Philosophy & Technology (2024) 37:90
https://doi.org/10.1007/s13347-024-00777-1

RESEARCH ARTICLE

Datafeudalism: The Domination of Modern Societies by Big Tech Companies

Carlos Saura García[1]

Received: 28 March 2024 / Accepted: 29 June 2024 / Published online: 15 July 2024

Abstract
This article critically examines the domination exerted by big digital companies on the current social, economic, and political context of modern societies, with a particular focus on the implications for the proper functioning of democracy. The objective of this article is to introduce and develop the concept of datafeudalism, expose its emergence for the proper functioning of modern societies and democracy, and to propose courses of action to reverse this situation. To achieve this purpose, firstly, the evolution from surveillance capitalism to datafeudalism will be discussed. Secondly, the structures and operating logic of data feudalism will be analyzed. Thirdly, the harmful impacts of datafeudalism on the proper functioning of the democratic systems of the European Union will be examined. Finally, an attempt will be made to outline courses of action that will make it possible to reverse the situation of economic, social and political tyranny exercised by big digital companies through datafeudalism.

Keywords Datafeudalism · Technofeudalism · Surveillance capitalism · Digital feuds · Digital platforms · Open data · Data activism · Democracy

1 Introduction

Over the past 25 years, there has been a substantial increase in the power of the big United States (US) technology companies, commonly referred as GAMAMs (Google, Amazon, Meta, Apple, and Microsoft). This growth is evident in the ranking of the top five companies worldwide by market capitalization. In the 1999, 2004 and 2009 rankings, only Microsoft was listed. In 2014 Microsoft was joined by Apple and Google, and finally in 2019, the five big US technology companies were in the

✉ Carlos Saura García
saurac@uji.es

[1] Department of Philosophy and Sociology, Universitat Jaume I de Castelló, Castelló, Spain

top five worldwide (Economic Research Council, 2019). It is worth noting that in the ranking for this year, the big Chinese technology companies Alibaba and Tencent have taken positions seven and eight.

In relation to this data, at the beginning of the second decade of the 21st century, Lanier (2011, 2013) already anticipated that wealth was becoming increasingly concentrated around a small group of big technology companies with the ability to extract, control, store, and exploit large datasets. He also predicted that the burgeoning information economy under construction could end up becoming a new form of feudalism. This new reality has led to a monopolization of cyberspace and a progressive increase in the dominance of big technological companies over modern societies, which has resulted in a new form of economic and political tyranny that degrades and oppresses governments, markets, and society itself (Lanier, 2011, 2013; Srnicek, 2016; Webb, 2019; Zuboff, 2019; Durand, 2020; Hawley, 2021; Varoufakis, 2023). Zuboff (2019) coined the term "surveillance capitalism" to describe the new logic of domination by big tech companies[1]. Zuboff (2019) defines this system as a new form of tyranny exercised by big digital companies, based firstly on cyber-physical ecosystems that constantly extract and analyze large amounts of data, secondly on tools and mechanisms for predicting and modifying human behavior, and finally on a system of massive social surveillance. Simultaneously, scholars such as Posner and Weyl (2018), Mazzucato (2019), Durand (2020) and Varoufakis (2023) corroborate the predictions of Lanier (2011, 2013) and argue that various political, economic and social circumstances have caused or are causing surveillance capitalism to evolve into technofeudalism[2] or digitalfeudalism. These social systems are founded on the domination of data through the creation of digital fiefdoms and digital serfs, and the exploitation of the world's vast datasets, i.e. datafeudalism.

The aim of this article is to develop the concept of datafeudalism, to explore its negative impact on modern societies, particularly on democracy, and to propose possible courses of action. To achieve this goal, firstly, the differences between surveillance capitalism and datafeudalism will be detailed. Secondly, the characteristics and implications of datafeudalism will be analyzed. Thirdly, it will examine the pernicious effects of datafeudalism on the proper functioning of democratic systems in the European Union (EU). Finally, it will attempt to outline courses of action to reverse the economic, social, and political tyranny exercised by big digital companies through datafeudalism.

[1] Big tech companies refer to both big US digital companies (Google, Amazon, Meta, Apple and Microsoft) and big Chinese digital companies (Alibaba, Baidu, Huawei and Tencent).

[2] The first reference to the term technofeudalism was introduced in a role-playing manual entitled *Gurps Cyberpunk. High-tech Low-Life Roleplaying* (1990) written by the famous hacker Loyd Blankenship (Blankenship, 1990, p. 104).

2 From Surveillance Capitalism to Datafeudalism

The discovery and creation of mechanisms to exploit behavioral surplus by Google engineers and scientists and the subsequent promotion by the US government of a global structure of mass social surveillance based on the collection, sharing, and analysis of large datasets from big digital companies in the early months of the 21st century were the embryo of surveillance capitalism (Zuboff, 2019). On the one hand, behavioral surplus refers to the large datasets of people's information from cyberspace that contain a large amount of behaviors, patterns, information and singularities of each individual citizen (Zuboff, 2019). These datasets are extracted for free by digital companies through the various actions, activities and processes that each person or group of people performs through any digital device, platform or service (Mayer-Schönberger & Cukier, 2013; Mayer-Schönberger & Ramge, 2018, 2022). On the other hand, the George W. Bush administration, in the wake of the 9/11 terrorist attacks, initiated a comprehensive social surveillance program. This program was predicated on the objective of fostering the growth of big U.S. technology corporations and leveraging their vast datasets to construct a governmental pervasive global monitoring, surveillance, and control apparatus (Greenwald, 2014; Snowden, 2019)[3].

The operational logic of the so-called surveillance capitalism is based on the free and unilateral extraction and use of citizens' data by big technological companies as free raw material for its transformation into future behavioral predictions and for improving mechanisms for predicting and modifying people's behavior (Zuboff, 2019). The datafication of citizens' personal experiences gives big technological companies a large knowledge capacity, which in many cases allows them to discover patterns and peculiarities that people or groups of people do not know about themselves (Mayer-Schönberger & Cukier, 2013; Mayer-Schönberger & Ramge, 2022). This situation allows big digital companies to create large asymmetries of knowledge about citizens and to impose instrumental power based on radical indifference and radical behaviorism, the creation, development and use of means to predict and modify behavior, the abolition of the right to future time, and the degradation of individuality and the hindering of the cognitive capacities of citizens (Zuboff, 2015, 2019; Han, 2017b, 2022).

