CAPITALISMO DE VIGILÂNCIA E SOCIEDADE BRASILEIRA: ANÁLISE CRÍTICA E JURISPRUDENCIAL A PARTIR DE SHOSHANA ZUBOFF

SURVEILLANCE CAPITALISM AND BRAZILIAN SOCIETY: A CRITICAL AND JURISPRUDENTIAL ANALYSIS BASED ON SHOSHANA ZUBOFF

Anderson Filipini Ribeiro[1]
Filipe Mello Sampaio Cunha[2]
Natalia Maria Ventura da Silva Alfaya[3]

RESUMO

Este artigo analisa criticamente a teoria do capitalismo de vigilância desenvolvida por Shoshana Zuboff, articulando-a com a realidade brasileira contemporânea. O problema central investigado reside na forma como a extração massiva de dados pessoais, impulsionada por grandes corporações tecnológicas, afeta direitos fundamentais no Brasil, aprofundando desigualdades sociais e comprometendo a soberania informacional do país. O objetivo principal é examinar como o capitalismo de vigilância se manifesta no contexto brasileiro, especialmente em relação à desigualdade digital, à utilização de tecnologias de reconhecimento facial pelo Estado, à gestão de dados sensíveis em políticas públicas e aos desafios jurídicos para a proteção da privacidade. A metodologia adotada é de natureza teórico-conceitual e exploratória, com revisão bibliográfica das principais obras sobre o tema – destacando-se Zuboff (2019) – e análise de jurisprudência brasileira, especialmente decisões paradigmáticas do Supremo Tribunal Federal (ADI 6.387 e ADI 5.527) e do Superior Tribunal de Justiça sobre proteção de dados. Nas considerações finais, conclui-se que o Brasil enfrenta desafios específicos na contenção das práticas do capitalismo de vigilância, devido à combinação de desigualdades estruturais, dependência tecnológica e fragilidades institucionais. Contudo, também se observa a emergência de resistências importantes, tanto no campo regulatório – com a promulgação da LGPD e a atuação da ANPD – quanto na atuação do Judiciário e da sociedade civil. O artigo aponta a necessidade de fortalecer políticas públicas,

[1]Mestrando em Direito, pelas Faculdades Londrina. Bacharel em Direito e Teologia. Pós-Graduado em Direito Penal, Direito Militar, Administração e Segurança Pública, e em Direito Civil e Processual Civil. Habilitações linguísticas, nível B1, nos idiomas: Espanhol (DELE), Francês (DELF) e Italiano (CILS). Lattes: http://lattes.cnpq.br/0703783803020290. E-mail: direito.andersonfilipini@gmail.com. ORCID: https://orcid.org/0009-0008-5145-2476.

[2]Mestrando em Direito, pelas Faculdades Londrina. Bacharel em Direito e Ciências Políticas. Pós-Graduado em Gestão Pública, Gestão de Processos BPM-CBOK, bem como Gestão das Águas e Sustentabilidade dos Recursos Hídricos no Brasil. Lattes: http://lattes.cnpq.br/4680398321828617. E-mail: filipemgm@gmail.com.

[3]Graduada em Direito, pela Universidade Estadual de Londrina, 2005-2009. Especialista em Direito Internacional e Econômico, 2010-2011; e em Filosofia Jurídica, 2020-2021, ambas pela Universidade Estadual de Londrina. Mestra em Direito Negocial, pela Universidade Estadual de Londrina, 2012-2014. Doutora em Ciências Jurídicas e Sociais do Programa de Pós-Graduação em Sociologia e Direito, pela Universidade Federal Fluminense, 2015-2018. Advogada inscrita na OAB/PR 59.792. Docente do curso de graduação em Direito da Escola de Direito das Faculdades Londrina (EDFL) e do Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias, pela mesma IES. Lattes: http://lattes.cnpq.br/9731930696524695. E-mail: naty.alfaya@gmail.com https://orcid.org/0000-0002-0312-3677.

regulamentações e movimentos sociais para garantir a proteção de direitos fundamentais na era digital.

Palavras-chave: Capitalismo de Vigilância. Proteção de Dados. Brasil. Jurisprudência. Shoshana Zuboff.

ABSTRACT
This article critically analyzes the theory of surveillance capitalism developed by Shoshana Zuboff, articulating it with the contemporary Brazilian reality. The central problem investigated lies in how the massive extraction of personal data, driven by large technological corporations, affects fundamental rights in Brazil, deepening social inequalities and compromising the informational sovereignty of the country. The main objective is to examine how surveillance capitalism manifests in the Brazilian context, especially in relation to digital inequality, the use of facial recognition technologies by the state, the management of sensitive data in public policies, and the legal challenges for the protection of privacy. The adopted methodology is of a theoretical-conceptual and exploratory nature, with a literature review of the main works on the subject – highlighting Zuboff (2019) – and analysis of Brazilian jurisprudence, especially paradigm decisions from the Supreme Federal Court (ADI 6.387 and ADI 5527) and the Superior Court of Justice regarding data protection. In the final considerations, it is concluded that Brazil faces specific challenges in containing the practices of surveillance capitalism, due to the combination of structural inequalities, technological dependency, and institutional weaknesses. However, there is also an observation of the emergence of significant resistances, both in the regulatory field – with the enactment of the LGPD and the actions of the ANPD – and in the Judiciary's and civil society's actions. The article highlights the need to strengthen public policies, regulations, and social movements to ensure the protection of fundamental rights in the digital age.

