pensar
Revista de Ciências Jurídicas
e-ISSN: 2317-2150
Universidade de Fortaleza

The right to personal data protection at the intersection of data capitalism and digital colonialism[1, 2]

O direito à proteção de dados pessoais na fronteira do capitalismo de dados e do colonialismo digital

João Pedro Seefeldt Pessoa[*]

Têmis Limberger[**]

Pedro Victor dos Santos Witschoreck[***]

Abstract:

This article seeks to examine the development of regulatory models concerning the right to personal data protection, analyzing how the current regulatory framework — based on the free flow of data — legitimizes data capitalism and reinforces digital colonialism in the Global South, with particular emphasis on Brazil's General Data Protection Law (*Lei Geral de Proteção de Dados Pessoais*, LGPD). To do so, the study adopts a phenomenological-hermeneutic approach, along with monographic and comparative methods of procedure, and employs indirect documentation and literature review techniques. The conclusion is that the Brazilian data protection legislation, inspired by the European regulatory framework, may inadvertently reproduce patterns of data capitalism and digital colonialism, given that actual control over personal data by data subjects is virtually nonexistent in a digital economy dominated by large technology corporations.

Keywords: Big Tech. Data capitalism. Digital colonialism. Right to personal data protection.

Resumo:

O presente artigo pretende observar o desenvolvimento de modelos regulatórios do direito à proteção de dados pessoais, analisando como o modelo atual de regulação, fundado na livre circulação de dados, legitima o capitalismo de dados e fortalece o colonialismo digital do Sul Global, com ênfase na Lei Geral de Proteção de Dados Pessoais. Para tanto, adota-se o método de

[1] This study was funded by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) – Funding Code 001.

[2] Artigo traduzido a partir de Inteligência Artificial.

[*] Master's student in Law at Universidad de León, Spain, with a scholarship from Fundación Carolina. Master of Laws from Universidade Federal de Santa Maria (UFSM), funded by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. Researcher at the Center for Studies and Research in Law and the Internet at UFSM, registered on the Conselho Nacional de Desenvolvimento Científico e Tecnológico research platform. His research focuses on the line "Risks and (dis)control of cyberspace." Member of the research project "Digital activism and new media: challenges and opportunities for global citizenship." Universidad de León, León, Spain. Lattes; http://lattes.cnpq.br/3238221565472756 Orcid; https://orcid.org/0000-0003-1974-0247

[**] Postdoctoral degree in Laws from University of Seville (Spain). PhD in Law from Pompeu Fabra University (Spain). Master and Bachelor of Laws from Universidade Federal do Rio Grande do Sul. Professor in the Graduate Program in Law and Undergraduate Law Program at UNISINOS. Universidade do Vale do Rio dos Sinos (UNISINOS), Porto Alegre, Rio Grande do Sul, Brazil. Lattes: http://lattes.cnpq.br/4818791232370274 Orcid: https://orcid.org/0000-0003-0670-583X

[***] Ph.D. student in Law at the Graduate Program in Law at UNISINOS, funded by CAPES/PROEX. Master of Laws from UFSM. UNISINOS, Porto Alegre, Rio Grande do Sul, Brazil. Lattes: http://lattes.cnpq.br/2701429384864910 Orcid: https://orcid.org/0000-0002-5399-0023

abordagem fenomenológico-hermenêutico, o método de procedimento monográfico e comparativo, bem como técnicas de pesquisa de documentação indireta e revisão de bibliografia. Conclui-se que a legislação brasileira de proteção de dados, ao se inspirar na regulamentação europeia, pode, inadvertidamente, refletir padrões de capitalismo de dados e de colonialismo digital, considerando que o controle dos dados pessoais pelos titulares é inexistente em meio à economia digital dominada pelas grandes corporações tecnológicas.

Palavras-chave: *Big tech; capitalismo de dados; colonialismo digital; direto à proteção de dados pessoais.*

1 Introduction

The rise of data capitalism and the resulting emergence of a new regulatory paradigm for personal information have sparked a critical and necessary debate on the effectiveness of current legislation in the context of global digital transformation. At the heart of this discussion lies the question of how regulations concerning the right to personal data protection — particularly those inspired by the European Union's General Data Protection Regulation (GDPR) — reflect the dynamics of data capitalism and may in turn perpetuate a form of digital colonialism.

Considering the social and democratic dimensions of data protection regulation, this article presents a counterpoint to data capitalism, which often prioritizes profit over privacy and informational self-determination. In this context, it raises the question: to what extent can the adoption of data protection regulations — especially those inspired by European models based on the free flow of digital assets — reflect forms of data capitalism and digital colonialism?

The general objective of this study is to critically examine the regulation of the right to personal data protection, inspired by European models, as new expressions of data capitalism and digital colonialism. Specifically, the study aims to: a) discuss the emergence of data capitalism and the dominance of Big Tech, analyzing the development of regulatory models for personal data protection, with particular emphasis on the European Union's GDPR; and b) understand how the current regulatory model — based on the free circulation of data — reinforces and legitimizes data capitalism as well as identify the presence of digital colonialism in the Global South, with a focus on Brazil's General Data Protection Law (*Lei Geral de Proteção de Dados Pessoais*, LGPD).