The convergence and hybridization of a series of economic, political, and social factors during the first two decades of the 21st century have been essential for the growth, consolidation, and progressive empowerment of big technological companies. Among these situations, the promotion of the so-called *Californian ideology* and the absolute freedom of big digital companies in cyberspace stand out (Barbrook & Cameron, 1996; Dyson et al., 1996), the empowerment of technological solutionism and technological inevitability (Morozov, 2011, 2019), the historical circumstances of heightened social insecurity related to terrorism, national security and public health (Snowden, 2019; Zuboff, 2019; Lyon, 2022; Varoufakis, 2023), the implementation of expansionary monetary policies since the 2008 economic crisis (Varoufakis, 2023) and the concentration and monopolization of cyber-physical

[3] It is important to note that this massive governmental social surveillance infrastructure was discovered and partially dismantled from 2013 onwards (Snowden, 2019).

spaces and digital ecosystems by big tech companies (Khan, 2017, 2019; Durand, 2020; Petit, 2020; Mayer-Schönberger & Ramge, 2022).

The outbreak of the Covid19 pandemic in 2020, combined with the aforementioned economic, political and social circumstances, was a turning point for the functioning of surveillance capitalism and for the dominance of big digital companies over modern societies (Varoufakis, 2023). On the one hand, the merging of real life and virtual life and the total digitization of most people's social and work activities forced by health restrictions led to an increase in the use of digital platforms and devices, resulting in an increase in big datasets and thus in the dominance of big digital companies over citizens. On the other hand, most traditional markets were forced to close and trade shifted mainly to algorithmic platforms and services, and thirdly, there was also an increase in investment in these companies from expansionary monetary policy money as the rest of the economic sectors were hit or crippled by the pandemic, and thus their technological innovation. Varoufakis (2023) argues that this set of situations provoked by Covid19 led to the transformation of surveillance capitalism into a new technofeudal system in which big digital companies constitute themselves as dominant social forces and exercise political and economic domination over social spaces and the individuals who inhabit them through the monopolization, dispossession, and depredation of large datasets.

This new system is called datafeudalism. Datafeudalism is based, on the one hand, on the dependence of states, markets and civil society on algorithmic platforms and services in which big digital companies exercise monopolistic control over data and mastery over algorithms and, on the other hand, on the instrumentalization and refeudalization of markets and civil society by big digital companies to achieve economic and political goals (Zuboff, 2019; Crouch, 2020; Durand, 2020; Bremmer, 2021; Varoufakis, 2023; Staab, 2024)[4].

The main differences between datafeudalism and surveillance capitalism can be analyzed in four principal aspects: three pertaining to socioeconomic factors and one pertaining to political considerations. The first socioeconomic aspect is the total hybridization of the functioning of modern societies with the datafication, algorithmic domination and automation of the mechanisms of prediction and behavioral modification exercised by big tech companies not only on the activities of users within their platforms, but also on workers and markets, leading to the creation of feudal relations of dispossession, predation, domination, servitude and vassalage between big tech companies and the different actors in modern societies (Mayer-Schönberger & Ramge, 2018, 2022; Durand, 2020; Teachout, 2020; Varoufakis, 2023)[5].

[4] It is important to highlight that there are two different models of operation within big digital companies (Saura García, 2024). On the one hand, there is the instrumentalist model of the big US companies based on the exploitation of citizens' behavior in order to gain knowledge that allows them to control, commercialize and monetize social learning and the mechanisms of prediction and behavioral modification and thus increasing their economic income. On the other hand, the authoritarian model of China's big companies, controlled by the Chinese Communist Party, seeks to limit, sacrifice, shape and dominate the behavioral freedom of the citizens in order to apply and disseminate China's culture, ideology and values in various forms and intensities and to protect China's security and strategic objectives.

[5] Firstly, there is a relationship of servitude of citizens to big digital companies, as they are the ones who produce the large datasets in exchange for the algorithmic services offered by big tech companies (Posner & Weyl, 2018; Durand, 2020). Secondly, there is a relationship of dispossession and predation

The second aspect relates to the creation and expansion of ubiquitous digital platforms and services and their constitution as digital fiefdoms (Durand, 2020; Varoufakis, 2023). On the one hand, the expansion of big tech platforms and algorithmic services to encompass practically all the activities of modern societies in terms of the state, market, and civil society, with the capacity to penetrate the public, private and intimate activities and behaviors of each individual. On the other hand, the constitution of large digital fiefdoms consisting of all the platforms and algorithmic services of each of the big tech companies, based on the centralized exploitation of large amounts of behavioral surplus data.

The third and last socioeconomic aspect has to do with the elimination of any kind of competition and the domination of modern societies by big digital companies as a result of the acceleration and hybridization of cyberspace monopolization, investment monopolization, intellectual monopolization, knowledge asymmetries and economies of scale and scope in the dispossession, predation and exploitation of large datasets (Srnicek, 2016; Zuboff, 2019; Crouch, 2020; Durand, 2020; Schwartz, 2022; Wörsdörfer, 2022b; Varoufakis, 2023). The increase in anticompetitive business practices carried out by big digital companies, including structural dominance, leveraging, gatekeeping, self-preferencing, copycat expropriations, discriminatory platform access, predatory pricing, and monopsony power, in conjunction with governmental permissiveness, has been a significant factor in the elimination of competition and the domination of markets by big digital companies (Wörsdörfer, 2022a, b).

In addition to the socioeconomic aspects, it is also necessary to consider the political influence that big technology companies have managed to exert in political and legislative processes and decisions. Over the past decade, big technology companies have dramatically increased their spending on lobbying in political and legislative decision-making, have expanded the number of meetings between their top executives and presidents and senior state officials, and have created revolving door systems between governments, government agencies and big digital companies (Zuboff, 2019; Wörsdörfer, 2020). This situation has resulted in a phenomenon known as "regulatory capture," in which government regulatory agencies are dominated by the very industries they are meant to regulate (Taplin, 2017; Meghani, 2021; Taylor, 2021). This occurs in order to protect the interests of the industries in question and to ensure that their activities and expansion are not hindered.

The introduction of this datafeudal system in modern societies has succeeded in institutionalizing big tech's algorithmic political and economic domination of consumers, workers, markets, governments, social spaces, and the individuals who inhabit them through the feudalization of digital platforms and services, the instrumentalization of their users and the domination of the large datasets they produce.

over big data sets and domination over the activities of states, markets and civil society (Zuboff, 2019; Durand, 2020). Thirdly, there is a relationship of vassalage between the powers that be, governments, political actors and big digital companies, as the former seek to acquire and use the knowledge and tools of big digital companies for various economic and political purposes (Moore, 2018; Da Empoli, 2019; Snowden, 2019).