Keywords: Surveillance Capitalism. Data Protection. Brazil. Jurisprudence. Shoshana Zuboff.

INTRODUCTION

In recent decades, the transformations driven by digitalization have profoundly changed the structure of contemporary societies, redefining modes of production, circulation and consumption of information. This new scenario is characterized by an intensification of the practices of collection, storage and analysis of personal data, which begin to play a central role in economic and social dynamics. Shoshana Zuboff (2019), in her seminal work "The Era of Surveillance Capitalism", identifies in this process the emergence of a new economic logic, which she calls surveillance capitalism: a regime

that appropriates unilaterally human experience, converting it into behavioral data for purposes of prediction, modulation and profit.

According to the author, this model not only explores information as a strategic resource, but also inaugurates a new architecture of power, supported by pervasive surveillance and algorithmic automation (Zuboff, 2019). It is a qualitative transformation in relation to industrial capitalism, which was based on the exploitation of labor and natural resources, while surveillance capitalism is based on the extraction of subjectivities and daily interactions, transformed into informational raw material.

This phenomenon acquires especially relevant contours when analyzed from the perspective of the Global South, and in particular in the Brazilian context. According to the ICT Households Report (2023), approximately 84% of Brazilian households have access to the internet, which represents a significant improvement over the previous decade. However, the quality and intensity of this access reveal deep regional and socioeconomic asymmetries: while in urban areas internet penetration is 90%, in rural areas it does not exceed 60%. In addition, more than 17 million Brazilians still remain completely disconnected, according to data from the Brazilian Institute of Geography and Statistics (IBGE, 2022).

This digital inequality has direct effects on the way surveillance capitalism is installed and operates in the country, because data extraction is not homogeneous, but strongly conditioned by factors such as income, education, race and geographical location. As warned by Canclini (2005), the global dynamics of consumption and communication tend to reproduce and deepen existing structural inequalities, a phenomenon that is clearly manifested in the Brazilian society.

The performance of large technology corporations - so-called big techs, such as Google, Meta (Facebook, Instagram and WhatsApp), Amazon and TikTok - is central to this process. These platforms, widely used in Brazil, operate with business models based on monetization of behavioral data, employing complex artificial intelligence systems to analyze and predict consumption patterns and social behavior. In the country, WhatsApp is used by about 98% of internet users (Datafolha, 2023), consolidating not only as the main means of communication, but also as a privileged channel for the dissemination of

misinformation and political manipulation, phenomenon widely observed in the elections of 2018 and 2022.

The problem that motivates this research is the need to understand how this economic model - structured in massive data extraction - affects fundamental rights in Brazil, especially privacy, protection of personal data, individual freedom and informational self-determination. The Federal Constitution of 1988 assures, in its article 5, paragraph X, the inviolability of privacy, private life and honor, but the rapid technological evolution has created new frontiers and challenges for the realization of these rights (Brazil, 1988).

In response to these challenges, Brazil approved the General Law on Personal Data Protection (LGPD) - Law no 13.709, of 2018 -, which established principles and rules for the processing of personal data, inspired by the General Data Protection Regulation of the European Union (GDPR). More recently, with the promulgation of the Constitutional Amendment no 115 of 2022, the protection of personal data was formally elevated to the category of fundamental right in the Brazilian legal system, consecrating a constitutional directive that guides the actions of public authorities and private companies (Brazil, 2018).

However, as experts point out (Its Rio, 2022; Dados.org, 2023), there remain important regulatory and institutional gaps that undermine the effectiveness of these standards, especially given the capacity of big techs and the increasing use of surveillance technologies by the State, such as facial recognition systems deployed in several Brazilian cities, often without adequate legal basis or social control.

In this sense, the judgment by the Federal Supreme Court (STF) of the Direct Action of Unconstitutionality (ADI) no 6.387, in which it was stated, categorically, that "the right to personal data protection has constitutional stature, being a condition for the full exercise of citizenship" (Brazil, STF, ADI 6.387, Rel. Min. Rosa Weber, 2020). This decision represented a milestone in the construction of the Brazilian jurisprudence on the subject, reaffirming the centrality of data protection in the fundamental rights system.

The general objective of this article is to critically analyze the phenomenon of surveillance capitalism from the work of Shoshana Zuboff, articulating it with the Brazilian reality and reflecting on the legal, political and social implications of this

model. As specific objectives, we seek to: (i) present the theoretical foundations of surveillance capitalism; (ii) identify the technologies and architectures that support it; (iii) analyze its implementation in the Brazilian reality, based on emblematic cases and empirical data; (iv) evaluate institutional responses, especially legal ones, such as the LGPD and the performance of the Judiciary; and (v) discuss alternatives of resistance and paths for a democratic governance of technology.

The methodology adopted is theoretical-conceptual and exploratory, based on the bibliographical review of the main works and academic articles about surveillance capitalism, data protection, digital rights and informational sovereignty. In addition, a jurisprudential analysis is carried out, focusing on relevant decisions issued by the Brazilian superior courts, which elucidate how national law has sought to regulate and limit the practices associated with digital surveillance, as well as protecting the fundamental rights of citizens.