Regarding the methodological approach, this study adopts the phenomenological-hermeneutic method, due to the need to understand and interpret the

phenomenon of data capitalism and the regulation of the right to personal data protection within the contemporary social, economic, and legal framework, considering the researcher's interaction with the phenomenon of digital colonialism. As for the procedural methodology, the monographic and comparative techniques were selected, as they allow for an in-depth analysis of data capitalism and digital colonialism from specific perspectives, particularly through the comparison of regulatory models. For data collection, the study relies on indirect documentation, including literature review and the interpretation of data relevant to the field of study.

2 On Data Capitalism and the Right to Personal Data Protection

The contemporary economy is witnessing the rise of data as a central element in market dynamics. This new reality is defined by data capitalism, in which data are not merely tools for personalizing information, but rather critical economic assets. The collection and analysis of vast volumes of personal data have become the driving force behind an economic system that derives unprecedented monetary value from the prediction, modification, and surveillance of human behavior (Mayer-Scönberger, 1997; Pessoa, 2020; Zuboff, 2019).

The dataist notion views the universe as a "data flow, and the value of any phenomenon or entity is determined by its contribution to data processing," including human relationships (Harari, 2015, p. 321). In contemporary society, humanity is increasingly integrated into data processing, which has become the primary source of understanding and intervening in individuals' lives. In this new paradigm, data are not only tools for observation but also mechanisms for shaping humanity itself, creating a symbiotic relationship between people and the systems that process their information (Hui, 2020, p. 77-78).

In this context, data emerge as economic commodities, whose value is actively constructed through algorithms, artificial intelligence, and machines. This process is intrinsic to the capital accumulation logic of Big Tech — large technology corporations represented by digital platforms (Srnicek, 2016, p. 30-31) — which not only collect data but also process and analyze it to predict behavior. This creates a continuous cycle of value generation within their operations and services. The essence of this paradigm lies in the ability to capture, analyze, and use information to forecast and influence behavior, generating value that goes beyond the material sphere and enters the complex dimensions of the digital realm (Pessoa, 2020, p. 40-55).

The transformation of data — from mere digital records to strategic assets — has been driven by the innovative business models of Big Tech companies. These business models, based on monetizing attention and subtly manipulating user behavior, have become paradigmatic across various economic sectors. Google is, for many, the most prominent example of this social revolution, as it impacts "us," "the world," and "knowledge" itself. In what has been described as the "Googlization of everything," the company, "by cataloging our individual and collective judgments, our opinions, and — perhaps most importantly — our desires, is also becoming one of the most powerful global institutions" (Vaidhyanathan, 2011, p. 14).

This is what constitutes surveillance capitalism, characterized by the "behavioral surplus, discovered more or less ready-made in the online environment, when it was realized that the data exhaust clogging Google's servers could be combined with its powerful analytical capabilities to generate predictions of user behavior" (Zuboff, 2019, p. 404). In this way, Google — later emulated by other companies — "imposed the logic of conquest, defining human experience as free for the taking, available to be compiled as data and claimed as surveillance assets" (Zuboff, 2019, p. 404).

Google's executives eventually opted for an advertising-based business model, which relies on collecting user data to develop and refine algorithms that deliver ads through an innovative auction system. The exceptional profitability of this approach encouraged other tech companies to adopt similar strategies, expanding both the capitalization of Big Tech firms and the scope of data collection. These data go beyond being a mere byproduct of users' interaction with technology; they form the foundation of corporate strategies aimed at enhancing advertising and personalizing services — forming, in effect, a true "Great Other Brother" (Zuboff, 2018, p. 57-60).

The large-scale collection of data — often performed in nontransparent ways — feeds algorithms and artificial intelligence systems that drive continuous cycles of consumption, surveillance, and control. The market is driven by prediction and forecasting, in which users are not only the targets of commerce but also the subjects of shaping and anticipation of their needs. The panopticon, originally conceived as an architectural structure of control, has now evolved into a digital super-panopticon — or cyber-panopticon—ubiquitous, distributed, fluid, and embedded in everyday technologies. In this sense, panopticism "is alive and well, armed in fact with (electronically enhanced, cyborgized) muscles so mighty that Bentham or even Foucault could not and would not have imagined them" (Bauman, 2013, p. 22).

The result is a stark power asymmetry, in which a few actors appropriate vast amounts of information, while the majority are subject to choices made by algorithms — often without their knowledge or consent. Within this scenario, users have little to no understanding of this new informational dynamic, as the perceived benefits of free access, personalization, and technological speed tend to obscure the associated risks. As Rodotà (2008, p. 37) observes, "citizens are rarely capable of grasping the meaning that the collection of certain information may assume within complex organizations equipped with sophisticated means of data processing".

In the current socioeconomic context, the use of data as an economic asset and the phenomenon of the "digitalization of life" are becoming tools of domination and social reproduction, with effects that extend beyond individuals and influence society as a whole (Wolfgang, 2021, p. 115). Today, data processing mechanisms shape decisions and the social body itself, within a context permeated by *infocracy* — an environment in which the generation and manipulation of information are crucial to governance and the dynamics of power (Han, 2022).

The monetization of data is primarily realized through targeted and segmented advertising, which uses and sells detailed user profiles to enable advertisers to deliver personalized ads. This not only fosters more efficient consumption but also perpetuates a cycle of data dependency, where privacy is often sacrificed in exchange for "free" access to platforms and services. However, the value generated is not distributed equitably; instead, it is concentrated in the hands of a few corporations that possess the power to shape markets and influence social behavior (Morozov, 2018, p. 146-147).

