On the security discourse at the basis of surveillance practices

Sobre el discurso de seguridad que subyace las prácticas de vigilancia

Eline Marx[1]
Paris School of International Affairs. Paris, France
elinevmarx@gmail.com
ORCID: 0000-0002-7472-4066

Citar como: Marx, E. (2023). On the security discourse at the basis of surveillance practices. Desde el Sur, 15(3), e0045.

ABSTRACT

This essay wishes to expose and dismantle the ontological and political premises giving its ground to contemporary surveillance practices. It argues that surveillance policies and technologies are not abuses, but rather the continuation of Western political theory and practice which has always been apprehended as a security project establishing social classes to secure and others to be protected from. Surveillance practices pretend to protect our lives from insecurity on the streets, terrorism or a virus, while they actually conspire against our individual and collective autonomy, define norms of legal and illegal behavior, criminalize precarious social groups, make terrorist networks harder to identify, create an over-expanding market for risk assessment companies and national states, undermine claims for social justice and colonize the public sphere with war language. The essay denounces how the security project led together by public and private actors is thus one of securing a lucrative business for the powerful and an exploitative social order for the powerless. It suggests a few paths to counter the discourse at its basis.

[1] Eline Marx es escritora y cineasta. Tiene un posgrado en Ciencias Políticas de la Paris School of International Affairs.

KEYWORDS

Surveillance, risk, terrorism, COVID-19, society of control

RESUMEN

El ensayo propone exponer y desmantelar las premisas ontológicas y políticas que dan pie a las prácticas de vigilancia contemporáneas. Argumenta que las políticas y las tecnologías de vigilancia no son abusos sino la continuación de la teoría y práctica política occidental siempre pensada como un proyecto de seguridad estableciendo clases sociales para proteger y otras de las que protegerse. Mientras pretenden proteger nuestras vidas de la inseguridad en las calles, del terrorismo o de un virus, las prácticas de vigilancia maquinan en contra de nuestra autonomía individual y colectiva, definen normas de comportamientos lícitos e ilícitos, criminalizan a grupos sociales precarios, dificultan la identificación de las redes terroristas, crean un mercado en expansión para las empresas de evaluación de riesgos y los estados nacionales, debilitan las reivindicaciones de justicia social y colonizan la esfera pública con un lenguaje bélico. El ensayo denuncia que el proyecto de seguridad liderado en conjunto por personas públicas y privadas se encarga de asegurar un negocio lucrativo para quienes ostentan el poder y un orden social explotador para quienes han sido desposeídas. Sugiere algunos caminos para oponer el discurso en su fundamento.

PALABRAS CLAVE

Vigilancia, riesgo, terrorismo, COVID-19, sociedad de control

Introduction

The destruction of the World Trade Center on September 2001, claimed by the terrorist group Al-Qaïda, was understood by the United-States government as a declaration of war. The narrative of a permanent and unusual threat gave the National Security Agency (NSA) the support they needed within the government to standardize and systematize otherwise controversial surveillance practices formerly established within the office.

Nineteen years later, the COVID-19 pandemic —also introduced in war terms— further legitimized, normalized and extended surveillance practices, making real Félix Guattari's dystopian vision of «a city where one would be able to leave one's apartment, one's street, one's neighborhood, thanks to one (dividual) electronic card that raises a given barrier; but the card could just as easily be rejected on a given day or between certain hours; what counts is not the barrier but the computer that tracks each person's position —licit or illicit— and effects a universal modulation» (Deleuze, 1990, p. 7).

Contemporary surveillance practices are driven by a discourse on security and risk which preexisted, but spread dramatically with 9/11 and the COVID-19 pandemic. According to this specific discourse, risk is understood as any event, potentially predictable, that might threaten the biological existence and the capitalist market. Contemporary surveillance practices are a set of technologies gathering computerized information on individuals —data and biometric information— sorting people by the reduction of complex identities to risk assessments. These techniques, thought of as mathematical and thus neutral, stabilize a socially unjust, racist and classist status —deepening necropolitics— while in the meantime make political accountability more volatile.