The choice for the Brazilian section is justified by the need to understand how surveillance capitalism manifests itself in peripheral and unequal contexts, which have specific characteristics regarding access, use and regulation of digital technologies. As the largest country in Latin America, with a population of over 215 million inhabitants and one of the most dynamic digital markets in the world, Brazil is a privileged laboratory for the study of these new forms of power and domination, as well as the possibilities of resistance and the construction of democratic alternatives (IBGE, 2022; CETIC.br, 2023).

Thus, this article aims to contribute to the deepening of academic reflection on the transformations caused by surveillance capitalism, providing subsidies for public debate and the formulation of public policies that ensure the protection of fundamental rights, Information sovereignty and the promotion of a more just, inclusive and democratic digital society.

1 THEORETICAL FOUNDATIONS OF THE SURVEILLANCE CAPITALISM

Zuboff (2019) defines surveillance capitalism as "a new economic order that unilaterally claims human experience as a free raw material for hidden commercial

practices of extraction, prediction and sale" (Zuboff, 2019, p. 14). It is a regime that not only collects data, but also transforms the human experience into a source of profit, subordinating individual behavior to automated modulation and control processes.

The surveillance capitalism is not a simple extension of the informational capitalism described by Castells (2013), but a qualitative transformation of the mode of production, based on the continuous and massive capture of behavioral data. Its emergence occurs within the large technology companies, especially Google and Facebook, which inaugurate unprecedented data extraction practices.

Zuboff (2019) introduces the concept of "surplus behavioral data" to describe informational inputs that exceed what is needed to improve services and are used to generate new behavioral prediction products. These surpluses feed artificial intelligence systems that create profiles, forecasts and eventually interventions in human behavior.

This logic inaugurates a new cycle of capital accumulation, distinct from the industrial model, based on the extraction of natural resources and the exploitation of labor. Now, capital appropriates subjectivity and human interactions, converting them into digital commodities (Zuboff, 2019).

Zuboff distinguishes surveillance capitalism from other historical forms of power by coining the concepts of "instrumentarianism" and "Big Other". Instrumentarianism refers to the application of technological instruments for modulating behavior, without the need for direct physical coercion, but through persuasive and imperceptible digital architectures (Zuboff, 2019).

The "Big Other" represents a new instance of power, distinct from the Orwellian "Big Brother", because it acts silently, collecting and processing data in real time to predict and guide behaviors (Zuboff, 2019). It is a reconfiguration of power relations, in which control is not given by ostensible surveillance, but by the anticipation and invisible conditioning of human actions.

Although there are parallels with the panoptism of Foucault, the surveillance capitalism is distinguished by the absence of an explicit disciplinary centrality. Deleuze (1992) already anticipated this transition by proposing the concept of "control societies", in which power operates through continuous modulations, surpassing classical disciplinary institutions.

While industrial capitalism aimed to discipline bodies for production, surveillance capitalism seeks to capture the mind and behavior for prediction and modulation, inaugurating a new configuration of social power (Zuboff, 2019).

2 THE TECHNICAL AND SOCIAL ARCHITECTURE OF SURVEILLANCE

The materialization of the surveillance capitalism depends on a complex technological ecosystem, which includes cookies, trackers, Internet of Things (IoT) sensors, artificial intelligence and facial recognition systems. These technologies enable massive and continuous data collection, transforming everyday devices into ubiquitous surveillance tools (Zuboff, 2019).

In Brazil, the use of facial recognition systems in public spaces has grown, especially in public safety programs such as the São Paulo subway and video surveillance systems in several capitals (Dados.org, 2023).

Digital platforms such as Google, Facebook, Instagram and TikTok are central elements in the architecture of surveillance, functioning as inevitable intermediaries in everyday life. The ubiquity of mobile devices amplifies this dynamic, enabling the collection of data on location, habits and preferences in real time (Castells, 2013).

These architectures are designed to promote the permanence and engagement of users, maximizing the production of surplus behavioral data, as pointed out by Zuboff (2019).

Persuasive design, or "captology," explores cognitive biases to induce desired behaviors, promoting engagement time maximization and continuous data collection (Zuboff, 2019). Thus, the so-called "attention economy" is consolidated, in which time and user concentration are goods disputed between platforms (Han, 2018).

In Brazil, the impact of this dynamic is visible in the popularization of applications such as WhatsApp and TikTok, whose algorithmic architecture guides the behavior of users and structure everyday social practices (Zuboff, 2019; Datafolha, 2023).

3 SURVEILLANCE CAPITALISM IN THE BRAZILIAN REALITY

Although Brazil has more than 150 million internet users, access is deeply unequal, reflecting the social and economic cleavages of the country (Cetic.br, 2023). This inequality creates a digital divide that not only excludes millions from access to information, but also concentrates the most harmful effects of surveillance capitalism on vulnerable populations, subject to predatory data collection practices.

Although internet penetration has increased in Brazil, the country still lives with a significant "digital divide", especially in the North and Northeast regions. According to Cetic.br (2023), about 20% of the population does not have regular internet access, which compromises the full exercise of digital citizenship and shows that forms of surveillance and data collection affect social groups unequally.

