




ARTICLE



<https://doi.org/10.1057/s41599-024-02924-7>

OPEN

Digital expansionism and big tech companies: consequences in democracies of the European Union

Carlos Saura García ¹ 

Big digital companies have become key elements in economy, communication, education, and politics in 21st century societies. The neutral ideology in their digital platforms, applications, and services, as well as the exponential growth in their activities can be used by world superpowers —especially the United States and China— to implement geostrategical operations, massive social manipulation or influence democratic processes with the objective of increasing their power and dominance over other nations. The aim of this paper is to state the different strategies of digital expansionism performed by the United States and China, and, additionally, to showcase the negative consequences of these strategies on the population and democracies of the European Union. The first section of this paper will define the concepts of digital sovereignty and digital expansionism as well as their importance in 21st century geopolitics. Next, the important role that big digital companies have on digital expansionism will be analysed, and the usage of digital authoritarianism and digital instrumentarianism performed by the United States and China will be further examined. Finally, the negative consequences of the implementation of these methods in the democratic systems of the European Union will be analysed, as well as what possible solutions there might be for said consequences.

¹Department of Philosophy and Sociology, Universitat Jaume I de Castelló, 12071 Castelló, Spain. ✉email: saurac@uji.es

Introduction

In the past two decades, the emergence and development of a new economic system known as “surveillance capitalism” and its business model has provoked great changes in various aspects of western societies (Zuboff 2019). This new economic system has two main features. On the one hand, the exploitation of human experience in order to draw value and obtain economic or political benefits. On the other hand, the accumulation of huge concentrations of knowledge, wealth, and power by a small group of big tech companies.

This new form of capitalism and its features have huge negative effects on societies, especially on civilians’ sovereignty, on electoral processes and on the proper performance of democratic systems, in general (Han 2017, 2022; Zuboff 2019). Among the main weapons of the surveillance, control, influence, and manipulation of citizens, the most noteworthy are those such as massive social surveillance (Lyon 2019; Snowden 2019), micro-targeting (Kaiser 2019; Wylie 2019; Dawson 2021), information intoxication (Howard 2020; Woolley 2023), the creation of an artificial public opinion (García-Marzá and Calvo 2022, 2024) or the self-interested management of digital platforms (Bucher 2018; Moore and Tambini 2018; Dawson 2023).

Big tech companies have a variety of possibilities that have piqued the interest of governments (Hoffman 2019; Zuboff 2019; Hoffman and Attrill 2021). This has resulted in governments and the big tech companies in their countries allying and cooperating to obtain economic benefits for said companies and political benefits for the governments (Saura García 2022). Governments from both the United States (US) and China use the digital infrastructure of their big national tech companies in order to carry out digital expansionist practices and, therefore, increase their control and influence over the society, economy, and politics of foreign countries (Cave et al. 2019; Webb 2019; Zuboff 2019; Hoffman and Attrill 2021).

The aim of this paper is to present the negative effects that US and Chinese digital expansionism might have over the democracies of the European Union (EU). First and foremost, the concepts of “digital sovereignty” and “digital expansionism” will be defined, as well as the different strategies carried out by the US, China, and the EU, and their importance in 21st century geopolitics. Next, the role of big digital companies on digital expansionism will be analysed by further examining the phenomena of “digital instrumentalism” and “digital authoritarianism”. Lastly, the consequences of these two phenomena on the democratic systems of the EU will be presented, as well as the potential solutions to said consequences.

Geopolitics of the 21st century: digital sovereignty and digital expansionism

The fast growth of intelligent digital technologies that allow the autonomous and semiautonomous processing of large quantities of data and metadata with the aim of producing inferences, obtaining predictions, making decisions and generating value, have provoked great interest in world superpowers (Roberts et al. 2022). Throughout the last decade, the US, China, and the EU have implemented important strategies of digital sovereignty and digital expansionism (Roberts et al. 2023).

While the assertion of sovereignty by states represents a “defensive” mechanism to protect their authority against various perceived threats, its “offensive” counterpart can be understood in terms of “digital expansionism”. While digital sovereignty is defined by “legitimate control over the digital”, digital expansionism involves using different “forms of control” over other states. This includes using coercive capabilities to force compliance, consensual

inducements to incentivise it, and commanding it through the legitimate exercise of power. (Roberts et al. 2023: 9)

As Roberts highlights in this quote, “digital sovereignty” can be defined as “the legitimate control over the digital”. Further developing this definition, “legitimate control” alludes to the ability to influence and exert power over something through a perceived authority that operates and acts by means of a process that is generally accepted and that pushes the involved parties to meet certain instructions, rules or guidelines (Floridi 2020; Roberts et al. 2021). On the other hand, “the digital” alludes to the conjunction of data, hardware, software, services, standards, and rules that comprise the current ecosystem of digital technologies (Roberts et al. 2023).

Digital sovereignty policies encompass various aspects, such as regulation and restriction of data processing, exploitation and transference, limitation of certain content on the internet, or the prohibition of activities performed by foreign digital companies. In the current global geopolitical situation, the operations of digital sovereignty are used to create interdependencies with other nations, to enhance security and legal harmonisation, to build and defend economic markets, to achieve autonomy in some sectors and to yield sovereignty in other sectors in order to create digital barriers that will lead to a situation of total digital independence (Roberts et al. 2023).

