Surveillance Culture and Fundamental Rights: The Excluded and the Beneficiaries

Camila Costa, Federal University of Rio de Janeiro (Brazil)
Jonas FerrigoloMelo, University of Porto (Portugal)

Keywords: Surveillance culture, privacy ,fundamental rights, information ethics

ABSTRACT

Surveillance has progressively grown in social life in the 20th and 21st centuries. It happened partly because of the adoption of multiple sensors that can extract, collect and analyze an enormous volume of data. This expressive data volume, variety, and processing velocity are known as big data. The increasing adoption of big data and models based on algorithmic intelligence has a massive impact on society because of its dissemination among social spheres through relations between the public and private sectors. This paper aims to discuss surveillance culture and its consequences on fundamental rights such as privacy and freedom of speech. In addition, it is intended to debate the excluded and the beneficiaries of a surveillance society. The methodological approach is the literature review. The conclusion relies on the need for intercultural ethics to strengthen the right to privacy to guarantee not only itself but multiple fundamental rights nowadays.

Introduction

Surveillance tools have raised the concern of authorities and civil society in several cities around the world about privacy rights. Monitoring and surveillance systems have challenged the fundamental right to privacy because they depend on the use and massive extraction of data representing social dynamics (Aguirre et al., 2019).

David Lyon (2019) argues that surveillance capitalism is operated in a data-dependent surveillance culture that works in different ways and has several consequences. For the author, surveillance capitalism is the source that enables surveillance culture and vice versa.

According to Shoshana Zubboff (2021), surveillance capitalism has three dimensions: i) exploitation of data sources that record everything in every way; ii) data extraction, a single-direction process with no structural relationship or responsibilities but dependent on subjective signals; and iii) analysis that means that material technique replaces spiritual authority. Surveillance culture relates, on the one hand, to everyday experiences of surveillance, where individuals live with cameras in public and private spaces, in airports, buildings, vehicles, and other places. All these devices collect, store, transmit, and analyze data. On the other hand, surveillance culture resides in more active practices by individuals using search engines or, more likely, through social media.

Surveillance has emerged as a form of control by governments, businesses, and individuals, especially in public security. It has become a central component of modernity (Lyon, 2007). Fernanda Bruno (2009, pp. 1–2) understands surveillance as "the activity of systematic and focused observation of individuals, populations, or information about them, to extract knowledge and intervene on them to govern their conduct or subjectivities". The basis of this is a triple regime of legitimation: security, media visibility, and efficiency, especially regarding

network services and communication technologies. In the context of mass surveillance, all individuals become suspects until proven innocent, turning the whole society into vigilantes and potential suspects (Bruno, 2009).

Frank Pasquale (2015) argues that an incomprehensible surveillance state is as much a threat to freedom as fear of insecurity or terrorism. The author's critique goes on to state that those who watch over them have the power to classify critics of the system as enemies of the state, observing them even more. As such, the prominent harm of mass surveillance is its ability to silence dissenting voices (Čas et al., 2017; Oliveira, 2021; Pasquale, 2015; Solove, 2008; Véliz, 2021).

It is now much easier to collect data with less effort due to the difficulty in complying with the law and the ever-lower costs for storage and thus makes it is better to keep as much data as possible rather than discard it. In a world where surveillance is the norm, the very fact that it exists indicates the presence of structures and systems that are part of many spheres of society's life.

Behind confidentiality agreements and proprietary formats, government agencies and private institutions hide their actions. At the same time, everything people do in socio-technical networks has been captured in an almost absent world regarding legal regulations protecting individuals' privacy and surveillance. Even though networks collect more and more data from their users, few laws protect users from exercising control over their digital dossiers. Market pressures are advancing on consumers who become raw materials for data mining. Surveillance cameras and sensors are becoming cheaper and affordable in more places. Besides a wealth of data, the information from such operations results in detailed user profiles. All of this is blurring the boundaries between the public and private sectors (Pasquale, 2015).

Considerable aspects of social life, such as the economy, health care, security, and more, are managed by artificial intelligence models based on big data. These models are obscure, difficult to challenge, and keep accountable, operating on a large scale to optimize the lives of millions of people, or as O'Neil (2017) referred to, they are weapons of math destruction.

Automated systems are based on algorithmic logic. It applies artificial intelligence to processes transformed by digitalization, such as television, the financial market, public safety, and all spheres where data collecting serves as a means for extracting information capital (Silva, 2022). Life turned into data is the commodity of the surveillance economy that has turned citizens into data (Véliz, 2021). Or, in the words of Garcia Canclini (2020), citizens are replaced by algorithms.

Societies have used surveillance-driven technologies ostensibly to prevent crime, track suspects, victims, and witnesses, and manage the penal and penitentiary system based on social protection. Such a trend should be criticized for at least two reasons. First, societies have evolved into overprotected states based on a culture of fear and the diffuse implementation of surveillance technologies. Second, there are concerns about the erosion of the right to privacy derived from using surveillance technologies by private companies and public institutions (Vermeersch & de Pauw, 2017).

State surveillance for security purposes and corporate espionage are not similar if examined superficially. Private companies may argue that regulations reduce profits and the ability to innovate, while the state claims that society is in danger without full access to information. Based on the security argument, it is more difficult to crack down on state surveillance than corporate surveillance. However, their obscure structure and the intrinsic

collaboration between the public and private have shown that they are similar (Pasquale, 2015). There is a logic behind the idea of data-driven security that believes that the collection of personal data would enable and be directed to focus attention and resources on threats, allowing them to be prevented (Čas et al., 2017). It presumes that citizens value security more than privacy, as those who owe nothing also do not fear increased surveillance (Vermeersch & de Pauw, 2017).