This context is aggravated by the practice known as "zero rating", in which operators offer free access to certain platforms, such as Facebook and WhatsApp, to the detriment of full internet access. This creates a "bundled" internet that limits informational diversity and reinforces the dependence on platforms, main vector of surveillance capitalism (Zuboff, 2019).

The ubiquity of digital platforms in Brazil creates a scenario in which the daily life of most citizens is mediated by surveillance technologies. Datafolha survey (2023) points out that more than 95% of Brazilians who use the internet are active users of WhatsApp, while Instagram has consolidated itself as a primary source of information for 45% of the population.

This digital protagonism, often unregulated, exposes millions of Brazilians to opaque mechanisms of data collection and behavioral manipulation, as analyzed by Zuboff (2019), increasing the risk of silent and effective social control.

Digital platforms play a central role in the organization of social and economic life in Brazil, from e-commerce to interpersonal relations. WhatsApp, for example, is the main communication tool in the country, being also a fundamental vector in the dissemination of disinformation and the political instrumentalization of networks (Tarrow, 2021).

This centrality reinforces the dependence on platforms and the exposure of the Brazilian population to the dynamics of the surveillance capitalism.

The use of surveillance technologies by the Brazilian State deserves to be highlighted. Several public safety programs have implemented facial recognition systems, often without proper public debate and robust data protection guarantees (Dados.org, 2022).

Another example is CadÚnico (CadUnique), a database that gathers sensitive information from millions of Brazilians for the implementation of social policies (Brazil, MDS, 2023). Although fundamental to public policy, its centralization and digitization raise concerns about security, privacy and misuse of data (Dados.org, 2023).

In health, the Covid-19 pandemic has accelerated the digitalization of services and the creation of applications such as Connect SUS, exposing the population to new risks related to health surveillance and information security (Brazil, 2021).

The use of facial recognition for public safety purposes has expanded in Brazil, with controversial cases. The performance of the Court of Justice of the state of Bahia stands out, which, in the Process no 0005649-90.2020.8.05.0001, confirmed the legality of the use of smart cameras by the Military Police, defending the public interest in security. However, human rights organizations criticize the measure, pointing out the risk of discrimination and error, especially against the black population (Brazil, 2020).

In the area of public health, Connect SUS, a system that stores sensitive data from citizens, was the subject of legal debate when it suffered a hacker attack in 2021. Although the STF (Federal Supreme Court) did not directly judge the case, Recommendation 73 of the National Council of Justice, from 2020, already directed organs of the Judiciary to prioritize data protection measures in the treatment of personal information during the pandemic (CNJ, 2020).

The Single Registry for Social Programs (CadÚnico (Cad Unique)) concentrates data from more than 80 million Brazilians, and its governance raises concerns about consent and security. In the Direct Action of Unconstitutionality (ADI) no 6.387, the STF discussed aspects of the Provisional Measure no 954, of 2020, which determined the mandatory sharing of data by telecommunication companies with the IBGE (Brazilian Institute of Geography and Statistics). The Supreme Court, in a historic decision, considered the measure unconstitutional, stating that "the right to personal data protection has constitutional stature" (Brazil, STF, ADI 6.387, Rel. Min. Rosa Weber, 2020).

This decision set a relevant milestone by expressly recognizing the protection of personal data as a fundamental right, aligning Brazil to international trends.

The most vulnerable populations are also the most affected by surveillance capitalism in Brazil. The use of automated systems to determine access to benefits, services, or for public safety purposes can reproduce and deepen structural discrimination, a phenomenon known as “algorithmic racism.”" (Noble, 2018).

4 LGPD AND THE LIMITS OF THE BRAZILIAN REGULATION

The General Personal Data Protection Law (LGPD), enacted in 2018, represents a significant advance in data protection in Brazil. Inspired by the European General Data Protection Regulation (GDPR), the LGPD establishes principles, rights and duties related to the processing of personal data (Brazil, 2018).

The LGPD (Law no 13.709, of 2018) was approved after extensive debate, with direct inspiration in the European GDPR, and entered fully into force in September of 2020. Subsequently, the Constitutional Amendment no 115 of 2022 expressly inserted personal data protection in the list of fundamental rights provided for in the Constitution, conferring even more solidity to the Brazilian protective framework (Brazil, 2018).

Despite the advances, the LGPD has important gaps, especially with regard to its effective application and supervision. The absence of robust technical and institutional mechanisms limits its ability to contain the most harmful practices of surveillance capitalism (Its Rio, 2022).

In addition, the LGPD allows broad exceptions for data processing by the State, especially in areas such as public security, without sufficient guarantees of accountability (Doneda, 2020).

Despite the constitutionalization, normative gaps remain. The LGPD provides significant exceptions, especially for the processing of data by public authorities, which may be used for purposes of public security, national defense and State security, without being subject to the same restrictions applicable to the private sector (art. 4, III, of the LGPD). Such a gap may legitimize abusive practices of state surveillance.

In addition, the figure of consent, although central in LGPD, is often obtained in a flawed way, through adhesion contracts or confusing interfaces, which violates the principle of informational self-determination (Its Rio, 2022).

