ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΣΧΟΛΗ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΔΙΕΘΝΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«DIGITAL TRANSFORMATION: E-CAMPAIGNING, E-DIPLOMACY, DIGITAL LAW»

ΚΑΤΕΥΘΥΝΣΗ: E-CAMPAINGING

Digital mass surveillance in authoritarian and democratic states

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Παναγιώτα Τσενέ

Αθήνα, 2024

Τριμελής Επιτροπή

Παντελής Βατικιώτης, Αναπληρωτής Καθηγητής Παντείου Πανεπιστημίου (Επιβλέπων)

Μαρία-Ντανιέλλα Μαρούδα, Επίκουρη Καθηγήτρια Παντείου Πανεπιστημίου

Σταύρος Καπερώνης, Επίκουρος Καθηγητής Παντείου Πανεπιστημίου

Copyright © Νίκος Πατεράκης, 2015

All rights reserved. Με επιφύλαξη παντός δικαιώματος.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας διπλωματικής εργασίας εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της διπλωματικής εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Η έγκριση της διπλωματικής εργασίας από το Πάντειον Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών δεν δηλώνει αποδοχή των γνωμών του συγγραφέα.

To my parents,

Stavroula and Panagiotis

Contents

Abstract 5
Introduction 6
Chapter 1 8
Mass Surveillance in the digital era 8
Chapter 2 13
Objectives of digital mass surveillance 13
2.1 Digital mass surveillance in authoritarian states 13
2.2 Digital mass surveillance in democratic states 15
2.3 Authoritarian vs. Democratic surveillance 17
Chapter 3 20
The tools and methods of mass surveillance 20
3.1 Authoritarian surveillance methods 20
3.2 Democratic surveillance methods 23
3.3 Authoritarian vs. Democratic surveillance methods 26
Chapter 4 28
Citizenship under mass surveillance 28
4.1. Participatory surveillance 28
4.2. Citizens as targets of mass surveillance 30
Chapter 5 34
Human rights, civil liberties and ethical consequences 34
5.1 Human rights and civil liberties 34
5.2 Ethical questions as a result of digital authoritarianism 36
Chapter 6 39
Conclusions 39
References 42

Abstract

Mass surveillance of citizens is not a new phenomenon, yet digital technologies have expanded its capacities and transformed its methods. Authoritarian states are often associated with the indiscriminate mass surveillance of their own citizens. Nonetheless, as the Snowden revelations proved, democracies have repeatedly engaged in mass surveillance of their population as well. National security, public safety and crime detection and prevention are usually mentioned as a pretext to justify constant monitoring. Regardless of the political system, governments seek to maintain the status quo and hence, any challenge to the interests of economic and political elites must be controlled. Surveillance serves this purpose, by allowing states to shape, predict and prevent "unwanted" actions, beliefs and behaviors. In addition, the collaboration between governments but also between governments and the private sector have exacerbated the consequences of online monitoring: from the violation of fundamental human rights and the enhancement of social inequalities, to the invasion of freedom and human agency. Citizens are apparently the targets of online mass surveillance, but they also play a participatory role in it, by generating and handing over their personal data to telecommunications and internet companies. Even though their role is rather unconscious and passive, they can rectify their power through counter-surveillance practices, once they understand the technological and socio-political aspects of digital mass surveillance.

Keywords: digital mass surveillance, mass surveillance, authoritarian states, democratic states.

Introduction

Mass surveillance and especially digital mass surveillance remains a contemporary and intriguing issue. Technological advancements have increased the capacities and intensity of mass surveillance and as a result, its consequences. In this light, states, both democratic and authoritarian ones, are watching over their own citizens on an unprecedented scale. It has been argued that surveillance is necessary for national security, public safety and prevention of crime. However, such reasoning has been used as a pretext in order to justify suppression of political opponents, prevention of mass mobilization and control over narratives and behaviors.

Additionally, indiscriminate monitoring and collection of personal data violates fundamental human rights and raises ethical dilemmas. Scholars put emphasis on the violation of privacy as the primary concern and see finding a balance between security and civil liberties as the solution. This is partially true, but far more is at stake. It is not only the freedom of expression and the right of assembly and association, it is also (self)censorship and the escalation of social inequalities and exclusion of certain social groups.

In academic research, mass surveillance and the consequent breach of fundamental human rights is often associated with authoritarian regimes. The repercussions of mass surveillance in the western democratic states are either ignored or undermined, leaving a theoretical gap regarding not only the ethical dilemmas but also the potential responses to them. In this regard, it is important to examine the aspects of digital mass surveillance in democratic states and in conjunction with authoritarian ones. In this way, I will attempt to display how mass surveillance is becoming a globalized threat to human rights and freedom on a transnational level and regardless of the political system. That is not to say that there are no differences, but rather to offer a comprehensive framework of digital mass surveillance, which enormously impacts the socio-political landscape.

The research question I pose is: what are the objectives, methods and tools, targets and consequences of digital mass surveillance in democratic and authoritarian states? I argue that democratic and authoritarian states have more similarities than differences, regarding their objectives, ways and outcomes of mass surveillance. Thus,

further discussion can focus on civil society's response to this globalized phenomenon of "digital authoritarianism".

In order to support my point, I examined the existing literature about mass surveillance since 2013, in regards with western democracies as well as authoritarian states. Especially after the Snowden revelations, there is a variety of academic papers and research conducted. By employing the method of desk research, I collected the necessary data from academic journals, specifically from *Surveillance and Society* and *International Journal of Communication* due to their relevance and academic rigor, as well as online search engines such as Google scholar and Jstor. For this reason, I used a variety of keywords, such as mass surveillance, digital surveillance, (western) democratic states and authoritarian states. I then evaluated and compared findings and arguments about surveillance on both democratic and non-democratic states.

Concerning the outline of the thesis, the first chapter consists of basic terms and a theoretical introduction to surveillance in the digital era. The second one explores the objectives of surveillance in authoritarian and democratic states. In the third chapter methods, technologies and tools which facilitate widespread and multilayered monitoring of citizens are presented. The fourth chapter analyses the role that citizens play as participants and targets of mass surveillance. The last chapter focuses on the ethical consequences and the violation of a series of human rights. The conclusion summarizes the findings about digital mass surveillance in democracies and autocracies.

Chapter 1
Mass Surveillance in the digital era

Information gathering had always been indispensable for states and surveillance was necessary in order to acquire knowledge about potential enemies and threats (Iiu, 2023). Today, surveillance remains relevant. Foucault's panopticon and the Orwellian state have been continually mentioned when one is referring to surveillance, since both of these paradigms attempt to describe the intrusiveness and anti-democratic consequences of a surveillant authority over citizens. Foucault explains how only fear and not even the actual act of surveillance is enough to make people change their behavior in order to comply and conform. Orwell, on the other hand, pinpoints the totalitarian nature of widespread and ongoing state surveillance.

Even though the aforementioned allegories give important insights into mass surveillance, technological advancements –from CCTV, smart devices, digital media to facial recognition, biometrics and machine learning, or as it is widely known, AI– make today's surveillance practices, methods and its consequences far more complex and multilayered. It is true that digital technologies have enabled people to raise awareness on certain topics, avoid the censorship of mainstream media and organize their actions (Zayani, 2019). They have also reduced participaton costs and facilitated information exchange (Ortiz, 2016). However, the initial optimism that the Web 2.0 and ICTs would democratize and increase political participation, is diminishing. The exact same technologies and digital means that were expected to enhance citizenship are now used by intelligence agencies and corporations in ways that restrict or undermine political engagement.