Criticism of these business models is not confined to the economic sphere but extends to ethical and political dimensions, as the accumulation of data by big tech companies raises concerns regarding data sovereignty, public opinion manipulation, and the weakening of democratic institutions. The influence of these corporations in the public sphere — often without proper transparency or accountability — poses a significant challenge to the maintenance of free, fair societies (Morozov, 2018).

The dominance of big tech companies in the technology market is undeniable. Major corporations such as Google, Amazon, Facebook, and Apple — here referenced by their commonly known names, although they operate under broader corporate conglomerates — not only control a substantial share of the global technology market but also play a pivotal role in shaping economic and social standards. The power exercised by these companies is

subtle yet deeply embedded in daily behavior, making them even more influential. Through algorithms and digital platforms, they shape everything from consumption patterns to perceptions of reality, establishing a new form of power — psychopower — that is difficult to challenge or regulate (Han, 2022, p. 2).

Thus, technological solutions — far from being a panacea — often serve to consolidate power in the hands of a few, exacerbating inequality and technological dependency. With their vast economic and technological might, big tech companies set the rules of the data market, influencing public policy and business practices, frequently to the detriment of fundamental individual and collective rights (Zuboff, 2019, p. 14-15). In this context, examining the business models of big tech firms and analyzing their dominance and influence reveals the extent to which these entities shape not only markets but entire societies.

This influence extends to the legislative arena, where intensive lobbying by such corporations can distort the creation of public policies and regulations, favoring private interests over the common good. Their ability to operate across multiple jurisdictions — often employing strategies to minimize tax and regulatory obligations — places them at a significant advantage over states. The concentration of power in the hands of a few companies creates an oligopolized digital ecosystem, where innovation and diversity may be stifled by anticompetitive practices.

Furthermore, the influence of big tech companies in the information sphere is particularly concerning, as their control over social media platforms, search engines, and other online tools and applications places them in a privileged position to shape public discourse and opinion formation (Han, 2018, p. 23-24). This raises critical concerns about election manipulation, the spread of disinformation, and the erosion of trust in democratic institutions, in what O'Neil (2020) refers to as potential "weapons of math destruction."

Assuming that regulatory diversity reflects global dynamics, it is essential to view the evolution of regulatory frameworks as a continuous process of adaptation and engagement with social complexity. Privacy and the protection of personal data are in constant flux, reshaped by ongoing technological innovations and evolving societal perceptions of private life and digital security (Pérez-Luño, 2012, p. 93). This evolution is crucial to maintaining the relevance of regulatory frameworks in a world where data has become an extremely valuable commodity — especially in the context of artificial intelligence (Hoch; Engelmann, 2023, p. 11-12).

The development of data protection regulations often follows a reactive pattern, where new laws and guidelines are introduced in response to data breaches, disruptive technological advances, or shifts in consumer behavior (Pessoa, 2020, p. 83-85). Although this response cycle is necessary, it presents legislators with the challenge of striking a balance between user protection and the promotion of innovation. Regulations must be robust enough to ensure the security of personal data and flexible enough to adapt to future scenarios that have yet to be fully envisioned — particularly given the social complexity mediated by information and communication technologies.

Since the importance of privacy, it becomes essential to recognize algorithms as agents of social interpretation and to understand metadata as safeguards of both individual and collective freedom. These reflections underscore the urgent need for policies aligned with democratic principles in the context of digital society. In this scenario of technological surveillance, privacy — and particularly the right to personal data protection — gains prominence as a means of defending human dignity and ensuring collective protection (Limberger, 2009, p. 46-47).

A paradigm shift is thus evident, marked by a "reinterpretation of concepts shaped by the mass flow of information, encompassing new dimensions of the right to secrecy, the right to intimacy, the right to private and family life, the right to informational self-determination, and the right to personal data protection" (Pessoa, 2020, p. 85). With this new perspective, despite predictions about the "end of privacy at the close of the twentieth century," attempts have been made to reconceptualize the right to privacy beyond the rigid and static norms of closed legal texts, toward a more open, dynamic, and fluid interpretation suited to technological society (Pérez-Luño, 2012, p. 93).

Regarding the protection of personal data, a long and evolving regulatory process can be identified, commonly divided into four legislative phases (Doneda, 2011, p. 96). The first phase, based on the state of the art in technology, introduced rules requiring user authorization and consent for the creation and maintenance of structured databases, as well as regulating the role of public authorities in handling collected information. The second phase, in response to the growing use of databases, established regulations that framed privacy as a negative liberty, enabling individuals to restrict or deny public authorities' access to their personal data.

By the 1980s, in response to the growing need to regulate the processing of personal data within the information flows of a global economy, the third legislative phase moved beyond the narrow view that mere authorization or consent was sufficient for activities

involving personal information, emphasizing the principle of informational self-determination. Finally, the fourth legislative phase — representing the current stage — recognizes that privacy cannot be reduced to a purely individual choice. Instead, it must be framed through the creation of collective norms, establishing guarantees and rights for data subjects. This allows for a shift beyond consent, especially in light of the new possibilities for data processing and the clear imbalance in legal relationships between entities and users, highlighting the importance of independent authorities to ensure public oversight of data processing in society.

Nevertheless, the current landscape remains characterized by increasingly pervasive surveillance mechanisms targeting data subjects — through the collection and processing of both personal and non-personal data — to sustain a new information-based socioeconomic order and a decentralized surveillance infrastructure (Pessoa; Oliveira, 2019, p. 11). In this context, the regulation of the right to privacy must account for global and transnational information flows, treating data as economic assets and sources of advertising revenue — hallmarks of a new phase of capitalism.