Compared to the GDPR, the LGPD presents weaknesses in terms of enforcement and protection of sensitive data. While the European Union has a consolidated tradition of privacy protection, Brazil still lacks an institutional and social culture in this field (Canclini, 2005).

The European GDPR enshrines a more protective logic, highlighting, for example, the right to data portability and forgetting, both of which are still uncertain in terms of implementation in Brazil. The Superior Court of Justice (STJ) has already signaled openness for the application of the right to be forgotten in certain cases, as in REsp 1.335.153/ RJ, but the Supreme Court (STF), in the Issue 786, decided that the right to be forgotten is not compatible with the Brazilian Constitution, which limits the application of this guarantee in the country (Brazil, 2021a; Brazil, 2021b; European Union, 2016).

The National Data Protection Authority (ANPD) is the body responsible for supervising the application of the LGPD. Although its creation represented an advance, its operational capacity and autonomy are still limited, which compromises the effectiveness of regulation (Its Rio, 2022).

Brazilian courts, in turn, are beginning to position themselves on issues related to data protection, but the jurisprudence is still incipient (Silva, 2022).

The National Data Protection Authority (ANPD) began its operations in 2021, with the publication of important guidelines, such as the Guide for Definitions of Personal Data Processing Agents and Data Processors (ANPD, 2021).

On the judicial side, we highlight the decision of the Court of Justice of the state of São Paulo (TJSP), which applied for the first time sanctions based on the LGPD, condemning a company to pay compensation for data leakage (TJSP (Court of Justice of the state of São Paulo), Civil Appeal no 1006569-13.8.26.0100). The decision emphasized the need for effective protection of personal data as an expression of the right to personality (TJSP (Court of Justice of the state of São Paulo), 2022).

5 SOCIOPOLITICAL IMPACTS IN BRAZIL

Surveillance capitalism poses profound challenges to privacy and individual freedom in Brazil. The massive and opaque collection of personal data, often without free and informed consent, compromises the autonomy and informational self-determination of the subjects (Zuboff, 2019). In the Brazilian context, where digital education is precarious and there is a lack of awareness about privacy-related rights, this situation is even more serious.

Ubiquitous surveillance creates an environment in which individual choices are shaped imperceptibly by algorithmic systems that define what is seen, consumed and often decided, configuring what Zuboff calls "behavioral modulation" (Zuboff, 2019).

The recognition of data protection as a fundamental right by the STF (Federal Supreme Court), in the ADI 6.387, created jurisprudence that strengthens the field of protection of privacy and autonomy in the country (Brazil, 2020). However, the challenge remains: how to operationalize this protection against the overwhelming dynamics of digital platforms?

Behavioral manipulation reaches contours especially worrying in the political field. The performance of digital marketing companies, the spread of fake news and the use of electoral micro targeting in Brazilian elections reveal the power of platforms to shape public opinion and influence democratic processes (Tarrow, 2021).

The paradigmatic case is that of the 2018 presidential elections, when WhatsApp was widely used to disseminate misinformation in an automated and massive way, directly impacting the public debate and the election result (Dados.org, 2022).

The "informational bubbles" created by algorithms, which personalize and filter content according to predefined interests, reinforce political polarization and corrode the deliberative public sphere (Sunstein, 2018).

In addition to the elections of 2018, the Superior Electoral Court (TSE) has firmly positioned itself on the fight against disinformation. Resolution no 23.610 of the TSE, of 2019, introduced measures to regulate electoral propaganda on the internet (Brazil, 2019).

The TSE also created, in partnership with platforms, the Program to Confront Disinformation, recognizing the need to regulate the performance of big techs in the

electoral process, as a way to mitigate the deleterious effects of the surveillance capitalism on Brazilian democracy.

Surveillance capitalism in Brazil operates on a society deeply marked by racial and socioeconomic inequalities. The application of automated systems in public security, such as facial recognition, has revealed discriminatory biases that reinforce control practices on historically marginalized populations, such as black and peripheral youth (Noble, 2018).

Research indicates that facial recognition systems have significantly higher error rates in black people, increasing the risk of unfair arrests and rights violations (Data.org, 2022). Thus, the technology not only reproduces but enhances pre-existing structures of oppression.

The rise of surveillance capitalism reconfigures the Brazilian public sphere, shifting the space of political debate to private environments controlled by foreign corporations (Castells, 2013). The traditional public space, characterized by plurality and the possibility of democratic deliberation, gives way to environments mediated by algorithms whose main objective is the maximization of profit through continuous engagement (Zuboff, 2019).

This transformation compromises the Habermasian ideal of a rational and inclusive public sphere, favoring the segmentation and radicalization of opinions (Habermas, 1984).

6 DIGITAL COLONIALISM AND INFORMATIONAL SOVEREIGNTY

Zuboff (2019) describes the unilateral appropriation of personal data by large technology corporations as a form of "digital colonialism". It is a process by which data generated by individuals and institutions in peripheral countries are extracted, processed and monetized by companies based in central countries, without the original producers participating in the economic benefits of this extraction.

In Brazil, this logic manifests itself clearly: the main digital platforms that dominate the national market - Google, Meta (Facebook, Instagram, WhatsApp) and

Amazon - concentrate data processing and analysis capacity, while the country remains as a mere supplier of informational prime (Silveira, 2021).