Notions such as "surveillance state" and "surveillance society" are used to describe this top-down extensive and invasive nature of mass surveillance as well as the effects that it entails (Lyon, 2017). However, according to David Lyon (2017), both of these terms are inadequate, as they fail to address the role that citizens and consumers play in their own surveillance. Instead, he proposes the term "surveillance culture" to highlight the bottom-up –willing, reluctant and/or ignorant– compliance and acceptance of citizens to give away their personal data.

It can be said that "surveillance culture" is reinforced by our dependence on digital technologies for a series of reasons, ranging from practical to psychological ones. In addition, the fact that surveillance is nowadays normalized in peoples' consciousness and deemed necessary for the common good further contributes to the "surveillance culture". This necessity is reflected for example in policy makers' declarations, that citizens have to exchange their data and thus their privacy with their access to the world wide web. Another aspect is the institutionalization of mass surveillance. As scholars, including Milan and Hintz (2018), have mentioned, especially after the Snowden revelations, states introduced laws that strengthen rather than limit surveillance practices. Even in cases where there are established regulations in favor of privacy and individual autonomy, governments can and do yield the law in order to carry on with their surveillance practices, programs and methods (Laperruque, 2019).

Thus, mass surveillance comes to be understood as an inevitable aspect of modern societies. It is no coincidence that one of the definitions states that surveillance is the "purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection" (Surveillance Studies Network, 2006, p.3). Nonetheless, the words "purposeful" –that is occurring for a justified goal– and "systematic" –i.e. not random (Surveillance Studies Network, 2006, p.3) are nowadays debatable. Mass, compared to targeted surveillance, does not target only suspects of wrongdoing but entire populations (House of Lords, 2009), posing ethical questions and dilemmas.

Both, *Privacy International* and *Amnesty International* use the word "indiscriminate" to refer to mass surveillance. In particular, *Amnesty* (2015) explains that "indiscriminate mass surveillance is the monitoring of internet and phone communications of large numbers of people – sometimes entire countries – without sufficient evidence of wrongdoing" (para. 3). While *Privacy International* (n.d) focuses more on the violation of citizens' fundamental rights, including privacy and freedom of expression and assembly: "mass surveillance can subject a population or significant component thereof to indiscriminate monitoring, involving a systematic interference with people's right to privacy and all the rights that privacy enables, including the freedom to express yourself and to protest" (para. 2).

This bulk monitoring of individuals' online and offline activities is indiscriminate and invasive exactly because it includes the interception and analysis of vast and variable data, like phone calls, transactions, emails, internet searches, as well as personal information extracted from governmental services and social media (Amnesty, 2015). Recent technologies, analytics tools and AI are further enabling what has been called "dataveillance", the collection and processing of personal data and metadata (Kabanov, Karyagin, 2018). Personal data can incorporate information of one's age, gender, sexual orientation, education, marital status, religious and political affiliations. Metadata is often described as the "data about data" and varies from location, identity and duration of a communication to word processing (Lyon, 2014).

In order to mine, collect and process all these (meta)data, governments cooperate or enforce cooperation with the private sector. In either case, it would be misleading to focus only on the government as the primary agent of conducting surveillance. Lyon (2017), for instance, mentions that surveillance is also an industry. Private companies in the West, such as the Big Five (Google, Microsoft, Apple, Meta, Amazon) as well as Chinese companies like Huawei, Alibaba, Tencent and Baidu carry out mass monitoring of their users and interception of their personal information, even though in different socio-political and historical contexts. Personal data is then shared with intelligence agencies and law enforcement, unavoidably leading to the blurring of the lines of accountability between the private and public sphere.

Hayes' "surveillance industrial complex" perfectly describes the aforementioned public-private interconnected and interdependent partnership (Nurik, 2022) and thus the capacities that such collaboration entails for society and citizenship. In addition to "surveillance industrial complex", "surveillance capitalism" is used to particularly articulate the engagement of private corporations in surveillance practices. Shoshanna Zuboff (2020) explains how our data is extracted, monetized and sold by private companies to businesses and marketing agencies, in order for them to know, predict and eventually control our (purchasing) behavior. As a consequence, a "coup from above" takes place, where citizens unconsciously succumb to surveillant capitalists' needs and desires (Zuboff, 2020).

What is more worrisome is what she refers to as the "seventh extinction" resulting from the knowledge and power asymmetry that surveillance breeds for the

watchers and against those who are being watched (Zuboff, 2020). Specifically, the seventh extinction is the extinction of human agency and personhood, indicating that not only will our actions and reactions be controlled but our desires and needs will not even be ours in the first place. In this case, the ethical price and political cost for the future of citizenship and democratic participation is unfathomable.

Mass surveillance extends simply the act of "watching over", since it encloses the "intention and capacity to control" citizens' behavior and reactions (Iiu, 2023). And even though, in the public discourse, the monitoring and controlling of citizens is often associated with authoritarian regimes, that is not always the case. Incidents like the Wikileaks, the Snowden revelations and the Cambridge Analytica scandal brought to light significant information not only about the methods and the data that are exploited and the dynamic relationship of governments with the private sector but they also made clear that western democratic countries do spy on their own citizens as well. For instance, during the 2016 elections in the USA, Cambridge Analytica played a significant role in the victory of Donald Trump. The company did so by segmenting American citizens according to their personality. In particular, it used a five-factor personality model --that included openness, conscientiousness, extroversion, agreeableness, and neuroticism (OCEAN)-- in order to rank individuals and offer accurate predictions on their current and future behavior (Chester & Montgomery, 2017).

Mass surveillance has been employed by states all over the world in the name of national security, crime prevention and combating terrorism. Especially after the 11th of September and the declaration of "war on terror", surveillance practices were augmented (Franks, 2017, p.433). Likewise, the Covid-19 pandemic offered a solid ground for monitoring and restricting certain actions and aspects of everyday life (Königs, 2022). The pandemic brought forward the "state of emergency" which justified the expansion of governmental power in the name of public safety (Csernatoni, 2020). The latter was apparently evident in China. This is not surprising, since the Peoples' Republic and Russia are regarded as leading examples of authoritarian states which exploit the advances of technology to control and shapeshift their peoples' behavior in wide and subtle ways. Nevertheless, new

technological opportunities have also given democracies, and primarily the United States greater opportunities to largely monitor their citizens.

The deployment of information technology by states in order to surveil, exert control, repress, citizens and strengthen their rule is described as “digital authoritarianism” (Mantellasi, 2022). Its tactics range from misinformation campaigns, internet shutdowns and censorship to the deployment of trolls. What is interesting here is that, while in general, there is acknowledgement that democratic states also engage in surveillance practices that reinforce rather than limit digital authoritarianism, scholars often refer to authoritarian states when defining digital authoritarianism. For instance, Wilson (2022) notices that intrusive surveillance is evident in countries like South Korea, United Kingdom and the United States as much as it is in China and Russia, and concludes that “digital authoritarianism is now a generalized feature of nation-state governance” (p. 712).

In the next chapters, I will discuss in detail democracies’ and autocracies’ approach to mass surveillance.

Chapter 2
Objectives of digital mass surveillance

Examining the objectives of digital mass surveillance is important so as to understand the complicated social and political environment in which such practices take place. Mainstream narratives portray surveillance as necessary for security purposes, but it is important to comprehend that there may exist underlying causes that often include social control, repression and the accumulation of power by certain social groups in the detriment of collective well-fare. What follows is an unpacking of mainstream narratives and counter-arguments, which will help shed light into the implementation and motives of mass surveillance in authoritarian and democratic societies.