3 Datafeudalism: Digital Fiefdoms, Digital Serfs, and Identity Ownership

The overlap and hybridization of real and virtual life, and the digitization of the vast majority of citizens' social and work activities have led to a total datafication of modern societies that encompasses all areas of life (Mayer-Schönberger & Cukier, 2013; Van Dijck, 2014; Mayer-Schönberger & Ramge, 2022). In relation to this issue, Calvo (2019) notes that this trend has been made possible by the potential of the Internet of Things (IoT), the development of which has allowed the convergence of the diverse and versatile application technologies that make it possible — Key Enabling Technologies (KETs), Artificial Intelligence (AI), and Big Data (BD) — as well as its application in the different spheres of the human activity.

The aforementioned technologies have enabled the datafication of human activity ranging from marketplace transactions, online commerce, and real-life commerce (Mayer-Schönberger & Ramge, 2018), activities and behaviors during working hours (Kim, 2018; Varoufakis, 2023), navigation and movements on platforms and in the network (Bashyakaria et al., 2019; Aral, 2021), information related to smartwatches, smartphones and smart vehicles (Thompson and Warzel, 2019), interactions with digital devices such as virtual assistants, smart TVs, refrigerators, microwaves, vacuum cleaners, smart lights or toilets (Fowler, 2022) to the datafication of the iris of the eye or people's ideas, reactions, reflections, ruminations and memories of people by monitoring brain and body activity (Farahany, 2023).

The convergence of real and virtual life, social and labor digitalization, and mass datafication has given rise to a digital panopticon (Han, 2017a), which is based on the ideas of Bentham (1787) and Foucault (1975). This digital panopticon is managed and dominated by big digital companies through digital fiefdoms. The digital panopticon is a flexible, intelligent, silent, and practically imperceptible mass social surveillance structure that allows big digital companies to have an omnipresent and prospective vision of modern societies and to record and observe all movements, actions, and behaviors of every person, collective, or organization simultaneously, thereby creating an illusion of total freedom (Han, 2017a).

The operational logic of datafeudalism is a predatory development of the logic of surveillance capitalism. It is based on two fundamental elements: the creation of so-called digital fiefdoms — the private cyber-physical ecosystems where datafication takes place — and the encapsulation, oppression, and domination of the digital serfs — the entity that produces the big datasets — within these digital fiefdoms.

Digital fiefdoms are conglomerates of digital platforms and services owned by big digital companies, which modern societies depend on for their proper functioning (Durand, 2020; Varoufakis, 2023). In these digital fiefdoms, digital serfs are encapsulated, and their movements and activities create large datasets that are preyed upon. The analysis and exploitation of varied datasets are centralized, and the mechanisms of prediction and behavioral modification are applied[6]. The aim of digital fiefdoms is

[6] Two clear examples of digital fiefdoms can be seen in the Meta and Amazon conglomerates. On the one hand, Meta includes various algorithmic platforms and services, such as Facebook, Instagram, WhatsApp and Threads. On the other hand, Amazon includes various algorithmic platforms and services such as

to maximize infrastructure utilization by users and make it difficult to exit from them (Lanier, 2018; Williams, 2018; Aral, 2021). This situation leaves users with only two options in the case that they want to leave a digital fiefdom: switch to another digital fiefdoms, which comes with high exit costs, or flee from digital fiefdoms altogether, resulting in total social, economic, and political marginalization (Plantin et al., 2016). Durand (2020) describes the current situation of digital fiefdoms noting that in the era of digitalization and hyperconnectivity the augmented human cannot escape the dominion of algorithms. The crystallization of social surplus in the digital fiefdoms permeates individual existences, binding them as once serfs were bound to the glebe of lordly rule. This force of the social, which emanates from human communities and shapes individuals, is objectified in big data and it is a new kind of means of production, a terrain of experience to which the subjectivities of the 21st century are attached (Durand, 2020).

The hybridization of human existence and cyber-physical ecosystems has led to dependency of individuals and organizations on the algorithmic platforms and services of big digital companies which exercise a domination over big datasets and algorithmic platforms and services, transforming their users into digital serfs (Durand, 2020; Varoufakis, 2023). Digital serfs are individuals who perform movements and activities in digital fiefdoms and who produce sets of behavioral surpluses consisting of large datasets. Once the data is produced, the serfs are dispossessed of it and end up in the data centers of the big tech companies that owns the digital fiefdom. It is important to emphasize, on the one hand, that there is no coercive force forcing this collective to perform movements or activities in the digital fiefdoms, but that they perform them — practically without being aware of it — in exchange for the use of algorithmic platforms and services (Lanier, 2018; Williams, 2018). On the other hand, serfs are no obligated to use the infrastructure of a single digital fiefdom, i.e. they can use algorithmic platforms or services of different digital fiefdoms by adapting to their terms of use and having their data taken by the corporation that manages each digital fiefdom.

The foundations that make up the datafeudal structure are threefold. First, the economic and political domination of big tech companies based on the ability to control, monitor, persuade and manipulate people's behavior and the functioning of the market, civil society and democracy through algorithmic platforms and services. Second, big tech's monopolization and domination of large datasets of digital fiefdoms. And third and finally, the exploitation of the digital serfs by big tech through the dispossession and predation of the datasets created by their movements and activities within the digital fiefdoms without recourse to coercion of any kind.

In datafeudalism as in the case of medieval feudalism, big digital companies (in the case of feudalism, the feudal lords) own the digital fiefdoms that enable modern societies to function (in the case of feudalism, the land) and profit from the movements and activities of digital serfs on their algorithmic platforms and services through behavioral surplus rents from large datasets for economic or political gain (in the case of feudalism, the corvée or payments for the usufruct of land).

Amazon.com, Amazon Alexa, Amazon Music, Amazon Prime Video, Twitch, Ring LLC or Amazon Web Services (AWS).

The vast amount of data continuously produced by the serfs of the digital fiefdoms and the centralization of the analysis and exploitation of this data gives big digital companies detailed knowledge of each person's identity.

> […] our digital identity belongs neither to us nor to the state. Strewn across countless privately owned digital realms, it has many owners, none of whom is us […] Facebook is intimately familiar with whom -and what- you like. Twitter remembers every little thought that caught your attention, every opinion that you agreed with, that made you furious, that you lingered over idly before scrolling on. Apple and Google know better than you do what you watch, read, buy, whom you meet, when and where. […] With every day that passes, some cloud-based corporation, whose owners you will never care to know, owns another aspect of your identity (Varoufakis, 2023, p. 73).