There is a "need to conceptualize regulation within a society shaped by surveillance, which requires not only the adoption of legal instruments to protect data and information, but also the use of any tools or techniques capable of producing regulatory effects" (Rodriguez, 2021, p. 116). Notably, "implementing such measures may, at times, require acceptance of certain forms of positive virtual surveillance, guided by principles and guarantees related to the protection of information transferred across the material and immaterial domains of society" (Rodriguez, 2021, p. 116).

In this context, if privacy protection becomes subordinated to economic interests and technological advances — particularly under a model of regulated self-regulation by the market — it is worth questioning whether there is a genuine commitment from state and corporate actors to uphold this right. This concern arises from the fact that power networks tend to eliminate legal gaps and relativize normative boundaries in favor of advertising and profit (Rodotà, 2008, p. 105). Thus, relegating data protection to self-regulation, or to a lack of regulation altogether, risks reducing privacy to a mere commodity within a globalized market focused on the exploitation of surveillance-based economic assets, a logic that is fundamentally incompatible with the protection of fundamental rights tied to human personality.

The evolution of regulatory frameworks, which culminates in the design and implementation of data protection legislation, brings to the forefront the definition of key principles and rights that must be guaranteed to data subjects. These principles form the backbone of effective regulation, guiding the practices of both public and private entities and ensuring that citizens' interests are safeguarded in an increasingly intrusive digital environment.

The rights typically guaranteed by such laws include—but are not limited to—the right to access, rectify, erase, and port data, as well as the right to contest automated decisions and to be informed about data collection and usage. The inclusion of principles such as data minimization, purpose limitation, and transparency in data operations ensures that data controllers not only comply with legal obligations but also adopt ethical and responsible practices. These principles now serve as the foundation for the exercise of digital autonomy, enabling individuals to maintain control over their personal information and protect themselves from misuse, following a logic of "person–information–control–circulation" (Rodotà, 2008, p. 93).

In this regard, special attention must be paid to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which repeals Directive 95/46/EC. Commonly known as the GDPR, this legal instrument introduced a new regulatory framework for personal data protection within the European Union. It requires a proactive, conscious, diligent, and accountable posture from data controllers—one based on risk assessment and mitigation, and the adoption of administrative and technical safeguards to protect data subjects' rights, while also emphasizing best practices and privacy policies (União Europeia, 2016).

The GDPR ultimately transcends the territorial limits of the European Union by establishing conditions for its applicability regardless of the location where data is processed, the nationality of the data subject, or the domicile of the data controller. As a result, several countries outside the European Union have found themselves needing to align their national data protection frameworks with European standards — an effect widely referred to as "Europeanization" or the "Brussels Effect" (Bradford, 2012). This phenomenon is further reinforced by provisions within the GDPR that address international cooperation and impose restrictions on cross-border data flows. The European Union grants adequacy decisions to third countries that offer an adequate level of personal data protection, thereby enabling

continued commercial interactions and international data transfers (Pessoa; Limberger; Saldanha, 2023).

This reflects a dual perspective, as personal data protection regulation "on the one hand, seeks to protect individuals with regard to the processing of their personal data; on the other, it plays a role in fostering commerce by establishing common data protection standards across the region." In this sense, "the demands of a unified market such as the European Union, in its effort to broadly reduce transaction costs, include harmonizing rules concerning personal data" globally — particularly due to the EU's economic prominence (Doneda, 2011, p. 102).

The development of oversight mechanisms and the imposition of sanctions, as outlined in data protection frameworks, underscore the seriousness and commitment of legal systems to safeguarding the right to personal data protection. However, when such regulatory structures are exported beyond their original jurisdictions, they raise the issue of regulatory imperialism. By positioning the GDPR as an international standard, the European Union once again asserts itself as an exporter of regulatory norms — something that may be interpreted as an extension of its geopolitical influence.

This phenomenon of normative projection is not without criticism, especially when viewed from the perspective of nations on the periphery of the data capitalism system. The adoption of foreign regulatory frameworks is often carried out without the necessary adaptation to local contexts, potentially resulting in misaligned rules that fail to reflect the needs and particularities of other societies. This can lead to a paradoxical situation in which, rather than empowering data subjects, regulation ends up reinforcing technological and normative dependency.

The notion of regulatory imperialism also invokes broader debates concerning power imbalances within the global governance of data. While the GDPR offers a comprehensive framework of rights and protections for residents of the European Union, its adoption as a global standard may constrain regulatory innovation in other regions and perpetuate a center–periphery dynamic. Core countries define the rules that peripheral countries are expected to follow, thereby reproducing new forms of colonialism (Silveira, 2021, p. 33-52).

Within the context of regulatory imperialism, local adaptation and resistance emerge as essential counterpoints. These dynamics reveal the capacity and initiative of countries to develop their own interpretations of international — or even national or regional — norms that have extended beyond their original territorial boundaries, adapting them to their own sociopolitical, economic, and cultural realities. This process exemplifies the broader struggle

to maintain national sovereignty in the digital age, reinforcing the need for a data governance framework that is both globally informed and locally grounded.

3 On Digital Colonialism and the Emancipation of the Right to Personal Data Protection

The free flow of personal data is a foundational condition for the operation of data-driven products and services, enabling big tech companies (e.g., Google, Facebook, and Apple) to thrive in a borderless market by massively capitalizing on the continuous and unrestricted global flow of information. This is why the term "platform capitalism" is frequently used to describe this dynamic (Srnicek, 2016; Van Dijck; Poell; De Waal, 2018). This digital era, often referred to as the "new oil economy," has seen data transformed into an essential commodity for sustaining and expanding the economic power of tech giants (Zuboff, 2019, p. 14-15).