2.1 Digital mass surveillance in authoritarian states

Authoritarian states have been criticized for the deployment of surveillance practices in a wider context to control and suppress their populations, while digital tools have further increased their capacities and reach of mass surveillance. And despite the 2011 anti-authoritarian uprisings in the Middle East where social media acted as a facilitator for mobilization and political expression, regimes have learnt to use the exact same means to stifle collective action. Russia and China are leading examples and serve as role models in the technological and regulatory field of surveillance as well as in its implementation methods, which will be discussed in the next chapter. Bt first of all, it is important to discuss the official governmental arguments in favor of mass surveillance and afterwards analyze the main counter arguments.

The necessity of surveillance is almost always justified for reasons of national security. It is very common for states to introduce laws that enable constant surveillance and allow intelligence agencies to access citizens' personal information, without their consent or adequate indications of wrongdoing, under the auspices of anti-terrorism. For instance, the "Yarovaya package" introduced by the Russian government extends the period of data storage and permits access of intelligence agencies (Kabanov & Karyagin, 2018). The CCP, on the other hand, in its proclaimed attempt to combat terrorism, mafia and organized crime (Jiang, 2020), has leveraged

digital technologies and several projects, such as SkyNet and Sharp Eyes in order to monitor its population. In addition to this, China is promoting “mass reporting”, where citizens are obliged by law to report “suspected terrorist activities” and individuals (Jiang, 2020). This ostensibly bottom-up initiative has as a mere goal to establish the legitimacy of the extensive surveillance practices of the CCP (Jiang, 2020).

Mass surveillance is also justified for public safety purposes (Stoycheff et al, 2018). Covid-19 pandemic enabled governments to impose wider monitoring of everyday activities and restrict mobilization. In Meiyuan, China, the facial recognition system is supposed to “protect the neighborhood” (Jiang, 2020). Except for public security, “internet sovereignty” implemented by both Russia and China, is presented as a means to combat terrorism and extremism (Michaelsen & Glasius 2018). In reality, however, internet sovereignty, that is China’s Great Firewall and Russia’s Runet, coupled with propaganda from governmental media, have isolated their populations from the outside world (Khalil, 2020).

On the other hand, vague notions such as “terrorism” and “extremism” can be expanded to include any dissenting voice or action. They have been used by the Chinese government to target Muslim minorities and ban their religious activities and to suppress scholars that do not comply with the Chinese political agenda (Jiang, 2020). Digital repression is also enhanced by the Great Firewall, through which the CCP can track and suppress political expression and manipulate public opinion and behaviour (liu, 2023). Indeed one of the objectives of mass surveillance in authoritarian states, is to control peoples’ beliefs and increase the government’s legitimacy (Kendall-Taylor et al, 2020). Russia is extremely adept at online misinformation campaigns and at spreading pro-regime propaganda, while also limiting criticism, especially following the invasion in Ukraine (Frantz et al, 2020; Ünver, 2024).

Some scholars argue that the main threat to authoritarian regimes is protests (Frantz et al, 2020), hence surveillance aims at preventing mobilization, maintaining social control and “preventive repression to address threats before overt mass protests” take place (Xu, 2020). For example, China has engaged in preventive arrests to counteract collective action (Frants et al, 2020), while the Skynet program has allowed police to surveil protesters (liu, 2023). Additionally, surveillance and its

chilling effects, not only suppress political action but they also silence opposition and intimidate citizens from mobilizing (Kendall-Taylor et al, 2020). Lastly, it is interesting to mention that according to Iiu (2023), China's Sharp Eyes project limits protests but does not have any effect on criminal rates. This is proof that national security and public safety are mere pretexts for justifying higher and wider suppression and social control.

2.2 Digital mass surveillance in democratic states

Democratic states have been presented as the guardians of human rights that need to proselytize authoritarian regimes and watch over them in case of civil liberties violations. In the public discourse, it is often stated that democracies deploy surveillance practices for legitimate purposes and only when it is deemed necessary. Some scholars even argue that democracies are less likely to monitor their populations in order to target opposition or marginalized groups (Königs, 2022). Instead, surveillance is supposed to "facilitate governance through social control for social ends of fairness, justice and equality" (Monahan as cited in Miyamoto, 2020, p. 49). Monitoring and storing of personal data is viewed as indispensable for effective governance and as a consequence justified and accepted.

Moreover, national security and law enforcement are the main declared reasons for conducting mass surveillance. Especially after September 11, 2001, the war effort against terrorism enhanced the "surveillance state" (Lyon, 2014). In an attempt to prevent such crimes, many countries and specifically the United States intensified their surveillance initiatives. A series of anti-terrorism acts enabled the interception of personal data and vast monitoring in pervasive and extensive ways. Terrorism and the "politics of fear" has hence normalized mass surveillance and the consequent violation of privacy for the sake of an imagined national security (Schleusener, 2018).

In a broad sense the detection and prevention of crime, public safety and the safeguarding of the "common good" are often used to justify constant surveillance of citizens. That is, by continuous monitoring, authorities can efficiently maintain stability and security. For example, the limitation of the Covid-19 spread (Bibri et al,

2022), a high priority in the political agendas in 2020-2022, served as an opportunity for more extensive and invasive monitoring of individuals. Indicative of this are the cases of South Korea, Taiwan and Israel which used surveillance technology and methods for the absolute enforcement of lockdown measures (Königs, 2022).

Nonetheless, surveillance and the law framework, such as that of anti-terrorism, has been exploited to rather limit and restrict dissent. Giroux (2014) argues that this vague war against terror has turned every citizen into a suspect and every public space into a war zone. But even if this was an appropriate response, Lyon (2014) explains how trying to find "terrorist needles" in "big data haystacks" poses practical questions on the efficiency of such attempts. The pre-emptive nature of surveillance practices further complicates the situation. Instead of investigating criminality, surveillance serves as an annihilator of online political participation and expression, restricts collective action, targets dissidents, suppresses marginalized groups and intimidates citizens from mobilizing (Königs, 2022).

The control of Information and Communication Technologies (ICTs), the subsequent chilling effects and the state's need to interfere before incidents take place, has led citizens to refrain from certain online and offline political actions, because they fear prosecutions and do not trust the legal system (Hintz & Milan, 2018). There are numerous examples of the state abusing the power that comes with surveillance. In Britain and the United States, police have monitored social media in order to make pre-emptive arrests before protests even take place or to raid dissidents' houses (Earl, 2022). Targeting political groups and social movements is also an established practice in these countries (Hintz & Milan, 2018; Earl, 2022), for example the FBI has been spying on Black Panthers and anti-war activists (Giroux, 2014).

Greenwald (as cited in Hintz & Milan, 2018) has very eloquently expressed the interplay of chilling effects, public consciousness and political action: "mass surveillance kills dissent in a deeper and more important place as well, in the mind, where the individual trains him- or herself to think only in line with what is expected and demanded". Neoliberalism facilitates the rise of surveillance and surveillance sustains neoliberalism. As economic and political elites seek to maintain and increase their power, they will inevitably impose restrictions in actions and voices which

challenge them (Giroux, 2014). It is not uncommon for governments to defame activists and whistleblowers so as to minimize their credibility and their overall effect on public consciousness. After the Snowden revelations, the US accused Snowden of traitorship and several journalists of conspiring in favor of terrorism (Giroux, 2024).