The advent of datafeudalism has given big digital companies a detailed knowledge of many aspects of people's privacy and intimacy that exceeds the knowledge that states have of their own citizens and the knowledge that people have of themselves (Coeckelbergh, 2024). Such detailed knowledge of people's privacy and intimacy has a direct negative impact on the integrity, dignity, personality, anonymity, and identity of the individuals themselves. This results in a control over the activities and actions they perform and the data emanating from these behaviors, a monitoring of the freedom of communication, a limitation of access and knowledge about oneself, and a reduction of their freedom (Wörsdörfer, 2018). In relation to the obtaining and exploitation of people's privacy and intimacy by the datafeudal system, Balibar (2019) argues that individuals are expropriated of their own existence in all phases of their life as a consequence of a "total subsumption" of it that implies a total loss of individuality.

These facts have led to the application of a domination by big tech companies, which can be understood as a form of oppression. This involves the imposition of rules and power structures on the serfs of the glebe based on the exploitation of large datasets of digital fiefdoms that causes a limitation, reduction, and manipulation of these. The structure of domination of big digital companies is based on the various dynamics that make domination possible, as outlined by Young (1990). These dynamics are the creation of asymmetric power structures, the imposition of rules and values, the limitation of freedom, and the application of dynamics of oppression (Young, 1990).

The creation of asymmetric power structures has originated from two sources: the emergence of large asymmetries of knowledge between big tech companies and the citizenry, and the development of instruments and mechanisms of behavioral modification of people that have empowered big tech companies to intervene in the sovereignty, autonomy, and self-determination of the digital serfs (Han, 2017b; Zuboff, 2019; Varoufakis, 2023; Coeckelbergh, 2024). The imposition of certain norms and values and the limitation of freedom within digital fiefdoms silences and manipulates the opinions of the serfs of the glebe and prevents them from participating fully in decision-making in social, economic, and political arenas. Finally, the application of oppressive dynamics within digital fiefdoms, such as marginalization, exploitation, powerlessness, and cultural imperialism, serves to exacerbate and amplify the

effects of big tech domination on the sovereignty, autonomy, and self-determination of digital serfs.

The concept and scenario of datafeudalism draws a parallel with a scenario previously contemplated by John Stuart Mill in the 19th century. In his work, Mill posited a scenario in which all lands within a country were owned by a single individual (Mill, 2004). He observed that this arrangement would result in a profound dependence of the country's population on this person, enabling him to impose his conditions without limitations. Such an arrangement could potentially impact the freedom of individuals, organizations, and society, as well as the principle of happiness, the principle of no-harm and the general welfare (Mill, 1977, 2004). The phenomenon of datafeudalism has brought about a situation that closely resembles the dystopian vision of a single individual owning the land, as envisioned by Mill. In this case, a small group of big digital companies has amassed control over the algorithmic platforms and services that underpin the functioning of modern societies and the extraction of the vast datasets that are generated in these environments. The dominance of algorithmic platforms and services by digital fiefdoms, as previously discussed, results in the elimination of market and citizen freedom and the monopolization of big datasets and innovation. This leaves the general welfare of society in the hands of the economic and political interests of large digital corporations.

This scenario bestows considerable power upon big technological companies to dominate the citizenry and civil society. This poses a significant threat to the citizens freedom, the public interest and the proper functioning of democratic systems. In light of the aforementioned circumstances, which have the potential to negatively impact market competition, privacy and intimate aspects of citizens' lives, as well as the sovereignty, autonomy, and self-determination of society in general, and the reversion of the general welfare, authors such as Newell (2014a, b) and van der Sloot (2018), advocate the implementation of a set of measures based on the "non-domination principle"[7] through balanced, proportional and effective government interventions that prevent these harms, ensure the reduction of domination and interference by big tech corporations, and enhance the capacity of citizens to govern themselves.

4 Negative Impacts on the Proper Functioning of Dmocracy

The characteristics and operating model of datafeudalism pose an unprecedented threat to individual and collective freedoms, with direct impactions for public interest[8] and the proper functioning of democratic systems. On the one hand, the digital platforms and algorithmic services of digital fiefdoms have become the epicenter of

[7] The principle of non-domination does not focus on concrete violations of rights or freedoms, but on power relations as such and the potential for abuse (van der Sloot, 2018). Non-domination is understood as the state in which a person is not subject to the arbitrary will of another. This means that a person is free not only when his or her actions are not interfered with, but also when he or she is not under the discretionary power of another who can interfere at will (Pettit, 1997).

[8] The public interest is defined as a moral notion that is primarily concerned with the proper conduct of political life in democracies in general and with the proper ways of making collectively binding political decisions in particular (O'Flynn, 2010).

a privatized digital public sphere that has emerged as the main support of the public sphere (Hagen et al., 2017). The privatization of the public sphere has allowed big digital companies to control, monitor and manage the information and communication flows of the public sphere, to extract the data generated by these activities and to know in detail the public opinion and the ideology and sentiment of each individual person at any given moment (Crouch, 2020; Innerarity & Colomina, 2020; García-Marzá & Calvo, 2022; Staab & Thiel, 2022; Coeckelbergh, 2024). On the other hand, the dominance of digital fiefdoms and large datasets allows big tech companies to use and commercialize the tools and mechanisms of prediction and behavioral modification to carry out campaigns of influence, persuasion or political manipulation of citizens (Da Empoli, 2019; Zuboff, 2019; Aral, 2021).

The privatization of the digital public sphere by big digital companies results in a "refeudalization of the public sphere" (Habermas, 1962). The current situation of algorithmic domination of information, communication, and data by a small group of big digital companies, the great asymmetries of knowledge between these companies and individuals, and the unequal access to discursive power within the digital public sphere fits the hypothesis of the refeudalization of the public sphere put forward by Jürgen Habermas in *Strukturwandel der Öffentlichkeit (*1962).

The centralized exploitation of large, highly detailed and diverse datasets, knowledge asymmetries, the monopolization of innovation and the dominance of digital fiefdoms allow big digital corporations to carry out predictive and behavioral manipulation actions based on microtargeting, neurotargeting, information distortion and artificialization of public opinion (Ash, 2016; Saura García, 2023; García-Marzá & Calvo, 2024), in the creation of resonance chambers, bubble filters, spaces of social conformity or hypersocialization (Pariser, 2011; Sunstein, 2017, 2019; Aral, 2021; Woolley, 2023), and in the use of gamification, digital nudging and captology (Thaler & Sunstein, 2009, 2021; Wörsdörfer, 2018). These activities have sociopolitical implications that negatively impact the fundamental principles of democracy. They limit and contaminate the provision of information, adulterate opinion formation, and monitor and instrumentalize decision making (Zuboff, 2019).

