologies cannot even extend it.

In relation to this dimension of analysis, it is interesting to consider other contributions that converge with the discussion by Mattelart and Vitalis (2015) and bring elements that complement it. Feeding on Foucault's propositions[4], Silveira (2017) also conceives that, in the contemporary context, a new mode of government is inaugurated in which algorithms, such as technology, have a fundamental role. In his reflections, the researcher seeks to examine algorithms as a technology that has logos and is not neutral. As characteristics, the algorithms are "invisible, complex and written in mathematical language" (p. 272). They are produced within positivist rationality, articulated by neoliberalism, which reinforces the discourses of neutral technology. As a set of coded instructions for solving problems, expressing a computational solution related to logical conditions (knowledge about problems) from strategies aimed at solving them, the algorithms are developed, in general, within companies and corporations in the market and express the intentions of its creators. They embody original purposes, which can be changed by users and by the algorithms themselves if they contain self-correcting and learning encodings.

Silveira (2017) stresses the need to recover criticism and think about the public dimension and the political implications of the algorithms. They involve automating the data analysis and decision making processes. This second dimension entails risks for society. Its results are also not predictable in the case of those who have the capacity to learn or correct from the actions previously carried out, which gives these technologies decision autonomy difficult to estimate. Another characteristic is that they are performative devices; they can engender practices and procedures. This has implications that must be considered in several dimensions, such as in public sector decisions, in which "responsibility for acts of management, transparency and legal stability constitute fundamental issues" (p. 275).

[4] Silveira adopts the Foucauldian perspective of government that, in summary, involves "structuring the field of action of others" (Foucault, 1995, cited by Silveira, 2017, p. 270). Thus, the government includes the management of conducts, but expresses itself only as a confrontation, being constituted also through bonds.

It is worth mentioning, in relation to the risks that the algorithms may bring, those systematized by Doneda and Almeida (2018) from the examination of contemporary works: "manipulation, bias, censorship, social discrimination, violations of privacy and property rights, market power abuse, effects on cognitive abilities, in addition to growing heteronomy "(p. 145). In relation to this discussion, Fiormonte and Sordi (2019) help to think of algorithms as devices that produce personalization, a key element in the production of people's digital world experience. Personalization collaborates to keep subjects engaged in an experience of the networks that develops entirely within the limits drawn by the platform's algorithms. The algorithms also act in the control of time, instituting programmed obsolescence mainly in the scope of uses. Thus, such uses can be repeated at very short intervals, as the algorithms will always be able to organize and insert new content.

Fernanda Bruno (2008) also reflects on digital surveillance, which is understood by her as a process linked to "systematic, automated and remote monitoring of actions and information of individuals in cyberspace, in order to know and intervene in their possible behaviors or choices" (p. 11). The reflection on the nature of the profiles generated in this process is interesting for the discussion of cyber control. Data processing is no longer aimed at extracting regularities (averages) within a population to derive norms. The profile refers to patterns of occurrence of certain factors, trends and potential, not to a law. The author properly considers these taxonomies as *epistemic machines*.

Another interesting aspect is the reflection on these profiles as *identity machines*, which present specific modes of individualization. Profiles are simulations of identities, "both in the sense of anticipation and of modeling" (Bruno, 2008, p. 14). In contrast to disciplinary surveillance, which was based on models of descending individualization, digital control is characterized by "transversal or combinatorial individualization." This mode of individualization does not erase the previous one, rather overlaps it. The most connected, visible and participatory people in informational networks are more widely monitored. Profiles also configure identity effects insofar as they are predictive and act performatively.

POSSIBILITIES OF RESISTANCE AND SOCIAL CONTEST

The view of Mattelart and Vitalis (2015) does not fail to consider the contradictions, fissures and possibilities of resistance to cyber control. Researchers recognize the possibilities brought by new digital technologies to societies in

terms of generation and sharing of knowledge and information, accessibility to the conditions of content production, establishment of extended links, different experiments, the constitution of new movements and activisms, for reflection and aesthetic creation. They also consider the possibilities of building informational autonomy in the context of cyber control.

The mobilization of public opinion is an important element for questioning and promoting actions that allow the control of abuses by both governments and private institutions. They have recently been expanded through revelations about surveillance and espionage processes, such as those carried out by Snowden in July 2013 relatively to the clandestine Prism program, when he provided the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) with access to data from the telephone company Verizon and internet companies such as Microsoft, Yahoo, Google, Facebook, YouTube and Apple. Hackers, for their technical competence and their libertarian ideas, have been at the forefront of criticism and protest processes, with WikiLeaks being such an emblematic example.