Surveillance overall can be viewed as a zero-sum game. Where it increases and favors the concentration of power in the hands of states and corporations, it disempowers citizens and their capacity to instill change (Hadjimatheou, 2013). Controlling the communication flows allows governments and economic elites to shape and manipulate public opinion in ways that justify and serve their own interests (Wang et al, 2022). An example of this is the deployment of extreme monitoring and tracking in order to enforce laws that are not widely accepted or criticized (Königs, 2018). Drawing from the practices of USA and the FBI, Giroux (2014) explains how surveillance has been used by states as a way to facilitate or cover up illegal acts, such as committing serious crimes or wrongfully accusing people. The United States are pioneers in voter management software. Voter surveillance is also an important aspect of mass surveillance (Bennet, 2015) as it aims to manipulate voters through marketing "nudges". Finally, voters turn into consumers, instead of the opposite (Bennet, 2015).

2.3 Authoritarian vs. Democratic surveillance

All in all, it can be said that both authoritarian and democratic states have been engaging in mass surveillance methods on their own citizens for a series of reasons, making evident the rise of digital authoritarianism, that is the use of digital tools for authoritarian purposes (Chapter 1). The practices and official narratives of Russia, China and the United States indicate that mass surveillance is frequently justified for purposes of national security. An easily accepted objective by the public in the wider socio-political context of nation-states and the construction of an outside enemy that we must be protected from, even if it automatically means that we are deprived of our privacy and freedom.

Anti-terrorist regulations and measures, which often include extensive interception of data, fall under this category as well. Of course, this is not to deny the

existence of terrorism and terrorist organizations or the threat that they pose, but rather to remind that the exploitation of certain incidents or situations in order to safeguard the interests of political and economic elites in the detriment of the collective welfare is also a crime that needs to be prevented. Secondly, public safety and the "common good" are also used to justify surveillance by autocracies and democracies. They often go hand in hand with law enforcement and the consequent restrictions in offline and/or online actions, as the recent Covid-19 crisis showcased. In general, efficient governance, "law and order" have come to justify in people's minds the collection, storing and analysis of their personal information for their "own good" which is apparently dictated "from above".

Despite the aforementioned arguments in favor of mass surveillance, which are supported by governments all over the world and also by scholars, the literature suggests other objectives exist as well. Monitoring, tracking and targeting dissidents, journalists, marginalized groups and whomever is likely to demand social change and challenge the status quo is one of the aims in authoritarian and democratic states. Because both regimes require stability, and because collective action in its very nature seeks to change the power balance, surveillance aids governments to maintain this stability (Frantz, 2020). Controlling the information flows allows the state to manipulate public opinion and consciousness. In this sense, governments can aim to increase their legitimacy or enforce laws and policies that would not otherwise be accepted or implemented.

Governments not only need to control anyone who challenges their power but also to prevent political actions, mobilization and even online criticism. The chilling effects of surveillance, censorship, the fear of punishment and the defamation of activists serve this objective perfectly. The surveillance -democratic or authoritarian- state attempts to acquire absolute control over our beliefs, consciousness, actions and reactions in an effort to sustain and boost its power. Hadjimatheou (2013) argues in her research that: "the use of power for authoritarian purposes is unacceptable; surveillance leads to the use of power for authoritarian purposes; therefore, surveillance is unacceptable" (p. 2). Regardless of the political system, digital repression as a consequence of mass surveillance has escalated (Franz, 2020). For

understanding wholly the dynamics of mass surveillance, it is worth analyzing the methods and partnerships that mass surveillance involves, in the next chapter.

Chapter 3
The tools and methods of mass surveillance

Analyzing the surveillance methods that democracies and authoritarian states deploy, it will provide a clear framework of the different variations that surveillance can take. Whether low-tech or high-tech digital tools enable extensive monitoring, while the established laws and narratives justify mass surveillance of citizens. It is also essential to recognize the multilayered levels of cooperation between different actors for either commercial or monitoring causes. The next subchapters offer a in-depth analysis of these issues.

3.1 Authoritarian surveillance methods

The controlling and policing of the population, the suppression of political action, limitation of criticism and the strengthening of the regime through mass surveillance, all contribute to the sustenance of the status quo and the concentration of power in the hands of economic and political elites. Mass surveillance involves the state and the private sector which aim to collect, store and analyze as much data as possible for future use, in an attempt to pre-empt mobilization or challenges to the authoritarian rule. Digitally advanced countries such as China have developed, produced and exported surveillance tools and methods to other states that aspire to control their population to an extreme extent as well (Xu, 2020). The web 2.0 and ICTs have facilitated the access of intelligence agencies to personal information, as we live in a more and more interconnected environment and hence traces and data can be found on social media, web searches, online transactions and so on and so forth.

Technological advancements, like AI, Internet of Things (IoT), facial recognition and high resolution cameras further enable states to repress and suppress. For example, the Golden Shield project in China, even though it started as a project to support police officers, and initially included ID systems, population databases and street cameras has now been enhanced with AI, facial recognition systems and big data accumulation (Xu, 2020). The CCP in this way, aims to build both an online and offline surveillance system that is intertwined and leaves no blind area (Polyakova

&Maserole, 2019). Added to this, the Golden Shield attempts to facilitate information sharing between the Ministry of Public Security and local authorities (Jiang, 2020). It is evident then that the chilling effects of surveillance, the (self)-censorship and im-mobilization are enhanced.

Nonetheless, literature suggests that authoritarian rulers are uninformed in regard to public sentiments (Xu, 2020), showcasing that censorship is double-edged; it may restrict criticism against the government, but it also makes it difficult to gauge public opinion. For this reason, autocracies attempt to solve the information deficit by using digital tools. Ranging from internet shutdowns and digital surveillance to online harassment and cyberattacks, states are able to target political opponents and dissidents, thus avoiding indiscriminate repression and a possible backlash (Xu, 2020; Lamensch, 2021). The Chavez regime in Venezuela has used digital tools so as to target and punish political opponents (Xu, 2020). Research suggests that Chavez opponents had a decrease in income levels and increase in unemployment rates.

Disinformation campaigns and online censorship are common practices of digital authoritarianism. Autocracies can easily shape narratives and citizens' beliefs and sentiments towards the regime and sensitive social issues. "Microtargeting", that is targeted dissemination of information, and artificial images and videos or "deepfakes" as it is called, can be used to manipulate information, defame political opponents and undermine dissidents' credibility (Frantz et al, 2020). Publicly shaming activists as terrorists or traitors and accusing them of having criminal or mentally-unstable background (see Daryaei Ahoo case in Iran) is not new. Russia is known for its disinformation capabilities. Frantz et al (2020) argue that the Russian Federation is an expert at diffusing pro-government information, diverging the attention of the population from important matters and controlling critical voices.

This is also achieved with the deployment of "trolls" or automated accounts-bots, which are used to blur reality, mislead, amplify support for governmental policies, discredit and "bury" anti-regime views (Kendall-Taylor et al, 2020). On the other hand, those who express negative opinions towards the regime can be criticized for spreading "fake news" and even be prosecuted under respective laws and regulations (Shahbaz, 2018). Nonetheless, authoritarian states do not only surveil their opponents and critics, they also monitor their subordinates and other members

of the political elite. For instance, the CCP, through citizens' posts on Weibo, gains knowledge about local authorities. (Kendall-Taylor, 2020). In this context, governments allow citizens to report on different issues, such as pollution, via apps or polls (Egger, 2023). It is argued that "e-governance and e-participation" favors the sustenance of authoritarian rule (Kabanov & Karyagin, 2018).