The advent of generative AI tools developed, in most cases, by major digital corporations through new companies such as Open AI (in the case of Microsoft) or Anthropic (in the case of Amazon) through chatbots and large language models (LLMs) in modern societies has served to reinforce the characteristics and functioning of datafeudalism, to promote the dominance of these corporations over states, markets and civil society and to increase the negative impacts of datafeudalism on the functioning of democracy. These negative impacts are due to the increased prevalence of information distortion, the rise of artificialization in the public sphere, the emergence of deepfakes, and the use of personalization and manipulation techniques that can disrupt democratic processes (Coeckelbergh, 2024).

These practices lead to a hollowing out of meaning and a perversion of the main spaces and procedures of democracy, as a result of the management, restriction and modulation of the democratic public sphere, public opinion and political action by big digital companies — or by third parties such as governments, billionaires, powers that be or foreign governments — according to their economic and political interests (Crouch, 2020; Habermas, 2022).

Staab and Thiel (2022) delve into the current state of the democratic public sphere and conclude that it is undergoing a refeudalization based on the maximization of subjectivity and the singularization of people's movements and activities (Reckwitz, 2020), in the dispossession, accumulation and exploitation of the data generated by these actions by digital companies (Zuboff, 2019; Staab, 2024), and in the application — and commodification — of radical behaviorism based on large datasets to generate specific behaviors (Pentland, 2015). Crouch (2020) defines the current state of democracy as follows:

> […] the possessors of colossal wealth have been purchasing technology and expertise that enable them to discover the salient characteristics of millions of citizens and target them with vast numbers of persuasive messages, giving the impression of huge movements of opinion, apparently coming from millions of separate people, that in fact emanate from a single source. It is difficult to imagine a more perfectly post-democratic form of politics, giving an impression of debate and conflict that is really stage-managed from a small number of concealed sources. What seemed to be a liberating, democratizing technology has turned out to favour a small number of extremely rich individuals and groups. (p.XII)

The great asymmetries of knowledge between big tech companies and citizens, and the dominance of digital fiefdoms by these digital companies, have resulted in citizens becoming mere "puppets, dancing to tunes set by the manipulators of public opinion" (Crouch, 2020, p.X). In this situation, citizens are rarely able to autonomously and independently articulate their own opinions, demands or priorities, are completely influenced and manipulated by the economic and political interests of big digital companies, and are instrumentalized to legitimize these interests (Zuboff, 2019; Crouch, 2020; Coeckelbergh, 2024).

The characteristics and operating logic of datafeudalism, together with the refeudalization of the public sphere, the use of mechanisms and instruments to predict and modify citizens' behavior, and the emergence and use of generative artificial intelligence represent a real emergency for popular sovereignty, public interest, and the proper functioning of democratic systems. The perpetuation of the datafeudal system in modern societies and the consequences of the dominance of big digital companies over the main democratic spaces and processes may end up privatizing democracy.

5 Confronting Datafeudalism and its Impact on EU Democracies

Over the last few years, the EU has been developing regulations to try to control and reduce the dominance of big tech companies in market, state, civil society, democracy, and modern societies in general, and to protect and empower citizens[9]. The EU legislative package aims to protect and promote values by promoting informed

[9] Its legislative package consists of measures such as the Data Governance Act, the Data Act, the Artificial Intelligence Act (AIA), the Digital Market Act (DMA), the Digital Services Act (DSA) or the AI Liability Directive, as well as the General Data Protection Regulation (GDPR).

consent and the creating privacy and data protection standards — through the GDPR —, to establish responsibilities for big digital companies in relation to the spread of disinformation, illegal activities and the defense of fundamental rights on digital platforms — through the DSA —, to defend competitiveness and interoperability in cyberspace — through the DMA —, to promote the creation of common European data spaces — through the Data Act and the Data Governance Act —, to create a safe, reliable and ethical legal framework to ensure that AI-based technologies are human-centered and respect fundamental rights — through the AIA — and ultimately to develop a European digital sovereignty (Bradford, 2020, 2023; Roberts et al., 2021).

This set of measures is a good starting point for trying to reduce the dominance of big tech companies in modern societies, but constant updating of these measures and the implementation of more precise and stringent measures are needed to reverse datafeudalism and its negative impacts on modern societies. In this regard, Wörsdörfer (2022a, 2024) outlines a series of actions to be taken, including strengthening government regulatory agencies and eliminating the revolving doors between these agencies and big digital corporations; deepening the oversight and regulation of gatekeepers; moving toward true data portability and interoperability; improving antitrust regulation and enforcement; and improving and updating the AIA to address its lack of democratic accountability, oversight, and transparency and to regulate the potential negative impacts of general-purpose artificial intelligence on democratic processes (Kak et al., 2023).

In addition to the aforementioned measures, it is imperative to implement more precise and strict measures from various perspectives, levels and groups in order to effectively address the adverse effects of datafeudalism on the public interest and the proper functioning of democratic systems. These measures should be applied in parallel with the aforementioned actions, targeting the exploitative, predatory, and monopolistic practices of big digital companies in the data domain[10].

With respect to macro-level (i.e., by government or supranational government) actions, Mayer-Schönberger and Ramge (2022) argue that in modern societies based on the exploitation of large datasets there is no point in data limitation, fragmentation, compartmentalization, and minimization. They propose to apply a mandatory opening of corporate datasets to other organizations, companies, or individuals in order to reverse the dominance of big tech companies by de-monopolizing and socializing the large datasets they extract, store, master and exploit.

In Mayer-Schönbgerger and Ramge's proposal all companies and organizations would have to provide access to their datasets in a collectivized and anonymized manner. The more data collected by a corporation, the higher the level of openness[11]. Mayer-Schönberger and Ramge (2022) state that: "With an attitude of facilitating data

[10] In recent years, various proposals have been put forward to address the dominance of big tech companies. On the one hand, Rubinstein (2013) and Fischli (2022) proposed that data creators themselves manage their own data and share it as and with whom they wish, a model known as data-owning democracy (DOD). On the other hand, Stallman (2018) proposed restricting the collection of private data and limiting data extraction to what is strictly necessary for the operation of digital platforms and services.