The main difference between digital sovereignty and digital expansionism is the direction of their operations. The operations of digital sovereignty are inward-oriented regarding a nation or group of nations, with the purpose of affecting its technologically dependent relationship with other agents, companies, or external nations. Conversely, the operations of digital expansionism are outward-oriented and have the objective of generating influence, increasing control over other nations and/or strengthening measures taken regarding digital sovereignty.

“Digital expansionism” can be defined as a way of affecting, influencing, and subordinating foreign nations through “the digital”. The numerous strategies of digital expansionism are used to increase or improve the power and dominance of a nation over another, or to weaken the abilities of a competing nation to exert its own power (Doshi, 2021). Roberts et al. (2023) explain that digital expansionism has two main reasons and three key mechanisms to try to achieve these goals.

The two fundamental reasons for digital expansionism are the exportation of values and internal protection. On the one hand, exportation of social, political, and economic values of the nation that carries out expansionist strategies on other nations is intended to attain more outstanding geopolitical achievements. On the other hand, internal protection has the aim of shielding its citizens, institutions, and economy and to strengthen and support a nation’s digital sovereignty strategies. It is important to note that these two reasons for digital expansionism are not mutually exclusive. For example, in many cases it is possible to increase internal protection through the exportation of values (Hoffman 2019).

The three key mechanisms regarding digital expansionism are data exploitation, control through technological infrastructures, and influence through regulation. The first mechanism refers to the extraction and exploitation of huge datasets and metadata, which allows a great deal of economic, social, and political power to be obtained by big digital companies, and consequently, by the home nations of these companies (Saura García 2022). Data extraction can be carried out and promoted in different ways: by hacking big datasets or performing illegitimate—in many cases illegal—practices backed by governments of nations for the obtention of data (Macaskill and Dance 2013; Feldstein 2019;

Snowden 2019; Hoffman and Attrill 2021); by acquiring private datasets from citizens in a lawful manner (Zuboff, 2019); and by influencing the creation of rules regarding the data processing of other nations or simply infringing upon the rules currently in effect (Sherman 2020; Hoffman and Attrill 2021; Satariano 2023). The fast growth and expansion of big digital companies in namely every context of every world nation have provided these companies with great power and have allowed the enhancement of their source value system and the mining of a continuous quantity of data that may allow improving and increasing these companies' home nation's control over other nations (Lee 2018; Kliman et al. 2019; Snowden 2019).

The second mechanism concerns control through technological infrastructures. This tool for digital expansionism provides the expansionist nation with influence and control over other countries by putting their national companies and the technologies that they offer into effect. This fact, on the one hand, allows the modification of the digital infrastructure, the digital public sphere, and the Internet context of the target nations by matching the technological standards, the values, and the ideologies of the nation that performs the technological influence. On the other hand, it allows an economic link between the target nation and the expansionist nation; the dominance of the technological infrastructure of the target nation and its usage in favour of its objectives; and the prevention of other nations carrying out similar strategies of technological influence (Lee 2018; Kliman et al. 2019; Webb 2019; Helberg 2021).

The third mechanism pertains to the influence in the realm of regulation and governance. The ability to enact, influence or establish international treaty regulations and regulatory initiatives with extraterritorial consequences eases data exploitation practices and influence and control through technological infrastructures, and enables the enhancement of effectiveness and efficiency of digital expansionism strategies (Roberts et al. 2023).

World superpowers like the US, China, and the EU have conducted various types of digital expansionism and digital sovereignty with different purposes regarding their geopolitical objectives. In the case of the US, these are based on the exportation of surveillance capitalism, spreading free market values, and maintaining its economic and political world power. In the case of China, these are based on safeguarding its national digital infrastructure, isolating its citizens, increasing its international and economic power, and spreading its social model, which is based on surveillance and digital repression. Regarding the EU, its purpose is to develop and apply digital regulations based on its foundational values in order to strengthen the freedom of its citizens, the proper functioning of its democracies and its internal market, and to defend itself against the expansionist policies of the US and China. Moreover, these rules are also aimed at disseminating and expanding their digital legislation and regulations beyond their borders.

The US stands out for carrying out policies focused on digital expansionism. These policies have the aim of maintaining its digital, political and economic supremacy worldwide by means of creating, enhancing, and exploiting the technological dependency that other nations have on big US tech companies; by increasing influence in the creation of laws and regulations regarding digital technologies of other nations; and by limiting digital expansionist policies from China (Roberts et al. 2023).

These US policies are generally realised in three different ways. Firstly, protecting and enhancing the surveillance capitalism business model practised by the GAMAM companies (acronym that refers to the companies of Google, Amazon, Meta, Apple, and Microsoft). This is key in order to spread its economic, political, and social values as well as for the growth of US economy and the control of other nations' citizens (Zuboff 2019).

Secondly, pressuring other nations (India, Indonesia, the EU, etc.) to limit them from developing their regulations on protection, data processing, and data transfer, since these can negatively impact the business model of its tech companies (Suroyo et al. 2019; Sherman 2020). Lastly, limiting the development of Chinese tech companies and their infrastructures within its borders, while it also attempts that this development is minor within its spheres of influence (Ryan et al. 2021).