Contemporary surveillance practices have transformed global politics theory and practice. First of all, the emphasis shifted from sentencing crime based on evidence to preventing crime based on suspicious behavior, considered calculable through complex algorithms and data mining. Secondly, contemporary surveillance practices have blurred the boundaries between public governance and private industry by simultaneously involving governments, international institutions and private corporations. Finally, the idea that the danger might be inside the state bringed realpolitik within national borders and justified government surveillance of their own residents. Even more so, the idea that the danger might be inside the people themselves transformed the citizens into their own benevolent police, painfully eroding the social fabric.

In a liberal paradigm, one could argue that mass surveillance breaks the social contract between the state and the citizens that gives its legitimacy to the first one and is based on common trust. However, I argue that contemporary surveillance practices are the logical development of Western political thought that has always been apprehended as a security project. Thus, we are taught that states are built to ensure the survival of human beings and enable the creation and application of their rights, that is to say, their existence as political subjects. Nations are constructed on a dynamic of inclusion —the citizen— and exclusion —the alien— and so is its security premise which implies that there are people to secure and others from which to be protected from.

Thus, risk doesn't exist as an objective reality. It is a knowledge-power: a language that produces a reality and affects human agency. «It is not a noun that names something, it is a principle of formation that does things» (Dillon, 1996, p. 16). The will for security, by creating an Other, is inherently violent, and is also destined to failure and endless replication, because more security reveals new insecurities, because human action can never be grasped by mathematical estimations and because the mortal nature of our beings cannot be overcome.

To subvert the security discourse that drives contemporary surveillance practices, it is necessary to expose its various implications. First of all, the concept of risk is a political construct. It is the product of economic historic disruptions and is also creative of an History since it is used by decision-makers as a guide for action. The security discourse produces a reality. As Dillon notes, «we are not only users of language, we are used [...] by the language we use» (Dillon, 1996, p.16). I develop how contemporary surveillance practices, embedded in the security discourse, foster social sorting and exclusion; blur the boundaries between public governance and private expertise; are the opportunity for a fructifying liberal market; impose the dividing social reality it creates on people's everyday lives; justify the militarization of the public space and legitimize the nation-state.

In a second time, I critically discuss the fact that contemporary surveillance practices have been and are mainly addressed as issues of privacy. I argue that the security discourse abuses are constitutional of its very nature and that what is needed is, instead of a debate around its potential limitations, a deconstruction of its theoretical premises. Following Ulrich Beck's thought on the backlashes modernity brings (Beck, 2009, p.13), I stress that the security discourse produces a worldwide increase in violence.

A history of the political construct of risk

The notion of risk is grounded in time and space. In pre-industrial societies, uncertainty was part of a cosmology based on Providence: human control over its destiny was thought to be limited. From around the seventeenth century in the West, the emergence of a capitalist economic system revolutionized the conception of time: putting profits at stake on the market led to the implementation of systems of insurances and thus required the conception of a future under the realm of human action. This idea of a future not predetermined by God but malleable by human agency was summarized in the concept of risk: an event that might happen, depending on what is done in the present. Based on a linear conception of the world as relations of cause and effect, estimations about the future were thought possible based on the analysis of global trends of the past. Knowledge would thus make the universe more predictable and increase the control humankind can have over its destiny. However, the twentieth century scientific discoveries of the relativity of time and space, the disillusionment over absolute knowledge and the growing complexity of a globalized world portrayed an indeterminate and non-linear future. The notion of risk was then defined as a calculation of uncertainty, embodied by the notion of probability.