Moreover, the increasing value of personal data and its conversion into economic assets raises important concerns regarding wealth distribution and social equity. The disparity between those who generate data and those who ultimately benefit from its economic value reflects and intensifies preexisting inequalities within society. As currently structured, data capitalism appears to disproportionately favor capital accumulation by corporations equipped with the capacity and resources to process and monetize information (Cassino, 2021, p. 13-32).

Control over personal data, in turn, implies not only the ability to influence market behavior and economic trends but also the power to shape discourse, public opinion, and, ultimately, democracy itself (Han, 2022, p. 8-10). The treatment of personal data as a commodity has profound implications for informational self-determination, where the perceived ability of individuals to control their own data may in fact be a rhetorical illusion (Pessoa, 2020, p. 92-95).

In this context, while the implementation of data protection laws and regulations is essential for safeguarding privacy, it may inadvertently consolidate the power of entities already operating from a position of significant advantage in the digital space and data economy. The central issue lies in how data protection policies, rather than democratizing control over information, may actually reinforce existing inequalities — particularly because

such legislation is often accompanied by intense lobbying efforts that benefit large corporations.

Some scholars argue that regulatory frameworks have the potential to create market entry barriers in the data economy, favoring well-established tech conglomerates that possess the necessary resources to navigate the complex legal and technical landscape (Silveira, 2021, p. 33-52). Armed with advanced infrastructure and substantial capital, these corporations are better equipped to comply with regulatory demands, whereas startups and smaller firms face significant challenges. This not only strengthens the dominant position of major players but also restricts innovation and competition — both of which are essential for a healthy, sustainable market.

As regulatory environments become stricter in some regions compared to others, there is a growing trend of data industry centralization in areas with more permissive legal frameworks or more developed infrastructures, while data exploitation itself occurs on a global scale (Faustino; Lippold, 2023; Silveira, 2021; Cassino, 2021). This phenomenon not only reinforces the hegemony of certain countries and regions but may also result in a new form of digital dependency for those situated outside the dominant technological hubs.

The paradox is that regulation — designed to protect users — may, under data capitalism, inadvertently legitimize the power of big tech companies by authorizing data collection under specific conditions or through the assumption of informed, voluntary consent. In other words, the complexity of data protection regulations may, contrary to their intended purpose, serve to reinforce the very structures of data capitalism — especially within a global context driven by the free flow of data and the transnational transfer of digital assets.

The transformation from the "person–information–secrecy" paradigm to a "person–information–control–circulation" model — particularly marked by the advent of the European Union's GDPR and similar legislation — represented a milestone in attempts to regulate the processing of personal data. However, despite its emancipatory potential and its aim to empower users, such regulations may in practice endorse the data accumulation model by imposing compliance requirements that dominant corporations can easily absorb or circumvent, thereby reinforcing their market dominance.

Current regulations, even when stringent, often fail to dismantle the power infrastructures that sustain this economic model. Data collection, when permitted under specific regulatory conditions (e.g., informed consent) may be interpreted by companies as a green light to continue their practices, now under the guise of legal compliance, particularly

given that terms and conditions often resemble adhesion contracts, rarely read or fully understood by users (Sujeito a termos [...], 2013).

Indeed, although data protection regulations refer to users as “data subjects,” they may in fact reinforce the power of big techs by failing to address the issue of data ownership. These regulations tend to emphasize privacy protection and data security, involving the user in the process without questioning who ultimately owns — and therefore profits from — those data. This omission has significant consequences for market competition and innovation (Morozov, 2018, p. 146-147).

Moreover, the international transfer of data — an essential component in the consolidation of data capitalism — is often addressed in ways that further entrench this phenomenon. Regulations typically allow the free flow of these digital assets, even without the data subject’s consent, as long as the destination country ensures an “adequate level” of data protection — typically interpreted as equivalent regulation — or meets certain conditions, such as standardized contractual clauses or global corporate rules.

The issue of data colonialism emerges as regulatory frameworks often fail to consider the disparities between countries regarding their ability to collect, process, and monetize data. This may lead to a form of digital colonialism, wherein wealthier nations impose their standards and extract value from data generated in developing countries, thereby exacerbating existing inequalities (Faustino; Lippold, 2023; Silveira, 2021; Cassino, 2021).

The phenomenon of digital colonialism in the Global South represents one of the most problematic dimensions of the contemporary data economy. The dynamic between developed nations of the Global North and developing countries of the Global South establishes a form of neocolonialism in which data become the new domain of extraction and domination. Corporations from the North — often represented by big tech companies — possess the capacity and power to extract value from the data generated by users in the Global South, perpetuating historical inequalities and creating new forms of economic and technological dependence (Harari, 2024, p. 485-491).

The concept of data colonialism is essential for understanding digital extractivism which can be seen as a continuation of colonial practices. Big techs not only collect vast amounts of data but also control the means to process and monetize them — frequently without offering fair compensation or contributing to local development. This creates a scenario in which countries in the Global South serve merely as providers of digital raw material to be refined by advanced economies. The concept describes a reality where large

technological conglomerates act as digital prospectors, exploiting personal data as if it were an inexhaustible natural resource, with little regard for ethical implications or the depletion of privacy reserves.