[11] There are other proposals for openness and de-monopolization of data similar to the one by Mayer-Schönberger and Ramge (2022), such us Muldoon (2022). This proposal also seeks to reverse and redistribute the power of big digital companies through the implementation of collective social ownership

use in business, politics, and society, digitalization will finally be able to fulfil one of its grand promises. The information engines of the few will become instruments of empowerment for all" (p.104). The obligation to open and share large datasets would deal a severe blow to the dominance of big tech companies and the operating logic of datafeudalism. This would lead, on the one hand, to a reduction in the great asymmetries of knowledge, innovation monopolies, and the effectiveness and efficiency of mechanisms and instruments of behavior modification. On the other hand, it would lead to the reversal of the market, the state and civil society feudalization, and an empowerment of these spheres in the face of big digital companies.

It is also important to note that the proper and efficient implementation of Mayer-Schönberger and Ramge (2022) proposal to open and share large datasets of big digital corporations would require the creation and strengthening of EU government agencies (Meghani, 2021) to manage and control the opening of data and to monitor and ensure that big digital companies share all data correctly. The implementation of the openness of large datasets managed by the corporations themselves, as proposed by Mayer-Schönberger and Ramge (2022), without a set of government agencies to verify the processes of opening and sharing datasets and to enforce coercive measures in case of non-compliance, might not decisively affect the dominance situation of big digital corporations. The implementation of these open data policies could also be complemented by policies for the creation and promotion of open-structured European big digital companies in the medium/long term by EU institutions, in order to reduce dependence on large US and Chinese digital companies and to increase European digital sovereignty.

In addition to macro-level actions, meso-level (i.e., by organizations, corporations and civil society) and micro-level (i.e., by individuals) actions could also be taken, although it is important to note that these actions may not be as effective as government action or may not even have a significant impact on big tech companies' domination.

As for meso-level measures by big digital corporations themselves are concerned, the past decade has shown that attempts at self-regulation and the creation and enforcement of ethical guidelines in some of the big digital companies have not had a significant impact on reducing the negative effects of the datafeudalim operating model on democratic systems and do not seem to be the most effective option for reducing the dominance of large digital corporations over modern societies (Chomanski, 2021; Taylor, 2021).

Meso-level actions carried out by civil society and micro-level actions can also have an impact on datafeudalism and the power of big digital companies. Among these actions, cloud mobilizations, data activism, datawhistleblowing or ethical hackerism stand out (Gutiérrez, 2018; Milan, 2018; Lovink, 2022; Varoufakis, 2023; Calvo & Saura García, in press). These types of actions use the infrastructures of digital fiefdoms with the aim of exposing, denouncing and boycotting the functioning of datafeudalism, reversing the domination that big digital companies exercise over data in modern societies through data, and making citizens aware of, on the one hand,

of big data sets, the participation of individuals and communities, and the democratic control of digital infrastructure and big data sets (Muldoon, 2022).

the dispossession and depredation of their data and, on the other hand, the commodification of the tools and mechanisms of prediction and behavioral modification and the instrumentalization of people and markets.

The combination of the effects of the regulations being developed by the EU, the implementation of more precise and stricter measures to reverse datafeudalism, the socialization of large datasets proposed by Mayer-Schönbgerger and Ramge, and the various actions that can be taken by civil society actors and individual persons could have a major impact on the functioning of datafeudalism and break its model of domination over modern societies. In the democratic sphere, these effects could reverse the privatization and refeudalization of the public sphere, of public opinion, and of the main democratic spaces and procedures, leading to a sharp decrease in the ability to influence and manipulate citizens and an increase in their sovereignty, autonomy, and self-determination.

6 Conclusion

The development of surveillance capitalism towards a datafeudalism based on the refeudalization of modern societies and the domination of states, markets, politics and, civil society by big digital companies to achieve economic and political goals, the creation and domination of digital fiefdoms and digital serfs, the dispossession, predation, monopolization and exploitation of large datasets, and the commodification of prediction and behavioral modification of people have led to exponential growth and have given unprecedented power to big digital companies. This situation represents a major emergency for the proper functioning of spaces, democratic processes, and democracy in general.

Inaction or increased concentration of power by these big digital companies could exacerbate this situation, potentially leading to a state of tyranny and absolute social dominance that may be difficult to reverse. The implementation of more stringent regulations in the current EU package of measures aimed at reducing the dominance of big tech companies, along with the introduction of ambitious regulations to de-monopolize and socialize the vast datasets of these digital giants by states, and various civil society protest actions within digital realms, could have a significant impact on the logic of datafeudalism and potentially overturn the dominance of big tech companies over modern societies. The implementation of these measures could reduce power asymmetries between large corporations and states, markets, and civil society within modern societies, leading to greater sovereignty, autonomy, and self-determination of their citizens.

Acknowledgements This article was made possible thanks to the funding received from the Universitat Jaume I through a predoctoral contract (PREDOC/2022/08) and through a grant (E-2023-16) for a research stay in the Chair on Artificial Intelligence and Democracy of the Florence School of Transnational Governance at the European University Institute (Italy). This study is framed within the objectives of the Research and Technological Development Project "Cordial Bioethics and Algorithmic Democracy for a Hyper-Digitalized Society" [PID2022-139000OB-C22], funded by MCIU/AEI/10.13039/501100011033/FEDER,EU.

Author Contributions Not applicable.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature. There was no funding to disclose for this project.
Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

Data Availability This research does not involve the analysis or generation of any data.

Declarations

Ethical Approval and Consent to Participate Not needed, no data was collected for this study.

Consent for Publication Not needed, no data was collected for this study.

Competing Interests The author declares no competing interests.

References

Aral, S. (2021). *The hype machine*. Penguin Random House.

Ash, T. G. (2016). *Free speech: Ten principles for a connected world*. Atlantic Books.

Balibar, É. (2019). Towards a new critique of political economy: from generalized surplus value to total subsumption. In P. Osborne, É. Allex, & E.-J. Rusell (Eds.), *Capitalism: concept, idea, image* (pp. 36–57). CRMEP Books.

Barbrook, R., & Cameron, A. (1996). The Californian ideology. *Science as Culture*, *6*(1), 44–72. https://doi.org/10.1080/09505439609526455/ASSET//CMS/ASSET/04174C34-E9A8-4FD3-A69C-1B704CE68BD7/09505439609526455.FP.PNG

Bashyakaria, V., Hankey, S., Macintyre, A., Renno, R., & Wright, G. (2019). Personal data: Political persuasion inside the influence industry. How it works. Retrieved Novembre 2, 2022 from https://cdn.ttc.io/s/tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works.pdf

Bentham, J. (1787). *Panoptico; or, the inspection-house*. Thomas Byrne.