Thus, risk is considered to be a guide for action in the present in order to tame the unpredictability of the future. Risk management cannot prevent an event from happening but it provides the argument that the action was otherwise undertaken following the risk assessment: it «immunizes decision-making against failure» (Luhmann, 1993, p. 13). During the 2017 French presidential campaign, far-right candidate Marine Le Pen claimed that none of the 2015 terrorist attacks in France would have happened if she had been President at the time because she «would have taken all the necessary measures to avoid it». Likewise, the US government and risk specialists perceived the 9/11 terrorist attack as a risk management issue that could have been intercepted by integrated contemporary surveillance technologies. Any decision, hence any life aspect can fall into the security discourse: the very nature of the risk approach is to act on something that has not yet happened. Locked within technology and automatized within contemporary surveillance practices, the security discourse assumes that the tracking of suspicious behavior can prevent criminal events. It presents surveillance practices as necessary and makes them possible this way. «Software installs relatively unchangeable, taken-for-granted protocols in the day-to-day information practices of organizations, providing unified ways of interpreting events, influencing the ways in which decisions are made and standardizing such decisions over time and space» (Leyshon and Thrift, 1999, p. 453). The fictitious future, through the mechanisms of the security discourse, becomes the present. The gap between the present and the future is destroyed; the future becomes an extended present. Its commitment to secure the human body threatens the ontological existence of the self, in need of a dynamic projection into the future in order to build its identity; as well as the essence of politics, which presupposes the uncertainty of the future as a condition for decision and action.

Algorithms are based on classist and racist assumptions

What is considered a threat is an historical, and thus political, construct. However, the inscription of the security discourse in the algorithms developed by contemporary surveillance practices gives it an appearance of objectivity and neutrality. The technologies analyzing biometric information, personal data and financial transactions in order to profile people are built on a premise of what is normal or abnormal, what is legitimate or suspect, what is legal or illegal. Thus, profiling has focused and therefore criminalized specific characteristics and behaviors. For example, the surveillance practices implemented to trace terrorist funding have qualified irregular money activities as suspect. Yet, this concerns mostly unemployed individuals, students and immigrants. The close surveillance of hawala payments in the Middle East after 9/11 led the Bush administration to freeze the money remitter al-Barakaat, considered suspicious for banking voluminous amounts of cash and transferring this money from the US-based Somali diaspora to Somalia. The impossibility for the bank to deliver the money to its recipients had harmful consequences on the Somali community, while the 9/11 Commission found no links between the remitter bank and terrorist networks. According to the Commission, the fact that the authorities deduced a fraud based on the amount of cash money transferred is based on classist and racist assumptions on migrants. Thus, contemporary surveillance practices, providing data for risk assessments, «operate by abstracting human bodies from their territorial settings, and separating them into a series of discrete flows. These flows are then reassembled in different locations as discrete and virtual "data doubles"» (Haggerty and Ericson, 2003, p. 606). Hence, the intertwining of data analysis furnished by surveillance technologies and preexisting assumptions made by the designers of risk mathematical formulas construct chimerical identities. For example, the United-States Visitor and Immigrant Status Indicator Technology (US VISIT) is a program based on the sorting of legitimate travelers for touristic or business purposes and illegitimate travelers such as terrorists. Thus, «the coded body of a person who attempts to cross a national border may find that she is already welcome or already excluded on the basis of an identity that is established by the codes» (Lyon, 2003, p. 24). US VISIT opens its national borders to Mexican workers, but its vocation to track «risky profiles» beyond the entrance on the national territory leads to the intensification of the surveillance they experience within the country and to the actual displacement of the border to the very aspects of their lives such as the possibility to access housing, healthcare and banking, weakening further the already most precarious social groups. Similarly, Arab and Muslim people are disproportionately targeted by contemporary surveillance practices. For example, the Federal Bureau of Investigation (FBI) has kept on file Arab students of more than two hundred United-States universities'. Contemporary surveillance practices produce categories of insiders and outsiders based on what are considered licit and illicit behaviors that actually have the effect of a double penalty, criminalizing already discriminated groups. In a way, surveillance defines new social classes, while hiding its logic of classification in nontransparent practices. Yet, the power to classify is a power over the meaning of the social world.