Amid the intensification of surveillance capitalism as a new logic of accumulation — based on predicting and modifying human behavior — data extracted from the Global South becomes a tool for refining algorithms and technologies that, paradoxically, are often unavailable or inaccessible to local populations. This exacerbates both technological and economic inequalities. In the data economy, such asymmetries are clear: "Technology producers care little about consumers in the Global South, except when receiving feedback to improve their own products or in pursuit of profitable niche markets" (Cassino, 2021, p. 29).

Digital colonialism transforms data into a highly desirable, controllable resource whose access and use are determined by a small number of powerful actors — predominantly located in the Global North. Conversely, informational asymmetry reinforces a mindset of technical alienation in which there is an "active ignorance regarding how networks of technological creation, development, and usage function, sustained by the belief that there is no importance in understanding or mastering technological processes locally" (Silveira, 2021, p. 45).

In this context, certain issues are obscured by a colonial mindset, such as: "the questioning of the belief that digital companies and platforms are neutral and do not interfere in our daily lives, except to serve us"; furthermore, "the interrogation of the notion that the use of technological platform structures has no negative local or national consequences, assuming that they merely comply with contractual terms"; also, "the assumption that the economic, political, and socially modulatory effects of massive data collection in the central countries of platformization are equivalent to those in peripheral countries"; and finally, "the inquiry into whether it is possible to pursue the development of local computational intelligence, algorithmic sovereignty, and technological knowledge as a shared public good" (Silveira, 2021, p. 36).

Digital colonialism is sustained by a business model that views data not merely as an asset but as a primary resource for the development of new products, services, and competitive advantages. Mass data collection becomes a corporate imperative, where user consent is often reduced to a mere formality (Pessoa, 2018, p. 92). This continuous harvesting of detailed information about behaviors, preferences, and social relationships transforms human experience into a commodity — a source of profit.

The link between data extraction and economic power is reinforced by technological "awe" and the apparent gratuity of innovation, which often conceals the asymmetries and exploitations inherent in the data economy. As such, the infrastructure of the internet and digital platforms, controlled by big tech companies, fosters an unequal distribution of the benefits derived from global data traffic. While individuals generate data that fuel corporate profit engines, they rarely share in the resulting economic gains.

This dynamic of digital colonialism also reflects and amplifies geopolitical inequalities. Countries in the Global South — often with less stringent regulations and developing technological infrastructures, or implementing data protection laws inspired by Global North contexts — become fertile ground for data exploitation by companies based in centers of global economic and technological power. This perpetuates historical patterns of exploitation and subjugation.

Data extraction can thus be seen as an extension of colonial practices that seek not only material resources but also intellectual and cultural ones, aiming to homogenize and impose dominant values and belief systems (Fanon, 2005, p. 55-56). This imbalance underscores the urgent need to reexamine dominant business models in the tech sector and to pursue alternatives that more equitably distribute the benefits of the digital world to those who provide its raw material: personal data (Faustino, 2023, p. 53-55).

Analyzing technological innovation as a counterpoint to digital colonialism leads to a consideration of the relevance of data protection legislation. In this context, the GDPR appears to endorse digital colonialism when it states that the free movement of personal data within the European Union is not restricted or prohibited for reasons related to the protection of individuals with regard to the processing of personal data (União Europeia, 2016).

Notably, several countries have drawn inspiration from the European Union to develop their own privacy frameworks, adopting data protection standards similar to those set out in the GDPR. One of the requirements established by the GDPR for cross-border data flows is the necessity of an adequacy decision, determined by the European Commission. This has led many countries — including Brazil, Argentina, Uruguay, New Zealand, Japan, and even China — to align their regulatory frameworks with the European model (Pessoa; Limberger; Saldanha, 2023, p. 177-178).

In Brazil, Law No. 13.709/2018, known as the LGPD, represents a significant step forward in Brazilian legislation concerning the right to personal data protection. Inspired by the GDPR, the LGPD reflects this influence and constitutes an effort to align the country with

international privacy and data protection standards within the broader context of data capitalism (Brasil, 2018).

However, although the LGPD represents a foundational milestone in establishing a legal regime for data protection — aiming to empower users with control over their information — it must also be critically examined (Sarlet, 2021, p. 16-22). Despite the enthusiasm from some sectors regarding its alignment with the European regulatory model and Brazil's perceived advancement in privacy protection, the LGPD faces unique challenges. These challenges stem not only from issues of privacy and technology but also from broader structural inequalities and the complexities of data capitalism and digital colonialism in the Brazilian socio-economic context.

In the context of the Global South, the evolution of regulatory frameworks must take into account the risk of implementing decontextualized regulations that fail to reflect the specific realities of the region (Dussel, 2009). Striking a balance between adapting international best practices and developing innovative solutions tailored to local needs is a pressing challenge. It is therefore essential to question how the evolution of regulatory frameworks can influence not only the protection and processing of personal data but also the power and control that individuals hold over their digital information.

O desafio para os países do Sul Global é, portanto, duplo: por um lado, devem buscar a proteção dos dados pessoais de seus cidadãos, o que muitas vezes significa alinhar-se aos padrões internacionais, normas corporativas globais e padrões técnicos comuns; por outro lado, devem manter sua soberania e a capacidade de promover o desenvolvimento econômico e tecnológico de acordo com seus próprios termos, sem sucumbir à pressão de se conformar a um modelo que pode não ser totalmente adequado às suas realidades.