In contrast with the US, China promotes policies that focus both on digital sovereignty and digital expansionism. Regarding digital sovereignty, China has created a digital infrastructure based on control, surveillance, and repression of its citizens through programs focused on media control, digital social credit systems, and massive social surveillance structures in big cities (Jiang and Fu 2018; Lee 2018; Qiang 2019). In order to make this infrastructure happen, China has boosted the growth of big national tech companies that are strongly interfered with by the Chinese government, such as Baidu, Alibaba, Tencent, ZTE or Huawei. It has also developed a strong legislative network regarding the data exploitation and transference carried out by foreign tech corporations that makes it very difficult for the business model of big US tech companies to function properly (Cave et al. 2019; Ryan et al. 2019; Doshi 2021). Regarding digital expansionism, China has started the "Belt and Road Initiative (BRI)". This initiative seeks to increase China's economic and political power internationally by developing a wide network of both physical and digital infrastructures in various nations which is supported by big Chinese tech companies. Furthermore, it seeks to control and dominate other nations through the technologies used by said corporations (Kliman et al. 2019; Helberg 2021; Hillman 2021).

Finally, the European Union focuses its policies on digital sovereignty, but also uses them to pursue digital expansionism. The purpose of the new EU digital sovereignty policies is to face the negative consequences that digital expansionism (mainly that of the US, but also that of China) has on citizens, the economy, and European democracies (Floridi, 2020). Throughout the past years, a new package of digital regulations¹ has been developed. On the one hand, these measures aim to regulate the infrastructure and digital technologies that operate within the EU as well as the big tech companies that provide and make them possible, taking into account the foundational values of the EU (Floridi 2020). On the other hand, they aim to enhance legal certainty, harmonise the various legislations of EU countries, develop a consistent digital policy across all countries and regions, and compliance with the founding values in internal market activities (Bradford 2020, 2023). It is important to highlight that this package of digital regulations promotes a layered approach to regulation—the bigger the digital company is, the more regulation it requires—and creates two different regulatory environments: one for EU-based corporations and another for non-EU based corporations operating in the EU (Bradford 2023). Regarding digital expansionism, the EU implements its expansionist policies through regulatory influence. This is achieved through the *de jure* and *de facto* diffusion and expansion of EU digital legislation and regulations beyond its physical borders, as well as, the international expansion of EU-based digital corporations (Scott and Cremona 2019; Bradford 2020, 2023).

Big tech companies: from digital instrumentalism to digital authoritarianism

The three key mechanisms in digital expansionism (data exploitation, control through technological infrastructure and influence by means of regulations), both in the US and in China, are closely associated to activities carried out by big digital companies.

Mayer-Schönberger and Ramge (2022) present that the way big digital companies work:

[...] illustrates how control over information in a data-driven world is shifting in favour of those who generates, store, and analyze information flows on their digital platforms. [...] Today, data colonialists in Silicon Valley, and to a lesser extent China, rule much of the world. In fact, these private corporations shape information access just as much within the United States, influencing economic transactions and democratic decision-making. (p.5)

This excerpt highlights how big digital companies and their activities have acquired a leading role in expansionist policies of world superpowers. It should be noted that although American and Chinese digital companies offer similar applications, platforms, and services, they both have the aim of promoting and developing digital economic, social, and political models that are completely different in contrast. In the case of the US, it seeks to promote and apply what is known as digital instrumentalism, while China seeks to apply digital authoritarianism.

The US aims to export a form of digital society to the rest of the world in which citizenship, democracy and economy are subordinated, on the one hand, to the conditions, mechanisms, and operations of the business model of surveillance capitalism and, on the other hand, the laws of the free market. This society format is founded on the exploitation—and exportation to the US— of citizens' behaviour through their data, which is performed free of charge and with no supervision or regulation, by a small group of digital companies that accumulate wealth, knowledge, and power. This is what is known as digital instrumentalism.

Digital instrumentalism is based on the launch of what is known as “instrumentalist” power. Zuboff (2019) defines this type of power as “the instrumentation and instrumentalization of behaviour for the purposes of modification, prediction, monetization, and control” (p.352). On the one hand, instrumentation alludes to the spaces and “cyber-physical”² ecosystems up and down the length and breadth of the physical and virtual reality that drive data creation and continuously extract, transfer, convert and interpret huge datasets. On the other hand, instrumentalization is associated with the nature by which surveillance capitalists use huge datasets linked with human behaviour in order to achieve their own goals and third parties' goals.

“Instrumentalist” power does not aim at the transformation of citizens or the inculcation of certain principles or ideologies nor the mental and physical domination. It merely seeks to obtain as much behavioural data from as many measurable actions and activities as possible—both individually and collectively—with the purpose of extracting value from the data and monetising the modification in citizens' behaviour. All of this is done without having the slightest interest in citizens in an individual or collective level nor in their bodies, activities, thoughts, opinions, or emotions. The dominance exercised by this power stems from the hybridisation in today's hyper-connected, datafied, and algorithmised digital infrastructure of two doctrines: radical indifference and radical behaviourism (Zuboff 2019).

On the one hand, the radical indifference doctrine sees citizens as mere “organisms that behave”, in which there is no interest, except for the maximisation of instrumentation, so that their behaviour can be extracted, datafied, and explored. On the contrary, the radical behaviourism doctrine perceives citizens as organisms that are limited within behavioural guidelines that escape their own control. Its only goal is to observe and analyse citizens' actions, activities, and behaviour without regard to any subjective attributions (Skinner 1938, 1965, 1971).

The joint implementation of digital instrumentalism, the surveillance capitalism business model and the advocacy of free market laws by the US government seek to give rise to a form of society—subject to an automated instrumental economy that controls social learning and uses behaviour modification mechanisms—that has a series of negative impacts on citizens and democracy (Zuboff 2019). US digital expansionist policies seek to enhance and export that form of society to other nations so as to increase its influence, control, and dominance through its big digital companies.