China's mass reporting system aims at enhancing this bottom-up surveillance practice. In Xinjiang, citizens are encouraged to inform authorities about each other under the pretext of anti-terrorism measures (Jiang, 2020). Except for this, the Great Firewall is an initiative aimed to create a sovereign internet that is wholly controlled by the Chinese government. It filters and blocks content and websites that are regarded as inappropriate with the aid of telecommunication companies (Frantz et al, 2020). Moreover, the "Sharp Eyes", a video surveillance project coupled with facial recognition and high-resolution cameras is aspired to cover every region, leaving "no blind spots" (IPVM, 2018). At this point, it is necessary to discuss the notorious "social credit system". The term refers to a surveillance system which deploys high-tech in order to monitor and control the population. The social credit system attempts to "measure" how trustworthy a person is, according to its behavior and actions (Kendall-Taylor, 2020). The trustworthiness or lack thereof leads to benefits and rewards or to the exclusion from it respectively.

China along with Russia are role models for other authoritarian states in the field of mass surveillance and the implementation of the "internet sovereignty". China's technologically advanced surveillance tools and methods are being exported to a series of states, while Russia's low-tech surveillance model serves as a leading example in less advanced countries (Polyakova & Maserole, 2019). Russia combines both technical and legal methods coupled with disinformation and censorship in order to control its citizens. The Yarovaya package of laws demands telecommunication companies to store personal data for longer periods of time and also provide access to the *Federal Security Service*, FSB (Polyakova & Maserole, 2019). In addition to this, the Kremlin has installed a video surveillance system, called "Safe City" that allows the authorities to intercept a variety of data (Polyakova & Maserole, 2019).

What can be observed is that governments are collaborating with the private sector and with each other. For example, Hikvision, a Chinese tech company, is

providing the government with surveillance equipment, while the state invests in AI start-ups (Polyakova & Maserole, 2019). The private sector is, willingly or not, in cooperation with the state and is also producing and exporting its dual-use technology for surveillance and censorship purposes (Khalil, 2020). Autocracies share and exchange surveillance practices, knowledge and technology. China has not only exported its surveillance tools to many other governments, including Pakistan, Kenya, the United Arab Emirates, but has also provided training on how to use them (Iiu, 2023; Khalil, 2020). On the other hand, Russia's main exporting countries are those of the former Soviet block (Polyakova & Maserole, 2019).

3.2 Democratic surveillance methods

Taking advantage of the fact that citizens use the internet to express their beliefs and organize collective action, democratic states have continuously deployed mass surveillance practices so as to control and restrain political mobilization. Social media platforms are the source of vast amounts of personal data, including content and metadata. Technologies such as IoT, AI, blockchain, big data (Bibri et al, 2022) are exploited in order to implement a surveillance system that monitors citizens, collects and analyzes their data. “Datafication”, the process of turning actions, behaviors, relationships and consequently humans into measurable data, has enabled communication companies to watch over citizens and consumers in order to predict their actions (Bibri et al, 2022).

Broadly speaking, the surveillance method of “dataveillance” requires and enhances the cooperation of states and the private sector. The rise of the surveillance industrial complex allows intelligence agencies, like the American NSA or the British GCHQ , to intercept data in a routine and indiscriminate way, often without a warrant, directly from the servers of telecommunication and internet companies such as Google, Facebook, Apple, Microsoft, YouTube, Skype and Amazon (Hintz & Milan, 2018; Giroux, 2020). Governments heavily rely and depend on the private sector, as the former lacks skills, technology, and infrastructure (Miyamoto, 2020). The private sector also provides governments the know-how and “cyberweapons”, such as Pegasus, Predator and the Devil’s Tongue. Such surveillance tools and software are

responsible for extracting sensitive information from smartphones, while they are extremely difficult and expensive to detect. Additionally, the private sector, that is, primarily US-based companies, owns the majority of the internet infrastructure and thus the regulation of cyberspace reflects the interests of private corporations and in particular those of advanced western democracies (Gamal, 2020).

It is thus an interconnected and interdependent relationship that benefits from extracting, collecting and proceeding citizens' personal data for commercial and controlling purposes. Surveillance capitalism describes the increasingly intrusive role that corporations play in our everyday life, since they commodify every aspect of the human experience for the sake of profits. As Bibri has noticed, surveillance capitalism includes "dataveillance, geosurveillance, and anticipatory governance as a means to advance the hidden agenda of the ruling corporate and governmental elites" (Bibri et al, 2020, p. 721). Zuboff (2020), furthermore, explains how this corporate-driven surveillance breeds "extreme asymmetries in knowledge and power", enhances social inequalities and imposes new forms of social control. In general, neoliberalism has shifted the power relations and decision making from the state to big corporations (Bibri et al, 2020). This also entails a shift in responsibility in regard to internet monitoring and the safeguarding of online rights and duties (Hintz & Milan, 2018).

An interesting aspect of mass surveillance in democracies is the fact that it has become institutionalized, despite arguments that in democratic political systems there are laws and safeguards that protect human rights from extensive and indiscriminate state surveillance. Following the Snowden leaks, governments reformed the law framework only to legalize surveillance practices. A series of democratic states have passed legislation to strengthen the capabilities of large-scale state and corporate surveillance, such as bulk collection of data (Padden, 2023). Examples include Britain, France, Germany, the Netherlands and Denmark (Michaelsen & Glacius, 2018; Hintz & Milan, 2018). In other words, democracies have normalized and legitimized surveillance, through legislation and public discourse. Padden (2023) pinpoints the difference in language when surveillance is described as authoritarian and when it is "branded" as a neutral tool, which promotes efficiency and security.

This has led law enforcement to act pre-emptively, instead of reactively, establishing a punitive state and raising ethical questions regarding the presumption of innocence. Security agencies are able to monitor and track citizens' whereabouts, communications, purchase history, health and educational background (Giroux, 2014; Padden, 2023). They also have access to biometric data, such as fingerprints, DNA, and genetic codes "assembled from technologies once conceived for criminals" (Giroux, 2014, p. 118). Technologies, such as GPS, CCTV, satellites, drones and facial recognition, have enabled the interception of such extensive information on the population (Schleusener, 2019). Police, in addition, have exploited the social media affordances –creating fake accounts, combing activists' social media and so on– in order to monitor dissidents and social movements as in the case of Black Lives Matter, where police were monitoring protesters via Facebook (Nurik, 2022).

Broadly speaking, intelligence agencies deploy a variety of surveillance technologies and methods, such as interception of data via internet cables –an example of this is the British Tempora program– hacking and penetrating encryption (Hintz & Milan, 2018). The Tempora program used by the GCHQ (General Communications Headquarters) and the PRISM program used by the NSA (National Security Agency) grant direct access to the servers of big internet corporations (Lyon, 2014). It is worth mentioning that the NSA and GCHQ have been characterized as the "main enemies of the internet" due to exactly these kinds of invasive surveillance practices, which undermine political expression and instill (self)-censorship. Lyon (2014) explains how the NSA cooperates with telecommunication and internet companies as well as with contractors so as to mine, store and filter data for potential future use, in an attempt to control behaviors and incidents before they even occur. What is also interesting in the NSA's case, is that it analyzes behavioral patterns to reveal relationships between individuals or monitors "untargeted" citizens in case they are connected or referring to "targeted" individuals (Sinha, 2013).

Western democratic states, such as the United States, France and Germany produce and export surveillance technology and know-how. Digital authoritarianism has been particularly enhanced by the surveillance equipment that is developed in the west, by private corporations (Lamensch, 2019; Miyamoto, 2020). For instance, Belarus was able to block websites during the 2020 protests, thanks to the technology

acquired from the American Sandvine. The French Nexa and Amesys faced charges for complicity in torture and enforced disappearance, as they have exported equipment to Libya and Egypt (Lamensch, 2019). Mantellassi (2023) supports that digital authoritarianism is "western in origin", since western democracies deploy and sell their surveillance tools to both authoritarian and democratic states. An example of this is Iran, which is equipped with such technology originally manufactured in the west (Michaelsen, 2017).