Growing the market, stifling democracy

Contemporary surveillance practices are profoundly antidemocratic because they are based on the collaboration of governmental bodies and private entities that allows risk management firms to impact the lives of the people in broad and concealed ways. The Department for Homeland Security (DHS) bought the US VISIT project from the consulting company Accenture for US$ 10 billion. Thus, Accenture is directly responsible for the construction of information networks about individuals that conducts visa delivering or refusing. Similarly, the British risk management company Mantras and World-Check sells operating systems built to detect irregular money flows to financial institutions. The perspective of an integrated, unified and standardized system of surveillance practices may give the incentive to an increasing number of state agencies and multinationals to sell and buy the computerized information and the new algorithms. Handing the control of people's movements to private agencies depoliticize surveillance practices and legitimize them on the basis of the firms' technical expertise. Governance is removed from the ethical paradigm and placed instead in the realm of management and efficiency.

Obviously, contemporary surveillance practices foster the development of an expanding market and produce new financial directives to international institutions such as the United Nations (UN) and the International Monetary Fund (IMF) devised to fight terrorist funding while ensuring, by its non interference, the deregulation of these markets and of trade. Moreover, the risk approach generated by the security discourse is productive because it is endless: the imagination of an event that might happen can expand without ever being stopped by the actual happening of this event, because the very nature of the notion demands that action has to be taken preemptively. Thus, it is a vicious circle with a principle of self-amplification, because it assumes that more knowledge can prevent more risks while the surplus of knowledge, paradoxically, creates new possibilities of risk, and indefinitely.

The security discourse that drives contemporary surveillance practices affects our social lives in many aspects, reaching beyond the realm of security. Thus, it creates an atmosphere of general fear and suspicion that makes each individual responsible for the risk management of his everyday existence. In the subways of capitals such as London, Paris or New York for example, passengers are encouraged by automatic and repetitive messages to report to the police «any suspicious package or behavior». People are incited to internalize the notion of a constant threat and are impelled to take responsibility for it. Amsterdam's Schiphol airport implemented the Privium membership card program exclusively reserved to European-Union citizens, authorizing them to avoid the usual waiting line at customs in exchange of granting their biometric data to the authorities and paying US$145 annually. Common individuals become active actors in the security discourse and participate in the social sorting it performs. Social control, with contemporary surveillance practices, is a form of biopower defining and organizing the boundaries of a legitimate and illegitimate world. On one hand, it promises even more comfort to the wealthier, mainly through segregation (the Privium membership, besides granting shorter waiting times on security check, also includes access to priority parking, business class check-in and exclusive VIP lounges), while it literally publicizes a death threat on the deviants, delegating police power to vigilantes. On May 1st 2023, Daniel Penny, a 24-year-old white veteran of the Marine Corps, choked to death Jordan Neely, a 30-year-old homeless black dancer who was yelling for food and water in the New York subway in what the press has called a psychotic break. Daniel Penny was assisted by several passengers while the majority remained still or stepped aside. Some filmed the murder. Penny was arrested and released a few hours later without charges. While witnesses have said that Penny grabbed Neely from behind, Penny's lawyer firm stated that «Daniel never intended to harm Mr. Neely [...]. When Mr. Neely began aggressively threatening Daniel Penny and the other passengers, Daniel, with the help of others, acted to protect themselves.» «I feel sorry for the man» commented Maria Castaño, a 64 years-old interior designer interviewed by the New York Times on the subway, «but he was acting threatening». «Acting threatening», in this case desperately asking for solidarity to fulfill basic needs, is now liable to death (Cramer, Meko and Nierenberg, 2023).

Bringing the war home and the frontier within the body

The emphasis on the existence of a permanent risk and the colonization of the public sphere with war langage gives grounds for the implementation of legislations and surveillance practices where the state of exception becomes the rule. Such control becomes generalized and unlimited. In France, the state of urgency, which lasted from 2015 until 2017, justified the deployment of the army within the national borders and the expansion of the mandates of the police and the secret services. The supposedly exceptional measures put in place in the context of the state of urgency have been used in France during the 2016 spring to repress the growing social movement against the new work law and to survey its reporters. They were then turned into the law 2017-1510 «reinforcing homeland security and the fight against terrorism» (JORF, 2017).