When it comes to exerting control and government power within Chinese borders and increasing its control and dominance over other nations through “the digital”, China is aware of the threats posed by an open cyberspace that is run by big US digital companies and based on the surveillance capitalism business model and the free market laws. In order to keep control over the cyberspace and “the digital” and increase its government power, over the last years China has developed an infrastructure based on repression, censorship, manipulation, and information limitation, which is known as “The Great Firewall”. Therefore, it has created a panoptic infrastructure of massive social surveillance and of persecution of opponents (Jiang and Fu 2018; Shahbaz 2018; Cave et al. 2019; Wang et al. 2023). To increase its dominance over other nations, China has promoted and applied what is known as digital authoritarianism through “the digital” and the global cyberspace.

Digital authoritarianism alludes to the exportation of Chinese ideologies, values, moral rules and technology standards through digital platforms, services and infrastructure in order to face what is known as “open internet”, which is ruled by the US, and increase its control and dominance over other nations (Cave et al. 2019; Hoffman and Attrill 2021). Shahbaz (2018) asserts that digital authoritarianism “is being promoted as a way for governments to control their citizens through technology, inverting the concept of the internet as an engine of human liberation”. The main way in which China promotes and applies digital authoritarianism is through its big national digital companies' infrastructures, platforms and services, which are Alibaba, Baidu, Huawei, Tencent, ZTE, ByteDance, CloudWalk, Hikvision, etc. (Cave et al. 2019; Hoffman 2019; Ryan et al. 2019, 2021).

Through these big digital companies, China aims to boost an authoritarian proposal of Internet governance; promote that the Chinese Communist Party (CCP)'s ideology becomes predominant in the global cyberspace; and enhance its geopolitical goals (Feldstein 2019; Hoffman 2019; Webb 2019; Hillman 2021). China's efforts to manage, control and shape the global ecosystem of “the digital” are based on the implementation of both coercive and cooperative tools of control and domination (Hoffman 2019; Hoffman and Attrill 2021). Regarding these control and domination tools, Hoffman (2019) states that:

The CCP uses technology to make an unbreakable knot of the party's political control and China's social and economic development. Developments such as smart cities are the embodiment of this strategy because they allow the CCP to blur the line between cooperative and coercive control. It may seem contradictory, but as already outlined throughout this paper, the technology supporting the Chinese party-state's vision for tech-enhanced authoritarianism doesn't always involve distinctly coercive and overtly invasive technologies. In fact, it relies on technologies that provide services. Service provision helps the party collect data that's processed and turned into information that contributes to other tools for shaping, managing, and controlling society. (p.25)

In this excerpt, Hoffman stresses that the application and distribution of digital authoritarianism does not need to be done solely through coercive and invasive forms, but also by means of cooperation-based technologies. This control and dominance over other nations and its citizens can also be achieved by increasing user-friendliness, convenience, and desire when it comes to the usage of certain systems, platforms, and digital services that have been created, managed, and provided by big Chinese digital companies. Both coercive and cooperative tools allow China's values, culture, and ideology to be applied and distributed in different ways and to different degrees. They also allow for the protection of its security and its future strategic objectives (Hoffman 2019; Erie and Streinz 2021; Hillman 2021; Hoffman and Attrill 2021; Zhang et al. 2023).

The two models of digital expansionism hide projects with completely different features. Digital instrumentalism alludes to a market project based on an automated instrumentalism economy founded on the doctrines of radical indifference and radical behaviourism that exploits citizens' behaviour in order to get knowledge that will allow for the control, commercialization, and monetisation of social learning and behaviour modification mechanisms, therefore, increasing its financial income (Zuboff 2019). The US promotes digital instrumentalism by favouring the deregulation of the technological sector and the free market. It is used to export and promote to the rest of the world a form of society in which citizens, democracy and the economy are subordinated, controlled, and dominated by the power of its big tech companies.

On the contrary, in the case of Chinese digital authoritarianism, it is the CCP who executes it and manages it through big Chinese tech companies. Digital authoritarianism is not just linked to a market project, but also to a social and political project that seeks to limit, sacrifice, shape, and dominate citizens' freedom of behaviour so as to perpetuate CCP's power as well as apply and spread Chinese values, culture, and ideology and protecting China's security and strategic objectives (Zuboff 2019; Hoffman and Attrill 2021; Ryan et al. 2021).

Instrumentalism and digital authoritarianism can be summarised into two diverse models that seek to control, shape, and dominate human, social and political territories. In the case of instrumentalism, the power to control, shape, and dominate is exercised by big US companies, who seek to commercialise and monetise it without taking into consideration the potential consequences. On the contrary, in the case of digital authoritarianism, this power is exercised by the CCP so that it can apply its own ideology, moral rules and objectives. Both models entail great power and knowledge asymmetries, as well as a great threat to sovereignty in foreign nations (Zuboff, 2019). Its negative consequences on democratic systems, especially that of the EU, will be outlined below.

Consequences on the democracies of the EU

With the new package of digital regulations, the EU is trying to introduce regulations that protect the values, freedom and rules that support its democratic systems. These regulations seek to protect EU citizens' privacy and autonomy; demand responsibilities from and control big tech companies; and limit and reverse the impacts of instrumentalism and digital authoritarianism on the democracies of the EU as much as possible. Despite the legislative efforts from the EU, the US and China — through their big digital companies— have developed various intrusive, subversive, and covert mechanisms not only to exploit and expropriate human experience and social learning through data and metadata, but also to degrade individual auto-determination and use behaviour modification mechanisms on

EU citizens in order to ensure their influence, manipulation, and dominance capabilities.