This digital colonialism reinforces a relationship of technological dependence, in which Brazil is positioned as a consumer of foreign technologies and supplier of raw data, with no sovereign capacity to develop and control its own digital infrastructures (Canclini, 2005).

Informational inequality is not only economic, but also political and epistemological, because it limits the national capacity to establish proper parameters for regulation and use of technologies, deepening subordination to the interests of international capital (Zuboff, 2019).

The struggle for digital sovereignty emerges, thus, as one of the great challenges for Brazil and other countries of the Global South. It is about the ability to establish policies, infrastructures and regulatory frameworks that guarantee national control over data flows and the protection of fundamental rights of its citizens (Its Rio, 2022).

In this sense, proposals such as the construction of local data centers, the strengthening of public policies for technological innovation and the strict regulation of the performance of big techs are essential ways to reverse the framework of dependency and vulnerability (Silveira, 2021).

Brazilian jurisprudence begins to reflect on the need for digital sovereignty. The Supreme Court, in the judgment of the ADI 5527 (WhatsApp case), recognized that platforms must comply with Brazilian judicial decisions, under penalty of violating national sovereignty (Brazil, 2020).

Although the STF has not decided on the constitutionality of the judicial blockade of WhatsApp, the trial highlighted the tension between information sovereignty and big tech power, pointing to the challenge of establishing a framework for effective regulation in the country (Brazil, 2020).

7 PERSPECTIVES OF RESISTANCE AND DEMOCRATIC GOVERNANCE

The strengthening of regulatory frameworks that restrict the predatory practices of surveillance capitalism is one of the main resistance strategies. LGPD represents a first

step, but it is necessary to advance in its application and complement it with specific legislation that regulates the performance of digital platforms, such as the recent discussion on the Fake News Bill (PL 2.630, from 2020), which seeks to establish responsibilities for social network providers in Brazil (Brazil, 2020).

In addition, it is essential to ensure the protection of sensitive data collected in public policies and expand legal safeguards against discriminatory use of surveillance technologies (Dados.org, 2022).

Processed in the National Congress the Bill no 2.630, of 2020 (PL of the Fake News), which seeks to create a legal framework to hold platforms responsible for false content and combat information manipulation practices (Brazil, 2020).

In addition, projects such as the Civil Mark of the Artificial Intelligence (PL 21, of 2020) intend to regulate algorithmic systems, aiming to ensure transparency and accountability (Brazil, 2020).

Several theorists and social movements have defended the conception of data as a common good, that is, as collective resources that must be democratically managed and used in favor of the public interest, and not as private property of corporations (Velkova, 2016).

This perspective requires a radical revision of the legal foundations that currently allow the private appropriation of personal data, promoting governance models based on citizen participation and transparency (Doneda, 2021).

Transparency about algorithms is a recurring theme in case law. In 2022, the Superior Court of Justice (STJ), in REsp 1.770.105/ SP, understood that platforms are not obliged to disclose internal criteria for content ranking, under the argument of protection of business secrets (Brazil, STJ, 2022).

Such an understanding, however, is criticized by experts who argue that when fundamental rights are at stake, the public interest should prevail over commercial interests (Pasquale, 2015).

Another fundamental axis of resistance is the promotion of algorithmic transparency, that is, the obligation for companies and governments to disclose the criteria, processes and impacts of their automated decision-making systems (Pasquale, 2015).

Algorithmic accountability involves not only the disclosure of technical parameters, but also the effective possibility of reviewing and challenging decisions made by these systems, especially when they affect fundamental rights, such as in the case of social benefits or criminal proceedings (Miranda; Almeida, 2023).

Resistance to the surveillance capitalism is also manifested in lawsuits by civil society organizations. The Brazilian Consumer Protection Institute (IDEC) has filed several civil lawsuits against public companies for abusive practices of data collection and use, as in the case against Serasa Experian, which traded personal data without consent, see the ACP no 1010290-39.2021.8.26.0100 (IDEC, 2021; TJSP, 2021).

In Brazil, several civil society organizations work to resist surveillance capitalism, promoting research, campaigns and legal actions to defend digital rights. Groups such as the Rio Institute of Technology and Society (Its Rio), Coding Rights, Intervozes and Dados.org play a crucial role in denouncing abuses and proposing democratic alternatives for internet governance (Its Rio, 2023; Coding Rights, 2023; Intervozes, 2023; Dados.ORG, 2023).

These movements are articulated with international networks of digital resistance, evidencing that the struggle against surveillance capitalism is necessarily transnational (Zuboff, 2019).

CONCLUSION

This article critically analyzed the concept of surveillance capitalism, as developed by Shoshana Zuboff, articulating it with the Brazilian reality. It was demonstrated that, although this phenomenon is global, its manifestation in Brazil assumes specificities resulting from deep social inequalities, regulatory fragility and technological dependence.

It was identified that surveillance capitalism directly impacts fundamental rights - such as privacy and freedom -, reconfigures the public sphere and deepens historical processes of exclusion and discrimination. In addition, it was argued that the appropriation of Brazilian data by large foreign corporations constitutes a new form of digital colonialism, which compromises national sovereignty.