South–South cooperation also plays a vital role in this context, enabling developing countries to share knowledge, experiences, and strategies regarding data protection and privacy. This exchange can strengthen these countries' positions in international negotiations and policymaking, while also fostering an alternative vision that contrasts with the dominant narrative of the Global North. By addressing local needs and particularities, data policies can be reshaped to empower citizens, support the growth of native technologies, and promote a digital ecosystem that is both inclusive and representative.

Resisting externally imposed data regulation models does not mean rejecting the underlying values of data protection and privacy. On the contrary, it involves engaging in a critical dialogue with these models, questioning and reshaping them in ways that enhance

local capacities and promote digital autonomy. Thus, the right to personal data protection in the context of data capitalism and digital colonialism is not merely an economic issue but also one of social justice and human rights.

The right to personal data protection, as both a legal concept and a regulatory practice, has taken on a global dimension, primarily influenced by models developed in the Global North, such as the GDPR. However, when it comes to countries in the Global South, it is crucial to recognize that simply importing regulatory frameworks conceived in different realities may not suffice to address local specificities and the challenges posed by data capitalism and digital colonialism (Pessoa; Limberger; Saldanha, 2023, p. 177-179).

There is a need to explore the emancipation of the right to personal data protection in Global South countries through a decolonial and context-sensitive approach to technological advances. This notion suggests that the right to data protection must be transformed to reflect the unique socioeconomic, political, and cultural dynamics of these countries. Rather than being an imported and imposed concept, it should evolve into an instrument of empowerment and autonomy.

The emancipation of the right to data protection, therefore, involves the creation of regulatory frameworks that not only shield individuals from abuses in the collection and use of their data, but also promote the digital sovereignty of Global South countries. This means developing policies that enable these nations to exercise control over their data, ensuring that it is used in ways that benefit their own societies and economies, rather than serving only foreign corporations or the interests of the Global North.

In the Global South, the right to data protection should be understood as a dynamic, adaptable right that can withstand the pressures of digital colonialism and address the social inequalities generated by data capitalism. This calls for a critical perspective that challenges the assumptions underlying imported regulatory models and seeks, through law, to rebalance power within the global data economy.

4 Conclusion

The emergence of data capitalism represents a defining phenomenon of the contemporary digital era, reshaping the paradigm through which personal information is regulated, shared, processed, and monetized. The critical analysis developed in this article enabled a comprehensive exploration of a system that, inspired by regulatory models such as

the European Union's GDPR, may inadvertently reinforce unbalanced power dynamics, thus characterizing a form of digital neocolonialism.

What can be observed is the rise and consolidation of a data capitalism dominated by big tech companies — built upon the collection, processing, sharing, and commercialization of personal information — which often evades the protective intentions behind data protection frameworks. The European model, exemplified by the GDPR and widely adopted as a global regulatory reference, despite its aim to protect individuals, may fall short in addressing the complexities and specific needs of diverse socio-political and economic contexts, particularly in the Global South.

Thus, the current regulatory model, heavily influenced by the GDPR and centered on the free flow of data, ultimately reinforces and legitimizes data capitalism. The notion of user control over personal data proves illusory within a digital economy dominated by big tech platforms. The analysis of Brazil's LGPD highlighted how this legislation, though aligned with the European trend, offers an opportunity for critical reflection and adaptation to local realities — especially in the face of digital colonialism.

In other words, Brazil's data protection framework, by mirroring the European regulation, risks replicating the practices of data capitalism and digital colonialism. However, such adoption is not necessarily irreversible, as the LGPD can serve as a foundation for interpretation beyond mere imitation, fostering a more balanced dialogue between data protection and socioeconomic realities.

This points to the need for a decolonial vision — one that reclaims autonomy and promotes digital sovereignty across Global South countries. In this sense, the emancipation of the right to data protection emerges not only as a challenge but as an urgent and necessary action to ensure that privacy becomes a genuine instrument of social and economic empowerment, capable of resisting the pressures of data capitalism and the evolving expressions of digital colonialism.

References

BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013.

BRADFORD, Anu. The Brussels Effect. **NorthWestern University Law Review**, [*S. l.*], v. 107, n. 1, p. 1-68, 2012. Disponível em: https://scholarship.law.columbia.edu/faculty_scholarship/271. Acesso em: 10 dez. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 13 dez. 2023.

CASSINO, João Francisco. O sul global e os desafios pós-coloniais na era digital. *In*: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da. (org.). **Colonialismo de dados:** como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia literária, 2021. p. 13-32.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico,** Chapecó, v. 12, n. 2, p. 91-110, jul./dez., 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 01 dez. 2023.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006.

DUSSEL, Enrique. Meditações anti-cartesianas sobre a origem do anti-discurso filosófico da modernidade. *In*: SANTOS, Boaventura de Sousa; MENESES, Maria Paula. **Epistemologias do Sul.** Coimbra: Edições Almedina, 2009. p. 283-336.

FANON, Frantz. **Os condenados da terra.** Juiz de Fora: UFJF, 2005.

FAUSTINO, Deivison; LIPPOLD, Faustino. **Colonialismo digital:** por uma crítica hacker-fanoniana. São Paulo: Boitempo, 2023.

HAN, Byung-Chul. **Infocracia**: digitalização e a crise da democracia. Petrópolis: Vozes, 2022.

HARARI, Yuval Noah. **Homo Deus**: uma breve história do amanhã. São Paulo: Schwarcz, 2015.