Big US digital companies have performed several legally questionable digital expansionist activities related to the control and dominance of technological infrastructures and data exploitation and exportation with the aim of promoting digital instrumentalism. The EU has carried out some investigations and given the five biggest American digital companies different types of penalties. The penalties that stick out the most are the ones given to Google for infringing on the GDPR, illegally transferring data from Europe to the US and monopolising digital platforms and infrastructures (Satariano 2021; Commission Nationale de l'Informatique et des Libertés 2022; European Data Protection Board 2022). Amazon and Meta have also been investigated and penalised for infringing the GDPR and illegally transferring data from Europe to the US (Schechner 2021; Satariano 2023). Finally, Apple and Microsoft are being investigated for monopolisation and abuse of its dominant market position (Dave 2022; Sweny 2022).

The abovementioned activities from the GAMAM companies entail a blatant violation of the EU regulations and can cause negative effects on democratic processes (Moore 2018; Mayer-Schönberger and Ramge 2022). First of all, monopolisation, control and dominance over the digital platforms and infrastructures used daily by millions of EU citizens entail a boost in the behavioural data streams extracted by the GAMAM companies. Cyberspace monopolisation makes it difficult for citizens to look for alternatives to the digital platforms and infrastructures offered by these companies. Therefore, their control and dominance provoke a maximisation of the data and metadata that these companies extract from citizens and society in general, prompting a massive social surveillance context (Bartlett 2018; Fowler 2022).

Second of all, these big companies illegally export that data from the EU to the US, so that it can be processed there (Satariano 2023). This exportation is carried out so that they can perform the exploitation of this data without considering the European regulations regarding EU citizens' privacy and autonomy, and in order to use disruptive artificial intelligence with no limitations whatsoever. In other words, the GAMAM companies can exchange, share, and cross information among their various platforms, services, and applications; analyse, share, and exploit sensitive citizen data and metadata —such as medical, biometrical, ethnic, behavioural, and ideological data—; and use generative artificial intelligence, stochastic algorithms and learning technology so as to exploit these datasets.

Lastly, the GAMAM companies use the knowledge acquired from US data processing, as well as their monopoly position and control of digital infrastructures and platforms to monetise this knowledge and dominance of cyberspace and commercialise the possibility of behaviour modification practices and to influence and manipulate the opinion and ideology of EU citizens. These practices aim at starting processes like automated computational propaganda; various kinds of microtargeting; information intoxication mechanisms; and erosion of public opinion and creation of an artificial or synthetic public opinion (Howard 2020; Iyer et al. 2021; García-Marzá and Calvo 2022, 2024; Woolley 2023).

The various mechanisms used by the GAMAM companies to maximise digital instrumentalism efficiency entail a great risk for the democratic systems of the EU. The GAMAM companies hold great power when it comes to controlling, manipulating and modifying European citizens' behaviour, opinions, and ideology, and through the commercialisation of this power they allow other actors to influence and manipulate public opinion and electoral processes (Moore 2018; Da Empoli 2019; Wylie 2019).

Through big Chinese digital companies, the CCP has also started various strategies to increase its control and dominance over EU culture, values, ideology, and democratic processes (Hoffman 2019; Webb 2019; Hoffman and Attrill 2021). In this case, Chinese companies have not been penalised for infringing EU regulations, but they have been vetoed from certain infrastructures and segments of society and their expansion has been restrained so that European dependence on their technologies is limited, as well as CCP's capacity to control and influence European societies (Floridi, 2020). The clearest examples are the veto regarding the development of the 5G infrastructure by Huawei and ZTE (Espinoza 2023; Yun Chee 2023), and the ban on the use of TikTok —owned by the Chinese company ByteDance— by employers and politicians of the EU institutions (Sweney 2023).

The CCP has developed a framework of mechanisms and structures with the aim of profiting from big Chinese digital companies in order to, on the one hand, analyse and control EU citizens behaviour through data streams; and, on the other hand, apply various forms of strategic and political Chinese objectives on the EU through digital platforms and infrastructures (Cave et al. 2019; Hoffman and Attrill 2021; Ryan et al. 2021; Zhang et al. 2023).

This framework is partly based on the CCP intervention in big tech companies. This group of companies —especially Alibaba, Tencent, and Huawei (Cave et al. 2019)— are strongly audited by the CCP. Moreover, out of all the big multinational companies in China, these companies are the ones with the biggest number of Secretaries and politicians in their executive teams who are part of the CCP (Ryan et al. 2019). The abovementioned framework is also partly based on the cooperation agreements between China and the big tech companies, and the legislations regarding the processing of datasets from the companies and the Chinese government that allow the CCP to use their data streams either directly or indirectly (Hoffman 2019; Hoffman and Attrill 2021).

Regarding these cooperation agreements, Hoffman (2019) highlights the case of Global Tone Communications Technology Co. Ltd (GTCCOM), a public company subsidiary of the Central Propaganda Department of the Chinese government. This company provides hardware and software services related to translations for companies like Huawei and Alibaba. However, it indirectly grants the Chinese government and the CCP with the possibility of exploiting, processing, and using huge quantities of data streams derived from their applications, platforms, and digital services for numerous purposes. In relation to the regulations regarding the data processing in China, there are two key points that make it possible for Chinese companies to extract, utilize, and directly exploit data streams. These two key points are the privacy policies of Chinese companies and the Chinese legislation regarding data processing.