In general, democratic governments cooperate with each other, sharing knowledge and expertise. They also cooperate with private internet and technology companies, as the case of the Five Eyes indicate, where the governments of the United States, United Kingdom, Canada, Australia and New Zealand demanded from companies to create "back doors" into their encryption technology (Shahbaz, 2018). This surveillance apparatus includes multilayered collaboration with universities, social media platforms and outside contractors as well (Lyon, 2014). The above surveillance complex partnerships coupled with propaganda and misinformation that is evident in democracies as well (Glasius, 2018), further boosts the surveillance state.

3.3 Authoritarian vs. Democratic surveillance methods

Mass surveillance, whether in authoritarian or democratic states, reflects the invasive role of states, corporations and technology in the construction of social life and the shaping of the political future, signifying the rise of digital authoritarianism. A "coup from above" is taking place, positioning citizens in an almost completely passive role in the decision-making processes. Our future and precedent is shaped and defined by algorithms, made for suppressing and controlling human agency and free will. The cooperation between intelligence agencies, local authorities and the private sector highlights the advance of "surveillance capitalism" and the increasing power accumulation to the private sector in relation to the state.

Disinformation campaigns and propaganda are a customary practice in both political regimes. The control of information flows can take diverse forms: filtering and blocking content or disregarding it as "fake news", without changing the outcome which is nothing else but censorship. Different governments have employed different

surveillance programs and projects aiming to extract data that helps them predict and prevent undesirable outcomes. This is possible through technological tools, like AI, facial recognition, CCTV, social media, transactions and search history monitoring and though the “back doors” that states create in order to break encryption.

The legitimization and normalization of surveillance for the “common good” and public security further complicates the ethical consequences. Whether high or low tech, surveillance is an inherent element of contemporary nation-states. Regardless of the political system, the methods of conducting and implementing surveilling practices are similar. Glasius and Michaelsen (2018) support that (digital) authoritarianism is not restrained in the borders of autocracies but has become a global phenomenon. Exports of surveillance equipment from and to, both, authoritarian and democratic states, as well as the collaboration between governments is indicative of the globalization of mass surveillance authoritarian practices. Schleusener (2019) points out how governments of otherwise different political regimes with supposedly different social values are “united” in monitoring their own citizens.

Chapter 4
Citizenship under mass surveillance

4.1. Participatory surveillance

Democratic and authoritarian states engage in extensive mass surveillance of their own citizens so as to predict, control and shape their beliefs and actions in an attempt to preserve the status quo and limit any challenges to the power structures. Surveillance has been normalized and institutionalized in the name of the abstract notions of national security and public safety. Governments often cooperate with each other, exchange technology and knowledge, methods and surveillance models. The role of the private corporations is also deemed indispensable in both political systems, as they are the ones who provide intelligence agencies with technology and data or simply allow them access to users' personal information. Citizens complete the puzzle, since they take part in their own surveillance, yet in unconscious or passive ways.

Users generate personal data and hand them over to telecommunication and internet companies, accepting in this way and complying with digital surveillance (Lyon, 2017). Once online, people create a vast amount of data regarding their social, economic, political and educational background. Personal information can be mined through search histories, transactions, messaging apps, through social media accounts or simply interactions on posts, such as likes, shares and comments. They often accept "cookies" and agree with "terms and conditions" without being fully aware of what this actually entails for their privacy. By consenting to this, users allow companies to collect, store, analyze and share their personal data with third parties and law enforcement for commercial and policing purposes respectively.

It can be argued that this is happening for three reasons. First, individuals have been used to living and operating under this complicated and noncomprehensive surveillance environment, which also partly explains why there is no wide and organized resistance (Schleusener, 2018). Second, citizens are in general, ignorant of the internet infrastructure and the data collection and monitoring processes (Hintz & Milan, 2018). The lack of digital literacy and the complex digital environment contribute to this passive acceptance of constantly being tracked and monitored. Lastly, even if they are aware of digital surveillance and its consequences, they are not

provided with alternative choices but to close the website or log out from their social media profiles (Hadjimatheou, 2013). For example, oftentimes in order to browse a website, users must either accept "cookies" or exit the page. Users are thus treated as human sources of raw material, i.e. data, which is monetized and sold by corporations for commercial interests. Zuboff (Laidler, 2019) explains this practice:

> as the unilateral claiming of private human experience as free raw material for translation into behavioral data. These data are then computed and packaged as prediction products and sold into behavioral futures markets — business customers with a commercial interest in knowing what we will do now, soon, and later (para. 8).

The fact that surveillance is normalized and justified –whether through the legal framework or the language used in public discourse in order to describe such practices– in the perceptions of most citizens further complicates the situation. Wirth et al (2019) describe two main arguments which make citizens accept and participate in their surveillance and in detriment of their civil liberties and fundamental rights. The first one revolves around the concept of "perceived security", where individuals regard mass surveillance as necessary for the prevention of crime and terrorism. They accept this trade-off between security and privacy and the fact that more surveillance means more security and more security means less privacy. The second one refers to the statement of "I have nothing to hide". It is acceptable for intelligence agencies and the state to acquire personal information, since there is the belief that only criminals have something to hide.

Mass surveillance and the role of citizens in it as it was described above, contradicts and diminishes the initial optimism that the internet will facilitate political participation and enhance democracy across the globe. Citizens, willingly or not, give up their privacy and exchange it with superficial entertainment and social interactions. They become not only the object of surveillance but also participants and subjects (Giroux, 2014) . The same tools that were thought to enable political expression, collective action and greater access to information are deployed by intelligence agencies and the state in order to target political opponents, dissidents and

journalists, as well as to limit criticism and control the narratives through propaganda and disinformation campaigns.

4.2. Citizens as targets of mass surveillance

As I have previously argued, states, whether democratic or authoritarian, desire stability and the preservation of the existing power structure. Dissenting voices and collective action, such as social movements, on the other hand, seek social change and thus are viewed as threats to the regime's stability. Boghosian (2013), among others, argues that freedom and self-determination are incompatible with surveillance carried out by governments in collaboration with the private sector and states that: "by claiming that anyone who questions authority or engages in undesired political speech is a potential terrorist threat, this government-corporate partnership makes a mockery of civil liberties". Mass surveillance, censorship and digital repression serve as preventive measures to limit and control protests. Dissidents, protesters and activists are one of the categories of citizens which are affected by the state-industrial surveillance.

The United States and Britain have continually tracked and monitored political groups and organizations, including *Amnesty International*, *Doctors of the World* and *Human Rights Watch* and also citizens that simply engage with political content, blogs or websites (Hintz & Milan, 2018). For example, after the Wikileaks incident, the GCHQ started monitoring individuals that would visit the site. This preventive monitoring is aimed at predicting and interfering before certain behaviors and actions take place or certain beliefs become established. Specifically, surveillance technology in this context is used to detect and filter users' or political organizations' content about protests and political mobilization. China blocks posts that could initiate online or offline mobilization. Democracies on their part, in collaboration with Google and Meta, restrict relevant content in times of internal political upheaval (Stoycheff et al, 2018).

Furthermore, law frameworks which have been introduced for national security reasons serve the surveillance state rather than the safety of citizens. Russia, for instance, has utilized the supposedly anti-terrorist "Yarovaya law" in order to suppress protesters, silence critics and target independent media (Polyakova &

Maserole, 2019; Ünver, 2024). After 9/11, states, predominantly the USA, have waged a war, not against terror, but primarily against dissent (Giroux, 2014). Several social movements in the US, such as the Occupy or Black Lives Matter movement have been heavily monitored. The defamation and accusations of activists and human rights defenders, preventive arrests and economic exhaustion through trials fall under the category of what Giroux (2014) calls “domestic terror”.