Blankenship, L. (1990). *Gurps Cyberpunk. High Tech Low-Life Roleplaying*. Steven Jackson Games.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Bremmer, I. (2021). *The technopolar moment. How big tech will reshape the global order*. Foreign Affairs. Retrieved February 26, 2024 from https://www.foreignaffairs.com/articles/world/ian-bremmer-big-tech-global-order

Calvo, P. (2019). Democracia algorítmica: Consideraciones éticas sobre la datificación de la esfera pública. *Revista Del Clad Reforma Y Democracia*, *74*, 5–30.

Calvo, P. & Saura García, C. (in press). Democracia de la vigilancia: Datos, activismo y contrapoder. *Revista Internacional de Pensamiento Político*.

Chomanski, B. (2021). The missing ingredient in the case for regulating big tech. *Minds and Machines*, *31*(2), 257–275. https://doi.org/10.1007/S11023-021-09562-X/METRICS

Coeckelbergh, M. (2024). *Why AI undermines democracy and what to do about it*. Polity.
Crouch, C. (2020). *Post-democracy after the crises*. Wiley.
Da Empoli, G. (2019). *Gli ingegneri del caos: Teoria e tecnica dell'Internazionale Populista*. Marsilio Editori.
Durand, C. (2020). *Techno-féodalisme: Critique de l'économie numérique*. Le Découverte.
Dyson, E., Gilder, G., Keyworth, G., & Toffler, A. (1996). Cyberspace and the American dream: A magna carta for the knowledge age. *The Information Society*, *12*(3), 295–308. https://doi.org/10.1080/019722496129486
Economic Research Council (2019). *Top ten companies by market cap over 20 years*. Retrieved February 12, 2024, from https://ercouncil.org/2019/top-ten-companies-by-market-cap-over-20-years/
Farahany, N. A. (2023). *The battle for your brain*. St. Martin's.
Fischli, R. (2022). Data-owning democracy: Citizen empowerment through data ownership. *European Journal of Political Theory*, *23*(2), 204–223. https://doi.org/10.1177/14748851221110316/FORMAT/EPUB
Foucault, M. (1975). *Surveiller et punir*. Gallimard.
Fowler, G. A. (2022). *Tour Amazon's dream home, where every appliance is also a spy.* The Washington Post. Retrieved June 26, 2023 from https://www.washingtonpost.com/technology/interactive/2022/amazon-smart-home/
García-Marzá, D., & Calvo, P. (2022). Democracia algorítmica: ¿un nuevo cambio estructural de la opinión pública? *Isegoría*, (67), e17. https://doi.org/10.3989/ISEGORIA.2022.67.17
García-Marzá, D., & Calvo, P. (2024). *Algorithmic democracy: A critical perspective from deliberative democracy*. Springer.
Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books.
Gutiérrez, M. (2018). *Data activism and social change*. Palgrave Pivot Cham.
Habermas, J. (1962). *Strukturwandel Der Öffentlichkeit*. Luchterhand.
Habermas, J. (2022). *Ein Neuer Strukturwandel Der Öffentlichkeit Und die deliberative Politik*. Suhrkamp Verlag AG.
Hagen, L. M., & Wieland, M. and In der Au, A.-M. (2017). Algorithmischer Strukturwandel der Öffentlichkeit. *MedienJournal*, *41*(2), 127–143. https://doi.org/10.24989/MEDIENJOURNAL.V41I2.1476
Han, B. C. (2017a). *In the swarm: Digital prospects*. MIT Press.
Han, B. C. (2017b). *Psychopolitics*. Verso Books.
Han, B. C. (2022). *Infocracy: Digitalization and the crisis of democracy*. Polity.
Hawley, J. (2021). *The tyranny of big tech*. Simon & Schuster.
Innerarity, D., & Colomina, C. (2020). La verdad en las democracias algorítmicas. *Revista CIDOB d'Afers Internacionals*, 11–24.
Kak, A., West, S. M., Hanna, A., Gebru, T., Gahntz, M., Talat, Z., & Khan, M. (2023). *Five considerations to guide the regulation of General Purpose AI in the EU's AI Act*. AI Now Institute. Retrieved May 18, 2024 from https://ainowinstitute.org/publication/gpai-is-high-risk-should-not-be-excluded-from-eu-ai-act
Khan, L. M. (2017). Amazon´s antitrust paradox. *The Yale Law Journal*, *126*(3), 710–805.
Khan, L. M. (2019). The separation of platforms and coomerce. *Columbia Law Review*, *119*(4), 973–1098.
Kim, T. W. (2018). Gamification of labor and the charge of exploitation. *Journal of Business Ethics*, *152*(1), 27–39. https://doi.org/10.1007/S10551-016-3304-6/TABLES/1
Lanier, J. (2011). *You are not a gadget*. Vintage.
Lanier, J. (2013). *Who owns the future?* Simon & Schuster.
Lanier, J. (2018). *Ten arguments for deleting your social media accounts right now*. Henry Holt and Company.
Lovink, G. (2022). *Stuck on the platform: Reclaiming the internet*. Valiz.
Lyon, D. (2022). *Pandemic surveillance*. Polity.
Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Miffin Harcourt.
Mayer-Schönberger, V., & Ramge, T. (2018). *Reinventing capitalism in the age of big data*. Basic Books.
Mayer-Schönberger, V., & Ramge, T. (2022). *Access rules: Freeing data from big tech for a better future*. University of California Press.
Mazzucato, M. (2019). *Preventing digital feudalism.* Project Syndicate. Retrieved February 20, 2024 from https://www.project-syndicate.org/commentary/platform-economy-digital-feudalism-by-mariana-mazzucato-2019-10

Meghani, Z. (2021). Regulations matter: Epistemic monopoly, domination, patents, and the public interest. *Philosophy and Technology*, *34*(4), 1449–1474. https://doi.org/10.1007/S13347-021-00467-2/TABLES/1

Milan, S. (2018). Data activism as the new frontier of media activism. In G. Yang, & V. Pickard (Eds.), *Media activism in the Digital Age* (pp. 151–163). Routledge.

Mill, J. S. (1977). On Liberty. In J. M. Robson (Ed.), *Collected Works of John Stuart Mill*. University of Toronto.