In most privacy policies of big Chinese digital companies, it is explained that European data can be exploited and transferred to a country that is different to that where the data has been extracted, including China. It is also explained that, from that moment onwards, that data will be operated by both the legislation of the country of destination and the country of origin (The Australian Strategic Policy Institute 2021). In regard to this, Hoffman and Attrill (2021) claim that big Chinese digital companies:

[...] are committed to protecting personal information, but acknowledge that they may be required to disclose personal data to meet law enforcement or state security requirements. The definition of what meets the threshold of being a national security or criminal case can be highly politicised in the PRC, and the process of definition isn't similar to those that occur in a liberal democracy. (p.12)

This excerpt demonstrates that legislation in China is, above all, a political legislation used as a tool by the government and the CCP in order to defend, strengthen and expand its power and to foster the spreading of its digital authoritarianism model worldwide. Due to this legislation, the CCP and the Chinese government have created an infrastructure based on big Chinese digital companies. This infrastructure allows direct extraction, usage, and exploitation of their data streams (Hoffman 2019; Hoffman and Attrill 2021).

The CCP has the ability to access and store huge datasets, to exploit them and to extract knowledge from them through disruptive actions and techniques, which are not allowed by the EU legislation, with the aim of controlling, influencing and manipulating the behaviour, public opinion and electoral processes in the EU, as well as slowly exporting its culture, ideology and values through the platforms, applications, systems and services from companies like Alibaba, Baidu, Huawei, Tencent, ZTE or ByteDance. In essence: “For the Chinese party-state, bulk data collection and AI processing of data are tools for engineering global consent and shaping global governance in pursuit of its objectives” (Hoffman 2019: 6).

Both the strategies that enhance digital instrumentalism carried out by the US, and the digital authoritarianism enhancing actions carried out by China are based on the same premise: “Data is power and market dominance is power”. The implementation of instrumentalism and digital authoritarianism by extracting, exporting, and exploiting European datasets as well as the control and dominance of infrastructures, platforms and digital services of the EU entail a great impact for European societies, especially for European democracies.

Massive social surveillance, indiscriminate data exploitation and extraction, information intoxication, and self-interested management of digital platforms in a European social context marked by dependence on digital infrastructures and services and major knowledge asymmetries ultimately leaves European economy, politics, education, and democracies defenceless and at the mercy of the economic objectives of the GAMAM companies or the political and social objectives of the CCP. These features have turned big tech companies of the world into the core elements of a new form of democracy known as surveillance-democracy (Coudry 2017), in which citizens' characteristics, emotions and opinions can be analysed and manipulated at all times, which could result in the citizens becoming mere transmitters of the interests and objectives of big digital companies (Saura García 2023).

Conclusions

The implementation of strategies like digital instrumentalism and digital authoritarianism, which are based on the monopolisation of social learning, manipulation of the citizens' behaviour with economic or political motivations, the instrumentalisation of the self-determination of individual citizens, and the creation of a surveillance democracy not only pose a true threat to the freedom, autonomy and self-determination of citizens, but also to the proper functioning of the democratic systems of the EU and to the sovereignty of EU states.

Throughout the last decade, the EU has made great efforts to encourage digital sovereignty, regulate the activities performed by big digital platforms and face the digital expansionism of China and the US. These efforts have succeeded in mitigating some of the most damaging consequences of digital instrumentalism and digital authoritarianism on the EU's public sphere, public opinion, and democratic processes, but they have, by no means, eliminated them entirely. Despite these efforts, the weak state of the EU's digital infrastructure and services and the deliberate

passivity of the US and Chinese governments regarding the infringement of European regulations through big digital companies in their countries limit the effect of the EU's policies of digital sovereignty and digital expansionism and keep the EU subjugated to US and Chinese interests.

Given the steady development on techniques for data extraction, exploitation, and analysis, as well as the exponential development on the innovations regarding artificial intelligence that increase the dangers of instrumentalism and digital authoritarianism, the EU should continue the development and implementation of regulatory practices. It should also encourage a digital context based on the defence and advocacy of its foundational values with the purpose of strengthening its democratic systems.

Received: 17 October 2023; Accepted: 4 March 2024;

Published online: 22 March 2024

Notes

- 1 This legislative package is comprised of measures such as the Data Governance Act, the Data Act, the Artificial Intelligence Act, the Digital Market Act (DMA), the Digital Services Act (DSA), the AI Liability Directive or the General Data Protection Regulation (GDPR).
- 2 Spaces and cyber-physical ecosystems allude to hardwares, softwares, devices, applications and interconnected sensors directed by algorithms that allow the connectivity of the physical and social reality, including people, animals, processes or elements and their own behaviours and actions (Calvo 2019).