In the *field of uses,* Mattelart and Vitalis (2015) discussed the possibilities for people to also access control tools used by controllers and become vigilant. They point out various ways of using technologies in the service of citizen surveillance to denounce the methods and forms of abuse of security guards. In everyday life, people with greater technical competence have greater possibilities to protect themselves from cyber control through the use of tools that preserve anonymity or encryption. They can also use disconnection practices or choose not to visit environments whose abusive practices are more widely known.

Regarding the dimension of the uses and digital appropriations made by people, David Lyon (2018) allows adding other aspects to this discussion. The researcher argues about the need to investigate what he calls a culture of surveillance in order to make the relationship between digital control and people in everyday life more clearly visible. The notion of surveillance culture, under construction by the researcher, alludes to the ways of life made up of subjects who experience digital surveillance. It includes thinking about the practices and meanings related to surveillance in digital environments, i.e., the understandings and ways of acting of the subjects in these contexts permeated by cyber control. Such a culture is multifaceted and varies according to countries, regions and a number of other factors. It is socially constructed, therefore, can be challenged and rebuilt, which opens the way in terms of building digital citizenship. In this sense, he would add that we should think of cyber surveillance cultures in the plural, given that it is constituted differently in terms of practices and social conceptions.

The perspective of thinking about cyber control from the uses and appropriations of subjects, groups and collectives is, in my view, a fundamental dimension of investigation, in connection with a broader problematization of such processes. To investigate this dimension, it is important to consider skills, practices and meanings related to surveillance in digital environments, i.e., understandings, knowledge and ways of acting in contexts permeated by cyber control. These relationships are complex and may include forms of reproduction, complicity, negotiation and/or resistance to cyber control in digital communicative practices.

Some investigations that I have supervised in recent years, which aimed at understanding appropriations of digital media by collectives and socio-communicational movements, have included issues related to cyber surveillance. This is the case of the PhD research conducted by Marina Albuquerque (2018), which investigated the uses of digital networks by two collectives linked to new urban socio-communicational movements in the city of Porto Alegre, Brazil. In relation to these issues, the survey, whose data were collected in 2016 and 2017, evidenced that the subjects interviewed were aware of aspects of digital surveillance, also because the digital information of members was used by the police to criminalize people in the collectives. However, the reflection on this issue had neither reached a broader space in collectives nor the development of more effective strategies and/or tactics to deal with cyber control.

Empirical explorations developed between 2018 and 2019 with members of collectives linked to the feminist movement in the Brazilian cities of Porto Alegre and Salvador, carried out by Bruna Lapa Guia, who is developing a doctoral thesis under my supervision, point out that the concern with cyber control was present in several of these scenarios, especially from the new Brazilian conjuncture linked to the Bolsonaro government, which started in 2019, and brought broader risks of criminalization to social movements. Faced with insecurity and the fear of state and civil surveillance on social networks, women have been debating alternatives, such as migration to safer applications, to alternative and free digital spaces. One of the collectives approached had been gradually replacing the operating systems of the supports used (such as computers and cell phones) for free software. Another measure taken was to turn off cell phones at meetings. In addition, another tactic, motivated by an apprehension in the face of the increasing possibility of criminalizing social movements, was to move away from technological means and invest in face-to-face communication, less subject to surveillance. This retraction in relation to technological uses was also linked to the perception that the messages sent

and shared in the digital environment did not always reach the women with whom the feminist movements intended to dialogue, due to access limitations and the algorithmic configurations of the internet.

***

In this text I recovered contributions from the work *De Orwell al cibercontrol*, by Armand Mattelart and André Vitalis (2015), to reflect about cyber control. They allowed us to dimension it as a historically situated phenomenon constituted from a process in which connections and breaking points, and other forms of social control could be seen. In this process, the devices were being tested, tried and renewed according to state, geopolitical and economic interests, as well as of their connections.

Another contribution of the work is related to the understanding of the specificities of this new modality of exercise of power and its distinctions with the disciplinary control that preceded it (although still operating in our societies). Cyber control is characterized by its invisibility, opacity, automation, because it is based on prediction and, above all, on the prevention of behaviors through the application of algorithms to massive amounts of data to build profiles and performation the field of possible actions of individuals.