The security discourse that drives contemporary surveillance practices revives the legitimacy of the nation-state, which stands on a security promise. It is significant in this manner that all the candidates of the American and French 2017 presidential campaigns positioned themselves according to the fight against terrorism and praised the advantages of their own prevention methods to secure the country. The security discourse that drives contemporary surveillance practices defines a «we» and a «them» based on the nation-state paradigm. The security project points out who the «we» is and who the «we» is not ; who constitutes the «we» and who the «we» has to be suspicious of and fear. The terrorist attacks in 2001 in the US and in 2015 in France have been interpreted as an offense to the nation and its specific symbols. As Ulrich Beck writes, «[t]he risks which we believe we recognize and which fill us with fears are mirror images of ourselves, of our cultural perceptions» (Beck, 2007, p. 13). Thus, the hierarchies built by the security discourse constantly threaten the «suspicious» individual to become a foreigner in its own country. Fear assigns spaces of power and secures them as political order, while undermining the possibilities for contestation by surrounding the social world with its mark of urgency.

Behind the myth of the neutrality of algorithms

The algorithms, made out of big data recollection, are presented as mere objective, mathematical and neutral reflections of the social world rather than themselves makers of a specific reality. «The «harmlessness» of algorithmic governance is barely apparent, it creates reality at the same time that it records it» (Rouvroy and Berns, 2015, p. 48).

Many examples have shown that algorithms reproduce, and even potentiate, inequalities, while at the same time the discourse presenting them as neutral because based on hard sciences —and sometimes framed as more reliable and effective than human beings' decisional process— veils their discriminatory effects and removes responsibilities. In December 2020, the Ordinary Court of Bologna sanctioned the corporation Deliveroo for using a discriminatory algorithm violating the fundamental rights of its workers. The magistrate analyzed the internal design of the algorithm, which appeared to automatically penalize workers who would previously cancel the work hours they were assigned, without taking into account any motives. While the company affirmed not wanting to know the individual motives for cancellation, the Court asserted that it was exactly that blindness which was problematic because «it necessarily implies reserving the same treatment for different situations, which is what indirect discrimination typically consists». The judgment of the Court confronted the claimed neutrality of the algorithm, revealing the fact that it prevents the exercise of the fundamental right to strike and that of other work rights.

In the end, the security discourse and the surveillance practices aim at taming bodies and minds for the benefit of an unbridled capitalist market. It might not necessarily be about making Artificial Intelligence more human, but rather about making humans more machines : faster, more efficients, with no rights, virtually monitored, deprived of their capacity to empathize and collectively organize.

Advocating for the right to privacy against surveillance is limited

Activism in the face of contemporary surveillance practices has been generally struggling in the name of individual liberties such as privacy. Surveillance systems are understood as a governmental invasion of the civil private sphere'. Privacy International, for example, defines mass surveillance as the indiscriminate collecting of data on individuals and emphasizes the unprecedented power-imbalance which access to private information on people gives to the state in their control of public opinion. Similarly, Electronic Privacy Information Center (EPIC) in the US provides material for privacy litigation and advocates, among other things, for the protection of the consumer right to privacy against the selling of data to private companies. The Japanese Network Against Surveillance Technology (NAST) was born in 2002 to protest against the legal validation of a computerized inhabitants register. Statewatch, in Europe, documents the implementation of new surveillance practices. The discriminatory effects of the profiling made by contemporary surveillance practices have also been pointed out, however with little success. In 2004 in the US, for example, the American-Arab Anti-Discrimination Committee, the American Civil Liberties Union, National Immigration Law Center and Electronic Privacy Information Center addressed to the DHS their concerns about the human rights violations the US VISIT program could cause.