Mill, J. S. (2004). *Principles of political economy [1848]*. Prometheus Books.

Moore, M. (2018). *Democracy hacked: How Technology is Destabilising Global politics*. Oneworld.

Morozov, E. (2011). *The net delusion: How not to liberate the world*. Penguin.

Morozov, E. (2019, February 4). *Capitalism's new clothes.* The Baffler. Retrieved Septembre 13, 2022 from https://thebaffler.com/latest/capitalisms-new-clothes-morozov

Muldoon, J. (2022). Data-owning democracy or digital socialism? *Critical Review of International Social and Political Philosophy*, 1–22. https://doi.org/10.1080/13698230.2022.2120737

Newell, B. C. (2014a). Technopolicing, surveillance, and citizen oversight: A neorepublican theory of liberty and information control. *Government Information Quarterly*, *31*(3), 421–431. https://doi.org/10.1016/J.GIQ.2014.04.001

Newell, B. C. (2014b). The massive metadata machine: Liberty, power, and secret mass surveillance in the U.S. and Europe. *I/S: A Journal of Law and Policy for the Information Society*, *10*.

O'Flynn, I. (2010). Deliberating about the public interest. *Res Publica*, *16*(3), 299–315. https://doi.org/10.1007/S11158-010-9127-X/METRICS

Pariser, E. (2011). *The filter bubble: How the new personalized web is changing what we read and how we think*. Penguin Books.

Pentland, A. (2015). *Social physics: How social networks can make us smarter*. Penguin Books.

Petit, N. (2020). *Big tech and the digital economy: The moligopoly scenario*. Oxford University Press.

Pettit, P. (1997). *Republicanism: A theory of freedom and government*. Oxford University Press.

Plantin, J. C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2016). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, *20*(1), 293–310. https://doi.org/10.1177/1461444816661553

Posner, E. A., & Weyl, E. G. (2018). *Radical markets: Uprooting capitalism and democracy for a Just Society*. Princeton University Press.

Reckwitz, A. (2020). *The society of singularities*. Polity.

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1575

Rubinstein, I. S. (2013). Big data: The end of privacy or a new beginning? *SSRN Electronic Journal*, *3*(2), 74–87. https://doi.org/10.2139/ssrn.2157659

Saura García, C. (2023). El big data en los procesos políticos: Hacia una democracia de la vigilancia. *Revista de Filosofía, 80*, 215–232. https://doi.org/10.4067/S0718-43602023000100215

Saura García, C. (2024). Digital expansionism and big tech companies: Aonsequences in democracies of the European Union. *Humanities and Social Sciences Communications, 11*(448), 1–8. https://doi.org/10.1057/s41599-024-02924-7

Schwartz, H. M. (2022). Global secular stagnation and the rise of intellectual property monopoly. *Review of International Political Economy*, *29*(5), 1448–1476. https://doi.org/10.1080/09692290.2021.1918745

Snowden, E. (2019). *Permanent record*. Metropolitan Books.

Srnicek, N. (2016). *Platform capitalism*. Polity.

Staab, P. (2024). *Markets and power in digital capitalism*. Manchester University.

Staab, P., & Thiel, T. (2022). Social media and the digital structural transformation of the public sphere. *Theory Culture & Society*, *39*(4), 129–143. https://doi.org/10.1177/02632764221103527

Stallman, R. (2018). *A radical proposal to keep your personal data safe* The Guardian. Retrieved Sptembre 13, 2021 from https://www.theguardian.com/commentisfree/2018/apr/03/facebook-abusing-data-law-privacy-big-tech-surveillance

Sunstein, C. R. (2017). *#Republic: Divided democracy in the age of social media*. Princeton University Press.

Sunstein, C. R. (2019). *Conformity: The power of social influences*. New York University.

Taplin, J. T. (2017). *Move fast and break things: How Facebook, Google, and Amazon cornered culture and undermined democracy*. Little, Brown and Company.

Taylor, L. (2021). Public actors without public values: Legitimacy, domination and the regulation of the technology sector. *Philosophy and Technology*, *34*(4), 897–922. https://doi.org/10.1007/S13347-020-00441-4/METRICS

Teachout, Z. (2020). *Break 'em up: Recovering our freedom from Big Ag, Big Tech, and big money*. All Point Books.

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin Random House.

Thaler, R. H., & Sunstein, C. R. (2021). *Nudge: The final edition*. Yale University Press.

Thompson, S. A., & Warzel, C. (2019). *Twelve Million Phones, One Dataset, Zero Privacy* The New York Times. Retrieved June 23, 2023 from https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

van der Sloot, B. (2018). A new approach to the right to privacy, or how the European court of human rights embraced the non-domination principle. *Computer Law & Security Review*, *34*(3), 539–549. https://doi.org/10.1016/J.CLSR.2017.11.013

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance and Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Varoufakis, Y. (2023). *Technofeudalism: What killed capitalism*. Random House.

Webb, A. (2019). *The big nine: How the tech titans and their thinking machines could warp humanity*. PublicAffairs.

Williams, J. (2018). *Stand out of our light: Freedom and resistance in the attention economy*. Cambridge University Press.

Woolley, S. (2023). *Manufacturing consensus: Understanding propaganda in the era of automation and anonymity*. Yale University Press.

Wörsdörfer, M. (2018). *Engineering and computer ethics*. Great River Learning.

Wörsdörfer, M. (2020). Ordoliberalism 2.0: Towards a new regulatory policy for the digital age. *Philosophy of Management*, *19*(2), 191–215. https://doi.org/10.1007/S40926-020-00134-0/TABLES/1

Wörsdörfer, M. (2022a). Big tech and antitrust: An ordoliberal analysis. *Philosophy and Technology*, *35*(3), 1–39. https://doi.org/10.1007/S13347-022-00556-W/FIGURES/1

Wörsdörfer, M. (2022b). What happened to 'Big tech' and antitrust? And how to fix them! *Philosophy of Management*, *21*(3), 345–369. https://doi.org/10.1007/S40926-022-00193-5/FIGURES/2

Wörsdörfer, M. (2024). Mitigating the adverse effects of AI with the European Union's artificial intelligence act: Hype or hope? *Global Business and Organizational Excellence*, *43*(3), 106–126. https://doi.org/10.1002/JOE.22238

Young, I. M. (1990). *Justice and the politics of difference*. Princeton University Press.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for the future at the new frontier of power*. Profile Books.

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH ("Springer Nature").

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users ("Users"), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use ("Terms"). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com