Technological rationality has become political rationality in a scenario that uses privatization for cost reduction and profit maximization. Technological solutions are necessary for cost reduction and outsourcing decisions to intelligent machines (Benjamin, 2019). This context has shown that people become very visible. At the same time, other agents try to invisibilize themselves, as governments classify more documents as secret and delegate more functions to outsourced companies more easily to escape the scrutiny of the population (Morozov, 2020). Or, in the words of Bauman and Lyon (2013, p. 27), "the drones of the next generation will be able to see everything while remaining comfortably invisible - both literally and metaphorically."

Surveillance is not a new phenomenon, but it has been increasingly reinforced by technological development. The observation towers of Bentham's panopticon (Foucault, 1983) give way to interconnected camera systems with ever-increasing capabilities. Nowadays, they provide high-resolution images, record noise that recognizes faces, and alert operators to suspicious activities (Vermeersch & de Pauw, 2017). The boundary between public and private is dissipating with private cameras in public spaces (Firmino, 2017).

Surveillance is not only formed by video surveillance, but the association between the two is inevitable. This is due to the massive presence of cameras and the emergence of facial recognition technologies (Oliveira, 2021). Such correlation also leads to the need to understand facial recognition technologies as "algorithmic arrest technologies" because of their imprecision (Silva, 2022).

Rafael Capurro (2016) points to the transformation of the world into a panopticon, with expanded surveillance, as the digital economy has lost awareness about human freedom and the interactions between the physical and digital worlds. The main question is who exploits individuals in the physical and cyber world in how capitalism manifests itself today. This paper aims to identify and problematize the excluded and the beneficiaries in this process that comprises surveillance culture. Civil society must ask itself what kinds of mechanisms will be helpful to maintain civility in the two worlds that are, after all, the same.

Privacy is not only a fundamental right but also a guarantee of other fundamental rights and freedoms that balance the state and citizens in the development of democracy, social and economic innovation, and the exercise of autonomy, as pointed out by Daniel Solove (2008). Privacy is a condition for the individual to express himself freely. Mass surveillance is a symptom of disrespect for democratic principles (Čas et al., 2017). For Frank Pasquale (2015), the irresponsibility of a surveillance state can mean a more significant threat to freedom than specific security threats, as they erode various rights, such as those mentioned above.

Carissa Véliz (2021) argues that a world without privacy is dangerous because privacy consists of not sharing intimate matters, such as thoughts, experiences, conversations, and plans - we add our habits, our affections, our quirks, and our fears. Human beings need privacy to relax from the difficulty of living in society, explore new ideas liberally, and form their own opinions.

Privacy helps to protect against unwanted pressures and abuses of power. The emergence of a new civilization requires an open-minded intercultural dialogue that ensures more freedom of information and communication (Capurro, 2016, p. 1). Freedom of thought lies at the heart of intercultural information ethics for the future.

References

Aguirre, K., Badran, E., & Muggah, R. (2019). *Future crime: Assessing twenty first century crime prediction*. JSTOR.

Bauman, Z., & Lyon, D. (2013). *Vigilancia líquida*. Editora Zahar.

Benjamin, R. (2019). Race after technology: Abolitionist tools for the new jim code. *Social Forces*.

Bruno, F. G. (2009). Mapas de crime: vigilância distribuída e participação na cibercultura. *E Compós*, *12*(2).

Capurro, R. (2016). Cidadania na Era Digital. Trad. SCHNEIDER, Marco., BEZERRA, Arthur. *Comunicação, Cultura, Informação e Democracia: Tensões e Contradições. Lisboa, Portugal: MEDIA XXI–Pubishing, Research and Consulting*, 49–75.

Čas, J., Bellanova, R., Burgess, J. P., Friedewald, M., & Peissl, W. (2017). Introduction: Surveillance, privacy and security. In *Surveillance, Privacy and Security* (pp. 1–12). Routledge.

Firmino, R. J. (2017). Securitização, vigilância e territorialização em espaços públicos na cidade neoliberal. *Risco Revista de Pesquisa Em Arquitetura e Urbanismo (Online)*, *15*(1), 23–35.

Foucault, M. (1983). Discourse and Truth: the Problematization of Parrhesia. In *University of California at Berkeley*. University of California. https://web.archive.org/web/20220726122658/https://www.foucault.info/parrhesia/

García Canclini, N. (2020). *Ciudadanos reemplazados por algoritmos*. transcript Verlag.

Lyon, D. (2007). *Surveillance studies: An overview*.

Lyon, D. (2019). Surveillance capitalism, surveillance culture and data politics 1. In *Data politics* (pp. 64–77). Routledge.

Morozov, E. (2020). *Big Tech: a ascensão dos dados e a morte da política*. Ubu Editora LTDA ME.

Oliveira, S. R. de. (2021). Sorria, você está sendo filmado!: repensando direitos na era do reconhecimento facial. *São Paulo: Thomson Reuters Brasil*.

O'neil, C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Silva, T. (2022). *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais*. Edições Sesc SP.

Solove, D. J. (2008). Data mining and the security-liberty debate. *The University of Chicago Law Review*, *75*(1), 343–362.

Véliz, C. (2021). *Privacidad es poder: Datos, vigilancia y libertad en la era digital*. Debate.

Vermeersch, H., & de Pauw, E. (2017). The acceptance of new security oriented technologies: A 'framing experiment. In *Surveillance, privacy and security* (pp. 52–70). Routledge.

Zuboff, S. (2021). A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. *Rio de Janeiro: Intrínseca*.