Identifying and imprisoning political dissidents and censoring political speech annihilates collective action and intimidates moderates. In addition, literature suggests that authoritarian regimes prefer to deploy surveillance and targeted (digital) repression to radical opponents in order to prevent mobilization, as the latter are more likely to organize protests and disrupt social order, while mass repression could create a backlash (Xu, 2020). Except for protesters, governments have systematically monitored, suppressed and harassed journalists. The British government, following the Snowden leaks, coerced journalists of *The Guardian* to destroy relevant files (Glasius & Michaelsen, 2018). Surveillance generally restricts reporters from investigating and presenting their findings to the public, which overall undermines democratic processes especially when it regards critical issues (Franks, 2017). Online censorship and chilling effects, in combination with stifling journalism limits the free flow of information and consequently democratic dialogue.

Voters are another target for the surveillance state. Social sorting, profiling and micro-targeting are all practices aimed to manipulate citizens and determine election outcomes. Examples include the Cambridge Analytica scandal, where it was revealed that the company, after acquiring vast amounts of data from Facebook, sold psychological profiles of voters to political parties (Chester & Montgomery, 2018). The incident is linked with the Trump election in 2016 and the Brexit vote. Even though big internet and telecommunication companies’ main target is consumers, their unrestricted access to personal data expands their power to the political sphere. Voter surveillance is another aspect of mass surveillance. Voter management software, apps and other tools have been adopted by political parties in the USA, Canada and Australia (Bennett, 2015). Voters have turned into consumers and elections into a commercial industry, where decision making is determined by algorithms and data rather than active and conscious citizens.

Nonetheless, as Franks (2017) stresses out, this analysis of citizens as objects of mass surveillance would be incomplete, if factors such as gender, race and class were not taken into consideration. While every individual is subject to surveillance, some people are more vulnerable. Marginalized and minority groups are affected disproportionately by the state-industrial surveillance complex[1]. In particular, online censorship and digital repression can lead to the reinforcement of mainstream narratives or opinions and the further exclusion of such groups, be it women, the lgbtq+ community, racial and religious minorities. For these reasons, scholars support the idea that by only focusing on the privileged citizens, –the underlying and longstanding repercussions of mass surveillance cannot be fully comprehended.

According to *Privacy International* (n.d), it is essential to understand the close ties between surveillance and patriarchy, since they both seek to suppress and control women, trans and gender queer people. In a digitalized society where surveillance is becoming widespread and more intrusive, the online and offline oppression of women and gender queer people will likely grow. Revenge porn, hidden cameras and online stalking are only some of the concerns that digital surveillance brings (Franks, 2017). Racial, ethnic and religious minorities, along with migrants also face greater consequences. In China, Uyghurs are constantly monitored by the police. Huawei has even created a facial recognition system, the "Uighur alarm", that is said to identify Muslims and inform local authorities (Sahin, 2020). Reports state that chilling effects and self-censorship are higher in Muslim and black activists (Kuehn & Salter, 2020) and especially after the 9/11, Muslims are explicitly subject to "racialized" surveillance. Lastly, law enforcement, more often than not, coerces migrants to hand them over their devices, passwords and data (Privacy International, n.d)

Overall, digital mass surveillance interconnects governments and corporations on the one hand and the citizens on the other hand. While surveillance practices are conducted by states and the private sector, individuals consciously or unconsciously

[1] It is important to take into account how "If being forced to alter one's online search habits is considered a chilling effect that undermines democracy, being forced to alter one's clothing, job, school, choice of friends, communication with family, romantic relationships, or freedom of movement should surely be viewed even more seriously. For the less privileged members of society, surveillance does not simply mean inhibited Internet searches or decreased willingness to make online purchases; it can mean an entire existence under scrutiny, with every personal choice carrying a risk of bodily harm" (see Franks, 2017, p. 453).

participate in their own monitoring, as they allow access, mining and storage of their personal information. This “participatory surveillance” is the outcome of the normalization of mass surveillance, coupled with a lack of understanding of the complex digital landscape, the surveillance capabilities and the consequences it entails for human agency and self-determination.

At the same time, individuals are also the targets of various surveillance practices. As voters and consumers, citizens face digital surveillance, repression and manipulation in order to satisfy the agendas of economic and political elites. Protesters, human rights activists and journalists are watched closely by law enforcement to make sure that their actions and behaviors will be in alignment with the status quo and that they will not challenge the existing power structures. Marginalized groups, lastly, such as women, gender queer people, racial, ethnic and religious minorities are more vulnerable towards surveillance, which further exacerbates exclusion and inequality.

Chapter 5
Human rights, civil liberties and ethical consequences

5.1 Human rights and civil liberties

Mass surveillance in the digital age incorporates various technologies from CCTV to Artificial Intelligence. It involves multiple stakeholders, mainly the state, the private sector and citizens with their double role as participants and targets. It penetrates every aspect of social and political life on an individual and collective level. Eventually, ethical repercussions and moral dilemmas are raised in the domain of human rights and civil liberties. Particularly, the normalization of routine intrusive and extensive surveillance practices entails the invasion of privacy, freedom of expression and the right to assembly among others, while it increases social inequality, exclusion, and power imbalances between different social groups as well as, between the watchers and those who are being watched.

First of all, starting with the right to privacy, when one is referring to it, is referring to the "right to be let alone", to handle one's own data (Fernback, 2013) and who and for how long can have access to them. In the digital era, the preservation of privacy has become extremely complicated, since indiscriminate data collection and widespread online and offline monitoring are routinely conducted. Kovacs and Hawtin (2012), among others, pay closer attention to the violations of the right to privacy and the freedom of expression, while Giroux (2014) juxtaposes that focusing only on individual privacy to address the erosion of democratic values is a "kind of naiveté we can no longer excuse or afford" (p. 126). Indeed, the majority of the dialogue regarding digital mass surveillance revolves around privacy as the main issue, while in reality what is at stake is the enhancement of arbitrary power in the detriment of civil empowerment. The violation of privacy entails not only the government-corporate mining and analysis of personal information without consent, but more importantly the consequent restriction of individuality and self-determination (Glasius & Michaelsen, 2018). Therefore, breaches of privacy mean invasion of the human personality as a whole (Franks, 2017).

Freedom of expression, furthermore, that is the right to express opinions, thoughts and beliefs without fear, is being interfered with by censorship, content filtering and the chilling effects of surveillance. Violation of the freedom of expression also undermines open dialogue and the exchange of ideas, which are necessary in decision-making processes and the overall construction of the political future. In other words, as Glasius and Michaelsen (2018) state, infringing with the freedom of expression violates human dignity on an individual level, while on a collective level it stifles political speech and disables dissenting voices. Especially, the consequences are even greater when it regards minorities and journalists. In the first case, restricting self-expression can lead to further exclusion and social inequality, while in the second one, it facilitates state-sponsored propaganda and stifles plurality. What is interesting to mention here is that, even when citizens are encouraged to express their opinions via apps, polls and petitions, they are most likely monitored in order to gauge their political sentiments or identify grassroots conflicts.

Additionally, mass surveillance facilitates the violation of the freedom of assembly and association and the right to political participation. It must be evident by now, that governments around the world deploy a variety of surveillance techniques in order to suppress collective action and mass mobilization, such as social movements, that could potentially challenge the status quo. Internet shutdowns, social media monitoring and digital repression are common practices in both democracies and autocracies. In 2018, India had more than 100 internet shutdowns in order to restrain political mobilization (Earl, 2022). In the United States, police have been monitoring the social media of Black Lives Matter defenders almost since the creation of the movement (Nurik, 2022). Except for the above, preventive arrests, undermining the credibility of activists and labelling every protest as “terrorist” (Giroux, 2014), limits political participation while it normalizes surveillance.