It is concluded that resistance to this model requires coordinated actions at multiple levels: strengthening and improving national regulations, promoting alternatives based on public interest, developing autonomous technologies and social mobilization for the defense of digital rights.

Its central objective was to critically analyze the phenomenon of surveillance capitalism, from the theoretical perspective of Shoshana Zuboff (2019), articulating it with the Brazilian reality, marked by deep social inequalities, institutional fragility and technological dependence. The problem that guided the research was to understand how the practices of massive and opaque data collection - typical of surveillance capitalism - impact fundamental rights in Brazil, especially privacy, freedom and informational self-determination.

The methodology adopted was theoretical-conceptual and exploratory, with bibliographic review of the main works on the subject and analysis of relevant national jurisprudence, identifying how the Brazilian Judiciary has faced the challenges imposed by this economic and technological model.

From the jurisprudential point of view, it was observed that Brazil has been consolidating an important normative and decision-making framework for data protection. The decision of the Federal Supreme Court in the ADI 6.387 was paradigmatic in recognizing, expressly, the protection of personal data as a fundamental right, conferring constitutional stature to the subject. This understanding was recently reinforced with the Constitutional Amendment no 115 of 2022, demonstrating a progressive alignment between jurisprudence and international trends.

In addition, decisions such as the judgment of the ADI 5527, on blocking WhatsApp, reveal the concern of the Supreme Court with the defense of the national informational sovereignty before the performance of large platforms. In the infra-constitutional context, decisions such as the TJSP (Civil Appeal no 1006569-13.2021.8.26.0100) show that local courts begin to effectively apply the provisions of the General Data Protection Law (LGPD), making companies responsible for the misuse of personal information.

However, despite these advances, the research revealed that there are still normative and institutional gaps, which make it difficult to fully protect citizens from the

predatory practices of surveillance capitalism. LGPD, although it represents a relevant regulatory framework, presents worrying exceptions, especially in the treatment of data by public authorities, which can legitimize abusive practices of state surveillance.

Moreover, digital colonialism - manifested in the appropriation of Brazilian data by large foreign corporations - reinforces the need for public policies aimed at promoting digital sovereignty, as the strengthening of national technological infrastructures and the development of more robust regulatory frameworks, such as those being discussed in the PL of the Fake News and in the Legal Framework of Artificial Intelligence.

Finally, it should be noted that resistance to the surveillance capitalism in Brazil is expressed not only in the legal framework, but also in the performance of social movements, civil society organizations and academic initiatives seeking to build a democratic governance of digital technologies.

It is concluded that, to face the challenges posed by surveillance capitalism, Brazil needs to consolidate its institutional culture of data protection, strengthen the role of the National Data Protection Authority (ANPD), expand algorithmic accountability and foster transparency of corporate and state data collection and processing practices. This is the only way to ensure that the country advances in building a digital society that respects and promotes fundamental rights, reaffirming the centrality of human freedom and dignity in the face of new forms of informational power.

On the horizon, there remains the need for a critical reflection on the forms of freedom and autonomy in the digital age, recognizing that the construction of a more just and democratic society necessarily passes by confronting the challenges posed by surveillance capitalism.

This article demonstrated that, in Brazil, the surveillance capitalism acts on a ground marked by historical and institutional inequalities, but it is also the stage of significant resistance, both institutional and social.

Brazilian jurisprudence evolves to recognize and protect fundamental rights related to privacy and data protection, but faces challenges in the face of power asymmetry among State, citizens and transnational corporations.

Confronting surveillance capitalism requires strengthening regulatory institutions, consolidating a legal culture focused on data protection and promoting democratic and inclusive alternatives to digital governance.

REFERÊNCIAS

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo para definição dos agentes de tratamento de dados pessoais e do encarregado**. Brasília, DF: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-agentes-de-tratamento.pdf . Acesso em: 2 jun. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Senado Federal, 1988.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. **Emenda Constitucional nº 115**, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União, Brasília, DF, 11 fev. 2022.

BRASIL. Congresso Nacional. Senado Federal. **Projeto de Lei n.º 2.630, de 2020**. Estabelece a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, altera a Lei nº 12.965/2014 (Marco Civil da Internet). Brasília, DF, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. Acesso em: 2 jun. 2025.

BRASIL. Congresso Nacional. Câmara dos Deputados. **Projeto de Lei n.º 21, de 2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil. Brasília, DF, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2239760. Acesso em: 2 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.387**. Relatora: Min. Rosa Weber. Brasília, DF, 2020. Disponível em: https://www.stf.jus.br. Acesso em: 2 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 5.527**. Relator: Min. Edson Fachin. Brasília, DF, 2021. Disponível em: https://www.stf.jus.br. Acesso em: 2 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário com Repercussão Geral n. 1.010.606/RJ (Tema 786)**. Relator: Min. Dias Toffoli. Brasília, DF, 2021. Disponível em: https://www.stf.jus.br. Acesso em: 2 jun. 2025.

BRASIL. **Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome (MDS).** Cadastro Único para Programas Sociais. Brasília: MDS, 2023. Disponível em: https://www.gov.br/mds/pt-br/acoes-e-programas/cadastro-unico. Acesso em: 2 jun. 2025.