References

- Bartlett J (2018) *The People Vs Tech: How the internet is killing democracy (and how we save it)*. Penguin Random House, New York
- Bradford A (2020) *The Brussels effect: how the European Union rules the world*. Oxford University Press, Oxford
- Bradford A (2023) *Digital empires: the global battle to regulate technology*. Oxford University Press, Oxford
- Bucher T (2018) *If... then: Algorithmic power and politics*. Oxford University Press, Oxford
- Calvo P (2019) Democracia algorítmica: consideraciones éticas sobre la dataficación de la esfera pública. *Rev del Clad Reforma y Democracia* 74:5–30
- Cave D, Hoffman S, Joske A, Ryan F, Thomas E (2019) Mapping China's technology giants. *The Australian Strategic Policy Institute*, 15. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-05/MappingChina%27stechnologygiants.pdf?EINwiNpste_FojtgOPriHtHfSD2OD2tL
- Commission Nationale de l'Informatique et des Libertés (2022) Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply <https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply> Accessed 05/07/2023
- Couldry N (2017) Surveillance-democracy. *J Inf Technol Politics* 14(2):182–188. <https://doi.org/10.1080/19331681.2017.1309310>
- Da Empoli G (2019) *Gli ingegneri del caos: teoria e tecnica dell'Internazionale populista*. Marsilio Editori, Venezia
- Dave P (2022) Microsoft's cloud business targeted by EU antitrust regulators, Reuters, <https://www.reuters.com/business/microsofts-cloud-business-targeted-by-eu-antitrust-regulators-2022-04-01/>
- Dawson J (2021) Microtargeting as Information Warfare. *Cyber Def Rev* 6(1):63–80. <https://doi.org/10.2307/26994113>
- Dawson J (2023) Who Controls the Code, Controls the System: Algorithmically Amplified Bullshit, Social Inequality, and the Ubiquitous Surveillance of Everyday Life. *Sociological Forum* 1-24. <https://doi.org/10.1111/SOCF.12907>
- Doshi R (2021) *The Long Game: China's grand strategy to displace american order*. Oxford University Press, Oxford
- Erie MS, Streinz T (2021) The Beijing Effect: China's digital silk road as transnational data governance. *J Int Law Politics* 54(1):1–92
- Espinoza J (2023) EU considers mandatory ban on using Huawei to build 5G, *Financial Times*, <https://www.ft.com/content/a6900b0f-08d5-433d-bfb0-f57b6041e381>
- European Data Protection Board (2022) Italian SA bans use of Google Analytics: no adequate safeguards for data transfers from Caffèina Media S.r.l. to the U.S. https://edpb.europa.eu/news/national-news/2022/italian-sa-bans-use-google-analytics-no-adequate-safeguards-data-transfers_en Accessed 18/06/2023
- Feldstein S (2019) *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf
- Floridi L (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philos Technol* 33(3):369–378. <https://doi.org/10.1007/S13347-020-00423-6/METRICS>
- Fowler GA (2022) Tour Amazon's dream home, where every appliance is also a spy, *The Washington Post*, <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?. *Isegoria* (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, Cham
- Han BC (2017) *Psychopolitics*. Verso Books, London
- Han BC (2022) *Infocracy: digitalization and the crisis of democracy*. Polity Press, Cambridge
- Helberg J (2021) *The wires of war: technology and the global struggle for power*. Avid Reader Press, New York
- Hillman JE (2021) *The digital Silk Road: China's quest to wire the world and win the future*. Harper Collins, New York
- Hoffman S (2019) Engineering global consent: The Chinese Communist Party's data-driven power expansion. *The Australian Strategic Policy Institute*, 21. <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2019-10/EngineeringGlobalConsentV2.pdf?VersionId=efvKpmwu2iVwZx4oIn8B5MAnnC75qBT>
- Hoffman S, Attrill N (2021) Mapping China's Tech Giants: Supply chains and the global data collection ecosystem. *The Australian Strategic Policy Institute*, 45. https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2021-06/Supplychains.pdf?VersionId=56J_tt8xYXYvsMuhriQt5dSsr92AdAZH
- Howard PN (2020) *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*. Yale University Press, New Haven
- Iyer P, Riedl MJ, Trauthig IK, Woolley S (2021) Location-based targeting: history, usage, and related concerns. *The University of Texas Austin. Center for Media Engagement*. <https://mediaengagement.org/research/location-based-targeting-history-usage-and-related-concerns/>
- Jiang M, Fu KW (2018) Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit? *Policy Internet* 10(4):372–392. <https://doi.org/10.1002/POI3.187>
- Kaiser B (2019) *Targeted: My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy*. HarperCollins, London
- Kliman D, Doshi R, Lee K, Cooper Z (2019) *Grading China's Belt and Road*. Center for a New American Security. <https://www.cnas.org/publications/reports/beltandroad>
- Lee KF (2018) *AI Superpowers: China, Silicon Valley, and the New World Order*. Harper Collins, Boston
- Lyon D (2019) Surveillance capitalism, surveillance culture and data politics. In: Bigo D, Isin E, Ruppert E (eds.) *Data Politics: Worlds, Subjects, Rights*. Routledge, New York, pp 64–77
- Macaskill E, Dance G (2013) NSA files decoded: Edward Snowden's surveillance revelations explained, *The Guardian*, <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>
- Mayer-Schönberger V, Ramge T (2022) *Access rules: freeing data from big tech for a better future*. University of California Press, Oakland
- Moore M (2018) *Democracy Hacked: How Technology is Destabilising Global Politics*. Oneworld. Publications, London
- Moore M, Tambini D (2018) *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*. Oxford University Press, Oxford
- Qiang X (2019) The Road to Digital Unfreedom: President Xi's Surveillance State. *J Democracy* 30(1):53–67. <https://doi.org/10.1353/JOD.2019.0004>
- Roberts H, Cows 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>
- Roberts H, Hine E, Floridi L (2023) Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance. *Quo Vadis, Sovereignty?: New Conceptual Boundaries in the Digital Age of China*. Forthcoming
- Roberts H, Zhang J, Bariach B, Cows J, Gilbert B, Juneja P, Tsamadou A, Ziosi M, Taddeo M, Floridi L (2022) Artificial intelligence in support of the circular economy: ethical considerations and a path forward. *AI Soc* 1:1–14. <https://doi.org/10.1007/S00146-022-01596-8/METRICS>
- Ryan F, Cave D, Xu VX (2019) Mapping more of China's technology giants. *The Australian Strategic Policy Institute*, 24. <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2019-12/MappingmoreofChinastechgiants.pdf?VersionId=wpDVHlKgXJHzeK8rZ.kmy0Ei63RrXMO>
- Ryan F, Fritz A, Impiombato D (2021) Mapping China's Tech Giants: Reining in China's technology giants. *The Australian Strategic Policy Institute*, 46.