Nevertheless, these Non-Governmental Organizations (NGO) campaign against the abuses of power perpetrated by the governments and the business entities and not against the rationale that drives their actions and their so-called excesses. Accusing the abuses signifies that the premise is otherwise agreed on. Thus, it naturalizes the security discourse, giving it an aspect of necessity. It has also resulted simply inefficient in countering surveillance practices. In March 2020, eight phone companies provided the location data of their users to the European Commission to monitor the spread of the COVID-19 pandemic. To the various sectors that expressed concerns on the matter, the European Data Protection Supervisor Wojciech Rafał Wiwioroksk responded that «anonymous data fall outside the legal framework of data protection rules.» Understanding contemporary surveillance practices as a threat to the right to privacy fictitiously isolate individuals from the webs of meanings of the social world and the hierarchies and prejudice that are at play. It depoliticizes the language used by the security discourse : the creation of its classifications and the roles, or positioning, granted to the people that are supposed to fill in these categories.

In 2014, Facebook was able to secretly manipulate the data of 700 000 accounts to conduct experiments on the emotions of the users according to their social media reads. «It might be legal, but is it ethical?» wrote The Atlantic («Even the Editor of Facebook's Mood Study Thought It Was Creepy», June 28, 2014). Beyond the fact that big data seems to enjoy an immanent legality, it is evident that what is threatened are not the whereabouts of John Doe, supposedly protected by the right to privacy, but rather our autonomy, independence, dignity and integrity as historical and social beings.

Understanding contemporary surveillance practices as a threat to privacy silences the fact that the information is amassed in order to sort people on the basis of archetypes of identities constructed on racial, religious and social characteristics. It is primarily a practice taking its meaning in a social setting rather than in an artificial private sphere. Certainly, the security discourse is difficult to unveil because of its vast and expansive nature, its appropriation of language and thus its colonization of thought. Moreover, the competition for funding and the need for quick public support NGOs face spur them to follow commercial principles such as simplifying their messages and focusing on one aspect of otherwise complex issues.

However, the right to privacy emanates from a liberal conception of the state and the civil society. It presumes the existence of the state and the citizens as two interrelated, but separate, spheres. According to this paradigm, the function of the state, and thus legitimacy, is to enable and secure the individual private realm'. In this way, security, guaranteed by the state, is thought as the ground for freedom and the possibility for politics. In other words, the defense of the right to privacy as well as the security discourse that drives contemporary surveillance practices consider the security of the individual the condition for political freedom. Thus, questioning the respect of the right to privacy is assessing the competency of the state to accomplish its fundamental security promise. The surveillance practices of the state are not abuses or dysfunctions but the logical expression of its essence.

To counter the security discourse

The security discourse is about imagining a specific future that might happen and bringing it into the present by taking action in the now in view of what is thought to arise later. Subverting the security discourse can thus consist in contesting this imaginary future it proposes. In the 1980s, global activism against nuclear weapons confronted the security discourse by raising awareness on its paradoxical nature. Anti-nuclear weapon global activists gathered information about the powerful destructive effects of the nuclear bomb and showed that, instead of increasing US national security, nuclear weapons actually endangered the entire world. They deconstructed the government discourse about the secured future the bomb was supposed to provide to the country and instead stressed the dramatic (no-)future the bomb would cause, making thus appear that nuclear weapons should be prohibited in the now. This form of activism presupposed that the public was unaware of the implications of the nuclear bomb and that his support for such policies would fall with better information. Challenging the security discourse could focus on exposing to the public eye its prejudicial biases while also emphasizing on its very inefficiency to resolve terrorism. For example, Coutin, Amoore and De Goede demonstrated that the presupposed legal and illegal worlds contemporary surveillance practices claim to identify and assort are actually highly intertwined. Criminality is not a characteristic of the migrant, the poor or the undocumented but diverse and ambiguous types of profiles are implicated in money laundering and terrorist funding. Furthermore, the informal economy contemporary surveillance practices target as suspicious is more often the product of the labor market lack of regulation and the precarity it exploits than criminality. However, the scandalous aspects of the National Security Agency (NSA) mass surveillance recently revealed to the public by Edward Snowden didn't lead to much social change because public opinion still seems to think freedom can be exchanged against security and that security is required in order to access freedom. Consequently, resisting contemporary surveillance practices implies deconstructing centuries of Western political thought.