The work also allows us to reflect on possibilities of resistance, contestation and regulation of cyber control. The examined contributions reveal contradictions in the field of regulations related to the aggressiveness of corporate strategies and the speed of technological innovations; they pay attention to the role of public opinion mobilization, particularly through the massive dissemination of facts associated with cyber control and the possibilities derived from the social appropriation of technologies from the knowledge of tools and citizen surveillance.

It is essential, from my point of view, to include the questioning of cyber control in contemporary research that deals with phenomena linked to digital communication. In this context, the work of these authors offers an effective and thought-provoking contribution, both for the richness of the research and the insights and for issues it opens up to the investigation. The work also offers important subsidies to deepen the training processes in the academic and social spheres on the logic of cyber control.

I signal two investigative demands provoked by the reflection of the work of Mattelart and Vitalis (2015). One is related to the need for communicational research to invest in understanding the specifics of this historical process and its contemporary nuances in the Brazilian and Latin American context. In a

convergent direction to this demand, Domenico Fiormonte and Paolo Sordi (2019) argue about the need for a critical history of control technologies that must take into account, among other elements, the place of the south in these processes. One of the dimensions to be considered is the material construction of the digital world: a large part of the natural resources that feed its constitution come from countries located in the south part of the world. In this scenario, the South takes the place of resource provider and data producer based on unpaid work. Thus, a new colonialism is established in the view of these researchers: data colonialism.

Another field that requires investigative effort is related to the processes of advancing cyber control in the context of the coronavirus pandemic. In this dimension, investments will be necessary to account for the different facets related to the deepening of cyber control during the pandemic and its future developments, in different dimensions such as those related to telework and tele-education.

These are some of the provocations that the work of Mattelart and Vitalis (2015) brings, a work that disturbs, instigates, challenges and invites to take on the scientific, ethical and political challenge of deepening the understanding of this complex and multifaceted phenomenon, in addition to collaborating to the production of resistance and alternatives to the perverse processes that cyber control engenders. M

REFERENCES

Albuquerque, M. Z. (2018). *Entre as redes sociais digitais e as ruas: Processos comunicacionais dos coletivos Defesa Pública da Alegria e Bloco de Lutas* [Tese de doutorado, Universidade do Vale do Rio dos Sinos]. Repositório Institucional da UNISINOS. http://bit.ly/38p7Yfh

Bruno, F. (2008). Monitoramento, classificação e controle nos dispositivos de vigilância digital. *Revista FAMECOS*, *15*(36), 10-16. https://doi.org/10.15448/1980-3729.2008.36.4410

Doneda, D., & Almeida, V. A. F. (2018). O que é governança de algoritmos? In F. Bruno, B. Cardoso, M. Kanashiro, L. Guilhon, & L. Melgaço (Orgs.), *Tecnopolíticas da vigilância: Perspectivas da margem* (pp. 141-148). Boitempo.

Fiormonte, D., & Sordi, P. (2019). Humanidades Digitales del Sur y GAFAM: Para una geopolítica del conocimiento digital. *Liinc em Revista*, *15*(1), 108-130. https://doi.org/10.18617/liinc.v15i1.4730

Lyon, D. (2018). Cultura da vigilância: Exposição e ética na modernidade digital. In F. Bruno, B. Cardoso, M. Kanashiro, L. Guilhon, & L. Melgaço (Orgs.), *Tecnopolíticas da vigilância: Perspectivas da margem* (pp. 151-179). Boitempo.

Maldonado, A. E. (2015). *Epistemología de la comunicación: Análisis de la vertiente Mattelart en América Latina*. Ciespal.

Mattelart, A., & Vitalis, A. (2015). *De Orwell al cibercontrol*. Gedisa.

Silveira, S. A. (2017). Governo dos algoritmos. *Revista de Políticas Públicas*, *21*(1), 267-281. http://dx.doi.org/10.18764/2178-2865.v21n1p267-281

Ramonet, I. (2020, 30 de abril). Ante lo desconocido la pandemia y el sistema-mundo. *Le Monde Diplomatique*. http://bit.ly/34wJeRi

Zuboff, S. (2018). Big other: Capitalismo de vigilância e perspectivas para uma civilização da informação. In F. Bruno, B. Cardoso, M. Kanashiro, L. Guilhon, & L. Melgaço (Orgs.), *Tecnopolíticas da vigilância: Perspectivas da margem* (pp. 17-68). Boitempo.

Article received on September 30 and approved on December 15, 2020.