- <https://www.aspi.org.au/report/mapping-chinas-technology-giants-reining-chinas-technology-giants>
- Satariano A (2021) Google Loses Appeal of \$2.8 Billion E.U. Antitrust Fine, The New York Times, <https://www.nytimes.com/2021/11/10/business/google-eu-appeal-antitrust.html>
- Satariano A (2023) Meta Fined \$1.3 Billion for Violating E.U. Data Privacy Rules, The New York Times, <https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html>
- Saura García C (2022) El lado oscuro de las GAFAM: monopolización de los datos y pérdida de privacidad. *Veritas* 52:9–27. <https://doi.org/10.4067/S0718-92732022000200009>
- Saura García C (2023) El big data en los procesos políticos: hacia una democracia de la vigilancia. *Rev de Filosofía* 80:215–232. <https://doi.org/10.4067/S0718-43602023000100215>
- Schechner S (2021) Amazon Faces Possible \$425 Million EU Privacy Fine, The Wall Street Journal, <https://www.wsj.com/articles/amazon-faces-possible-425-million-eu-privacy-fine-11623332987>
- Scott J, Cremona M (eds) (2019) *EU Law Beyond EU Borders*. The Extraterritorial Reach of EU Law. Oxford University Press, Oxford
- Shahbaz A (2018) The Rise of Digital Authoritarianism. Freedom House. <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism>
- Sherman J (2020) The US Is Waging War on Digital Trade Barriers, *Wired*, <https://www.wired.com/story/the-us-is-waging-war-on-digital-trade-barriers/>
- Skinner BF (1938) *The behavior of organisms: An experimental analysis*. Appleton-Century-Crofts, New York
- Skinner BF (1965) *Science and Human Behavior*. Simon and Schuster, New York
- Skinner BF (1971) *Beyond Freedom and Dignity*. Hackett Publishing, Indiana
- Snowden E (2019) *Permanent record*. Metropolitan Books, New York
- Suroyo G, Kalra A, Potkin F (2019) Exclusive: U.S. helps Mastercard, Visa score victory in Indonesia in global lobbying effort, Reuters, <https://www.reuters.com/article/us-mastercard-usa-lobbying-exclusive-idUSKBN1WJ0IX>
- Sweney M (2022) EU claims Apple breaking competition law over contactless payments, *The Guardian*, <https://www.theguardian.com/technology/2022/may/02/apple-pay-contactless-payments-eu-competition-law>
- Sweney M (2023) European Commission bans staff using TikTok on work devices over security fears, *The Guardian*, <https://www.theguardian.com/technology/2023/feb/23/european-commission-bans-staff-from-using-tiktok-on-work-devices>
- The Australian Strategic Policy Institute (2021) *Mapping China's Tech Giants. Privacy Policies*, The Australian Strategic Policy Institute. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-05/Privacy-Policies_Mapping-Chinas-Tech-Giants_Thematic-Snapshot.pdf
- Wang M, Kaltheuner F, Klasing A (2023) The future of technology: Lessons from China. *Bull At Scientists* 79(3):170–173. <https://doi.org/10.1080/00963402.2023.2199595>
- Webb A (2019) *The Big Nine: how the tech titans and their thinking machines could warp humanity*. PublicAffairs, New York
- Woolley S (2023) *Manufacturing consensus: understanding propaganda in the era of automation and anonymity*. Yale University Press, New Haven
- Wylie C (2019) *Mindf*ck. Inside Cambridge Analytica's Plot to Break the World*. Profile Books, London
- Yun Chee F (2023) Breton urges more EU countries to ban Huawei, ZTE from networks, Reuters, <https://www.reuters.com/business/media-telecom/eu-countries-decision-ban-huawei-zte-networks-justified-eus-breton-says-2023-06-15/>
- Zhang A, Hoja T, Latimore J (2023) Gaming public opinion. The CCP's increasingly sophisticated cyber-enabled influence operations. *The Australian Strategic Policy Institute*, 71. <https://www.aspi.org.au/report/gaming-public-opinion>
- Zuboff S (2019) *The age of surveillance capitalism: the fight for the future at the new frontier of power*. Profile Books, New York

Acknowledgements

This study was made possible thanks to the funding received from Jaume I University through a predoctoral contract (PREDOC/2022/08) and 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

The author wrote and revised the manuscript. The author is fully and solely responsible for this manuscript.

Competing interests

The author declares no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Carlos Saura García.

Reprints and permission information is available at <http://www.nature.com/reprints>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2024