BRASIL. Ministério da Saúde. **Conecte SUS: saiba como funciona. Brasília: Ministério da Saúde, 2021.** Disponível em: https://www.gov.br/saude/conectesus. Acesso em: 2 jun. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial n. 1.335.153 - RJ (2012/0185646-6). Relator: Min. Luis Felipe Salomão**. Brasília, DF, 15 out. 2013. Disponível em: https://www.stj.jus.br. Acesso em: 2 jun. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.770.105/SP. Relator: Ministro Paulo de Tarso Sanseverino**. Brasília, julgado em 28 set. 2022. Disponível em: https://www.stj.jus.br. Acesso em: 2 jun. 2025.

BRASIL. Tribunal de Justiça da Bahia. **Decisão do Processo nº 0005649-90.2020.8.05.0001 confirma legalidade de câmeras com reconhecimento facial**. Salvador: TJBA, 2020. Disponível em: https://www.tjba.jus.br. Acesso em: 2 jun. 2025.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.610, de 18 de dezembro de 2019**. Estabelece normas para a propaganda eleitoral, utilização e geração do horário gratuito e condutas ilícitas em campanha eleitoral. Diário da Justiça Eletrônico, Brasília, DF, 20 dez. 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 2 jun. 2025.

CANCLINI, Néstor García. **Consumidores e cidadãos: conflitos multiculturais da globalização**. 5. ed. Rio de Janeiro: UFRJ, 2005.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2013.

CETIC.br. **TIC Domicílios 2023: Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros**. São Paulo: Comitê Gestor da Internet no Brasil, 2024.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). Recomendação nº 73, de 20 de agosto de 2020. **Recomenda aos órgãos do Poder Judiciário a observância de medidas voltadas à proteção de dados pessoais no uso de tecnologias no contexto da pandemia da Covid-19**. Brasília: CNJ, 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3395. Acesso em: 2 jun. 2025.

CODING RIGHTS. Disponível em: https://codingrights.org. Acesso em: 2 jun. 2025.

DADOS.org. **Relatório sobre tecnologias de vigilância no Brasil**. São Paulo: DADOS.org, 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Forense, 2020.

DELEUZE, Gilles. **Post-scriptum sobre as sociedades de controle**. In: DELEUZE, Gilles. Conversações. São Paulo: Editora 34, 1992. p. 219-226.

HABERMAS, Jürgen. **Mudança Estrutural da Esfera Pública**. Rio de Janeiro: Tempo Brasileiro, 1984.

HAN, Byung-Chul. **Sociedade do cansaço**. Petrópolis: Vozes, 2018
.
IDEC – INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. **Ações civis públicas para proteção de dados pessoais**. São Paulo, 2021. Disponível em: https://idec.org.br. Acesso em: 2 jun. 2025.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Pesquisa Nacional por Amostra de Domicílios Contínua: acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal**. Rio de Janeiro: IBGE, 2022.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO (ITS Rio). **Guia da LGPD para cidadãos**. Rio de Janeiro: ITS Rio, 2022.

INTERVOZES. Disponível em: https://intervozes.org.br. Acesso em: 2 jun. 2025.

MIRANDA, Carla; ALMEIDA, João. **Accountability e sistemas algorítmicos: desafios para a proteção de direitos fundamentais**. São Paulo: Editora Jurídica, 2023.

NOBLE, Safiya Umoja. **Algorithms of oppression: how search engines reinforce racism**. New York: NYU Press, 2018.

PASQUALE, Frank. **The black box society: the secret algorithms that control money and information**. Cambridge: Harvard University Press, 2015.

SÃO PAULO (Estado). Tribunal de Justiça. **Apelação Cível nº 1006569-13.2021.8.26.0100**, 12ª Câmara de Direito Privado, Rel. Des. José Carlos Ferreira Alves, julgado em 29 mar. 2022, publicado em 1º abr. 2022. Disponível em: https://esaj.tjsp.jus.br. Acesso em: 2 jun. 2025.

SILVA, Mariana de Almeida. **A proteção de dados pessoais no Brasil: avanços e desafios da jurisprudência**. São Paulo: Revista dos Tribunais, 2022.

SILVEIRA, Sérgio Amadeu da. **Exclusão digital: a miséria na era da informação**. São Paulo: Fundação Perseu Abramo, 2021.

SILVEIRA, Sérgio Amadeu da. **Tecnopolítica e o enfraquecimento da democracia**. São Paulo: Fundação Perseu Abramo, 2021.

SUNSTEIN, Cass R. **Republic: divided democracy in the age of social media**. Princeton: Princeton University Press, 2018.

TARROW, Sidney. **O poder em movimento: os movimentos sociais e o conflito político**. Petrópolis: Vozes, 2021.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO. **Apelação Cível nº 1010290-39.2021.8.26.0100**. São Paulo, 2021. Disponível em: https://www.tjsp.jus.br. Acesso em: 2 jun. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados – GDPR). Jornal Oficial da União Europeia, L119, p. 1–88, 4 mai. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 2 jun. 2025.

VELKOVA, Julia. **Data as commons**. In: SCHÄFER, Mirko Tobias; VAN ES, Karin (org.). The datafied society: studying culture through data. Amsterdam: Amsterdam University Press, 2016. p. 87-104.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2021.