Final considerations

In a way, the myth of total security by the means of technology has replaced the myth of total knowledge. «Isn't our need for knowledge precisely this need for the familiar, the will to uncover under everything strange, unusual, and questionable, something that no longer disturbs us? Is it not the instinct of fear that bids us to know?», asks Dillon (Dillon, 1996, p. 17). As stated above, the philosophers of the European Enlightenment thought that more knowledge would lead to a better understanding of the world and thus enlarge human control over its environment. Similarly, contemporary surveillance practices are a project of control over the social world. Contemporary surveillance practices undercut the individual in risk assessments and allocate simplified meanings to otherwise dynamic identities. The security discourse reduces humanity to «an index of calculation» (Dillon, 1996, p. 26) in a desperate attempt to tame the uncertainty of the future that relates to the unknown possibilities of humankind. It reduces our existence to a biological status and profoundly threatens any wish of social and political emancipation. Contemporary surveillance practices obliterate the question of living together by creating a concept of exclusion, which undoubtedly produces more violence in return. The language of the security discourse naturalizes an unjust political order and the context of fear that it shapes closes the possibilities for debate. It secures an infinite present and prevents discussion of the choice of the future, which finally requires questioning the model of society the people want to build in the present. Moreover, the embedding of the security discourse in technologies and the secrecy in which the classification and the sorting take place makes accountability even harder to obtain.

According to Ulrich Beck, the risks our societies currently experience are not side effects of its development but the successful outcome of it. «Climate change, for example, is a product of successful industrialization which systematically disregards its consequences for nature and humanity» (Beck, 2009, p. 8). Applying this thought to our subject, we could argue that terrorism is the successful result of war and imperialism and that the security discourse and its practices are nothing more than the continuation of this violent rationale ; and that the COVID-19 is the successful result of brutal capitalism (environmental damage) and colonial neoliberal politics (collapsing of the public services). Respectively, it will likely continue to spawn hostility and we are likely entering an era of repeated natural catastrophes. What is prevented is the disruption of the social order as it is. In this uncertain world, social classes are automatized and essentialized through risk discourses and surveillance practices, fixing unsurpassable identities and their systems of inequalities into an extended present.

Government bodies, public actors of the national political scenes, international institutions and private companies have no incentive to end terrorism: the designation of terror defines them alternatively as the civilized world and promises a flourishing industry. As for the COVID-19, the different winners and losers might be harder to identify for now, but according to Oxfam, the fortunes of the billionaires have increased more between March 2020 and October 2021 than in an entire decade, while the incomes of 99% of the world population have shrinked (Oxfam, 2022).

Subverting contemporary surveillance practices requires one to question what the security discourse wishes to secure and what society this mode of security offers to build. The security discourse and risk assessments are constructed on a binary distinction of normal or abnormal, brother or barbarian. Acting as a mirror of the hierarchies of our modern societies, it removes people from their backgrounds and histories to place them in racist and classist categories of legality or criminality. This process secures the political order by guaranteeing the legitimacy of the powerful and the illegitimacy of the powerless. As Amoore and De Goede exposed, the actions taken by governments and international institutions against informal economy because of consequent suspicions of terrorist funding is likely to further impoverish precarious social groups and create instead more dissimulated forms of economy. On the contrary, if exploited workers were offered accessible and affordable banking solutions, terrorist finance networks could be more easily located.

At the opposite of the security discourse and contemporary surveillance practices is an understanding that no political order is fixed and that the political organization is a fight and a negotiation over language, the meaning of history and the social reality we decide to believe in and make happen. Political emancipation is about admitting the very unknown possibilities of humankind; it is about accepting that individual existence cannot be secured and that our living together, instead, should be open to reimagination.

Contribución de autoría

Eline Marx fue la única autora.

Fuente de financiamiento

Autofinanciado.

Potenciales conflictos de interés

Ninguno.