HARARI, Yuval Noah. **Nexus**: uma breve história das redes de informação, da Idade da Pedra à inteligência artificial. São Paulo: Companhia das Letras, 2024.

HOCH, Patrícia Adriani; ENGELMANN, Wilson. Regulação da inteligência artificial no Judiciário brasileiro e europeu. **Pensar, Revista de Ciências Jurídicas**, Fortaleza, v. 28, n. 4, p. 1-18, out./dez. 2023. DOI: https://doi.org/10.5020/2317-2150.2023.14263

HUI, Yuk. **Tecnodiversidade**. São Paulo: Ubu, 2020.

LIMBERGER, Têmis. Da evolução do direito de ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos,** Itajaí, v. 14, n. 2, p. 27-53, 2009. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/1767/1407. Acesso em: 13 dez. 2023.

MAYER-SCHÖNBERGER, Viktor. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (org.). **Technology and privacy**: The new landscape. Cambridge: MIT Press, 1997. Chapter 8. *E-book*. DOI: https://doi.org/10.7551/mitpress/6682.003.0010

MOROZOV, Evgeny. **Big Tech.** São Paulo: Ubu, 2018.

O'NEIL, Cathy. **Algoritmos de destruição em massa:** como o *big data* aumenta a desigualdade e ameaça à democracia. Santo André: Rua do Sabão, 2020.

PÉREZ-LUÑO, Antonio Enrique. **Los derechos en la sociedad tecnológica.** Madri: Editorial Universitas, S.A., 2012.

PÉREZ-LUÑO, Antonio-Enrique. **Derechos humanos, Estado de Derecho y Constitución.** 9. ed. Madri: Editorial Tecnos, 2005.

PESSOA, João Pedro Seefeldt Pessoa; LIMBERGER, Têmis; SALDANHA, Jânia Maria Lopes. A proteção de dados pessoais entre capitalismo de vigilância e cosmopolitismo. **Revista da Faculdade Mineira de Direito**, Belo Horizonte, v. 26, n. 52, p. 156-185, 2023. Disponível em: https://periodicos.pucminas.br/index.php/Direito/article/view/30789. Acesso em: 27 dez. 2023.

PESSOA, João Pedro Seefeldt Pessoa; OLIVEIRA, Rafael dos Santos de. "Big Brother Watch and Others v. The United Kingdom": el regimen de vigilancia social y el derecho al respect a la vida privada y familiar y a la libertad de expresión frente a la Corte Europea de Derechos Humanos. **Pensar, Revista de Ciências Jurídicas**, Fortaleza, v. 24, n. 3, pp. 1-12, jul./set. 2019. DOI: https://doi.org/10.5020/2317-2150.2019.9528

PESSOA, João Pedro Seefeldt. **O Efeito Orwell na sociedade em rede:** cibersegurança, regime global de vigilância social e direito à privacidade no século XXI. Porto Alegre: Fi, 2020. Disponível em: https://www.editorafi.org/073orwell. Acesso em: 02 dez. 2023.

RODOTÀ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIGUEZ, Daniel Piñero. **O direito fundamental à proteção de dados:** vigilância, privacidade e regulação. Rio de Janeiro: Renovar, 2021.

SANTOS, Boaventura de Sousa. Para além do pensamento abissal: das linhas globais a uma ecologia dos saberes. In: SANTOS, Boaventura de Sousa; MENESES, Maria Paula. **Epistemologias do Sul**. Coimbra: Edições Almedina, 2009. p. 23-72.

SARLET, Ingo Wolfgang. O direito fundamental à proteção de dados pessoais na Constituição Federal Brasileira de 1988. **Revista Privacidade e Proteção de Dados,** [*S. l.*], v. 1, n. 1, p.1-49, 2021. Disponível em https://repositorio.pucrs.br/dspace/handle/10923/18868. Acesso em: 13 dez. 2023.

SILVEIRA, Sérgio Amadeu da. A hipótese do colonialismo de dados e o neoliberalismo. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). **Colonialismo de dados:** como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia literária, 2021. p. 33-52.

SILVEIRA, Sergio Amadeu da. **Democracia e os códigos invisíveis***:* como os algoritmos estão modulando comportamentos e escolhas políticas. São Paulo: Edições Sesc São Paulo, 2019.

SRNICEK, Nick. **Platform Capitalism**. Cambridge: Polity Press, 2016.

SUJEITO A TERMOS e condições. Direção de Cullen Hoback. Nova Iorque: Variance Films; Hyrax Films, 2013. (80 min.), son., color.

UNIÃO EUROPEIA. Parlamento Europeu, Conselho da 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **European Union law,** Luxembourg, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679. Acesso em: 12 dez. 2023.

VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. **The platform society:** Public values in a connective world. Reino Unido: Oxford University Press, 2018.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância.** Rio de Janeiro: Intrínseca, 2019.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (Org.). **Tecnopolíticas da vigilância:** perspectivas da margem. São Paulo: Boitempo, 2018, p. 17-68.

How to cite:

PESSOA, João Pedro Seefeldt; Limberger, Têmis; Witschoreck, Pedro Victor dos Santos. The right to personal data protection at the intersection of data capitalism and digital colonialism. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 30, n. 1, p. 1-21, jan./mar. 2025. DOI: xxxx

Correspondence address:
João Pedro Seefeldt Pessoa- E-mail: jpseefeldt@gmail.com
Têmis Limberger - E-mail: temisl@unisinos.br
Pedro Victor dos Santos Witschoreck – E-mail: pedroviktor@hotmail.com