BIBLIOGRAPHICAL REFERENCES

Amoore, L. and De Goede, M. (April 2005). Governance, risk and dataveillance in the war on terror. *Crime Law and Social Change*, 43, 149-173. https://link.springer.com/article/10.1007/s10611-005-1717-8

Baylos, A. (2021). El algoritmo no es neutral. No permite ejercer derechos fundamentales a los trabajadores de las plataformas. *La Defensa*. https://www.ladefensa.com.ar/La%20Defensa%2051/el-algoritmo-no-es-neutral..html

Beck, U. (2007), Beyond class and nation: reframing social inequalities in a globalizing world. *The British Journal of Sociology*, *58*(4), 679-705. https://doi.org/10.1111/j.1468-4446.2007.00171.x

Beck, U. (2009). World at risk. Polity.

Calvo, P. (2019). Democracia algorítmica: consideraciones éticas sobre la datafıcación de la esfera pública. *Revista del CLAD Reforma y Democracia*, *74*. https://www.redalyc.org/journal/3575/357560862001/html/

Cramer, M., Meko, H. y Nierenberg, A. (2023). What we know about Jordan Neely's killing. *The New York Times*. https://www.nytimes.com/2023/05/05/nyregion/jordan-neely-chokehold-death-subway.html

Deleuze, G. (1990). Post-scriptum sobre las sociedades de control. *Polis. Revista Latinoamericana*, *13*(2006). https://journals.openedition.org/polis/5509

Dillon, J. M. (1996). *Politics of security. Towards a political philosophy of continental thought*. Routledge.

France 24. (2022). Selon Oxfam, la fortune des dix milliardaires les plus riches a doublé avec le Covid-19. https://www.france24.com/fr/%C3%A9co-tech/20220117-selon-oxfam-la-fortune-des-dix-milliardaires-les-plus-riches-a-doubl%C3%A9-avec-le-covid-19

Gendler, M. A. (2016). Datos, algoritmos, neutralidad de la red y sociedades de control. IV Simposio Internacional LAVITS. Buenos Aires. https://lavits.org/wp-content/uploads/2017/08/P4_Gendler.pdf

Hernández Arteaga, L. (2018). Niklas Luhmann, ¿una teoría sistémica de la democracia? *Estudios Políticos* (México), (43), 11-34. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-16162018000100011&lng=es&tlng=es.

Huanca-Arohuanca, J. y Barria-Asenjo, N. (2022). Replanteando el concepto de justicia como equidad y velo de ignorancia en John Rawls desde el pluralismo ético. *Desde el Sur*, *14*(3), e0036. http://www.scielo.org.pe/pdf/des/v14n3/2415-0959-des-14-03-e0036.pdf

Journal Officiel de la République Française, JORF. (31 octobre 2017). LOI n.° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (1). JORF n.° 0255. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035932811/

LaFrance, A. (2014). Even the editor of Facebook’s mood study thought it was creepy. *The Atlantic*. https://www.theatlantic.com/technology/archive/2014/06/even-the-editor-of-facebooks-mood-study-thought-it-was-creepy/373649/

Masdeu, J. (2020). Rastreados por el móvil para frenar al coronavirus. *La Vanguardia*. https://www.lavanguardia.com/vida/20200327/48109834703/coronavirus-tecnologia-rastreo-movil-telecomunicaciones-datos.html

Mora, R. (2021). Pandemia global, crisis económica y política. *Desde el Sur*, *13*(1), e0007. http://www.scielo.org.pe/pdf/des/v13n1/2415-0959-des-13-01-e0011.pdf

Oxfam. (2022). *Les inégalités tuent*. https://www.oxfamfrance.org/wp-content/uploads/2022/01/Rapport_Oxfam_Inegalites_mondiales_Davos_170122.pdf

Schiphol Privium. Website. https://www.schiphol.nl/en/privium/

Teknautas (2014). Facebook manipuló 700.000 cuentas de sus usuarios para un experimento. *El Confidencial*. https://www.elconfidencial.com/tecnologia/2014-06-30/facebook-manipulo-700-000-cuentas-de-sus-usuarios-para-un-experimento_154343/

Recepción: 29/12/2022
Aceptación: 18/4/2023