In addition to the restrainment of political action and speech, monitoring and profiling voters in terms of marketing and surveillance capitalism poses questions about the outcome of the elections and the extent to which citizens are actually free to decide and determine this outcome. Voter surveillance and the implementation of marketing techniques in the political realm has turned voters into consumers, by limiting critical thinking. For example, certain governments, including the United

States and Canada, use voter management software in order to promote targeted messages to specific segments of the electorate (Bennett, 2015). It is hence argued that the role of citizens is limited to "consuming" the political decision, candidate or political party that is better marketed (Robles & Córdoba-Hernández, 2018).

Last but not least, the right to the presumption of innocence, which is also at stake, rests upon the fact that every individual is considered innocent until proven guilty. However, as it has been argued previously, states deploy mass surveillance in order to pre-empt actions and behaviors and interfere even before incidents take place. Preventive arrests of radicals to limit the impact of protests in both democratic and authoritarian states, is indicative of such practices. Another example is the use of AI to "preempt opposition and neutralize dissidents" (Frantz, 2020). There is also a growing reliance on big data and algorithms to predict who is more likely to commit crime (Lyon, 2014). In general, treating citizens as potential "threats" or collecting personal data for future use without sufficient evidence of wrongdoing clearly violates the right to the presumption of innocence.

5.2 Ethical questions as a result of digital authoritarianism

After discussing the objectives, methods, targets and finally the repercussions of digital mass surveillance in human and civil rights, it can be argued that digital authoritarianism has become the global trend for nation-states, regardless of their political system and the social values they claim to represent. It was mentioned in the first chapter that, in digital authoritarianism, the use of digital technologies aims to suppress, limit and control unwanted behaviors, actions and opinions that do not serve the interests of political and economic elites. These are the same elites which, in collaboration with each other whether on a domestic or transnational level, control the internet infrastructure and its services. By becoming a global normality, digital authoritarianism poses ethical questions in democratic and authoritarian regimes.

Ethical questions on human agency and autonomy circles back to Zuboff's (2018) "coup from above", where the watchers, i.e. the surveillant capitalists, not only monitor, track and identify individuals and actions but also dictate behaviors and what is accepted and expected. That is why focusing the debate only on privacy and the

balance between security and human rights is problematic (Giroux, 2014), since the cause of such violations is the abusive power; the capacity and possibility to control. Skinner articulates:

> To be free we not only need to have no fear of interference but no fear that there could be interference. But that latter assurance is precisely what cannot be given if our actions are under surveillance. So long as surveillance is going on, we always could have our freedom of action limited if someone chose to limit it. The fact that they may not make that choice does not make us any less free, because we are not free from surveillance and the possible uses that can be made of it. Only when we are free from such possible invasions of our rights are we free; and this freedom can be guaranteed only where there is no surveillance (Marshall, 2013, para. 16).

If digital authoritarianism is currently the prevalent governing system of the internet, then digital repression is its method of governance. Repression in regard to thoughts, opinions and beliefs on the one hand and repression of certain behaviors and actions on the other, incapacitates people as consumers, citizens and voters altogether. Especially in authoritarian states, digital repression increases the resilience of the regime and it often acts as complementary to other forms of repression (Frantz et al, 2020). While lack of transparency and accountability of the state towards its citizens exacerbates ethical consequences.

What is also troubling is the general environment of deliberate secrecy and lack of knowledge and understanding in which surveillance, the extraction and analysis of data take place. As a result, citizens are in general, unaware and unable to act in order to demand safeguards for their autonomy and freedom in online and offline spaces. On the other hand, neither governments nor corporations are willing to implement laws (Jiang, 2020) that restrict their sources of power, in this case, information and knowledge. Indeed, in this network society where information is the new currency (Barrenechea, 2015), the control of the information flows and its potential manipulation exceeds misinformation campaigns and propaganda for certain isolated incidents. It controls the minds of people and shapes the mainstream narratives which permit or restrict and dictate what is right, acceptable, and moral:

“[...] surveillance distorts a society. It transforms your perspective, your manners, your relationships with friends, colleagues, students, with every waiter and cabdriver you meet. It changes your relationship with yourself” (Nafisi, 2015, para. 1).

Nafisi (2015) describes her experience with the “surveillance state” in both Iran and America and concludes that, while surveillance and repression in Iran was extremely suffocating yet evident, in the United States, it is “insidious”. Taking into account the aforementioned, what is at stake, is not simply the right to privacy and all the other human rights that derive from it, be it freedom of expression, the right to assembly and so forth. What is at stake, is the very core of human agency that includes liberty, autonomy and self-determination. It is thus essential to deter this “seventh extinction” (Zuboff, 2018) of free will. Whether or not, citizens, albeit ignorant, indifferent or in some cases hopeless to act, can and should rectify their power. Counter-surveillance or sousveillance describe the bottom up watching of authorities, states and corporations in order to hold them accountable and address their wrongdoings and abuses of power (Reilly, 2023). Digital tools and technologies facilitate this exact objective with the dissemination of information through encrypted messages and tools, like TOR, using code-language to avoid censorship, VPNs (NIC, 2022), and even apps and websites that are directly created by hacktivists themselves to empower citizens (Hintz & Milan, 2018) and to serve the purpose of free internet.

Chapter 6
Conclusions

The evolution of digital technologies has expanded the capacities and repercussions of mass surveillance, which has come to defy and transcend national borders, political systems and governments. In other words, digitalized mass surveillance in modern societies cannot be attributed to certain states or authoritarian regimes. Both democracies and autocracies engage in such practices either with high or low tech methods. It is also common for states to cooperate with each other and exchange know-how and models of surveillance. Governments of otherwise different political ideologies that claim to represent different values, “are united in spying their citizens” (Schleusener, 2019, p. 175).

However, states could not extract, store and analyze all this vast amount and variety of personal data without the willing or unwilling collaboration with the private sector. Corporations usually operate or own the internet infrastructure and its services, while also producing and selling surveillance technologies. “Surveillance capitalism” describes the practices of the private sector which aim to exploit and commodify users' personal data for commercial interests (Zuboff, 2018). As it has been argued by scholars, this collaboration between the state and the private sector to monitor users-citizens creates the “surveillance industrial complex”.

It is an interconnected relationship which includes not only states and corporations but citizens as well. It has been examined how citizens play a double role in the surveillance landscape. On the one hand, they generate and hand over their personal information in exchange for convenience and entertainment, without being fully aware of the consequences. It is the “surveillance culture” where constant monitoring is normalized and a part of everyday life (Lyon, 2017). On the other hand, individuals whether as consumers, voters or citizens are the targets of indiscriminate, mass, top-down surveillance methods. Marginalized groups and minorities are disproportionately affected. Women, the lgbtq+ community, migrants, racial and religious minorities and the poor are positioned in greater danger.

Censorship, propaganda, filtering or blocking content are some of the surveillance techniques. Artificial intelligence, facial recognition or simply social media

and search histories facilitate the routine monitoring of individuals' personal information. Data about the educational, professional, economic and social background of each user is mined and stored. Even if some decades ago, this would have been unacceptable, nowadays the normalization and institutionalization of such practices in the public's consciousness have left little room for resistance.

Surveillance is usually justified as a necessary means to combat crime and terrorism and to safeguard national security and public safety. These are the exact same reasons that are used as a pretext in order to suppress political opponents, journalists, human rights activists and protesters. Whether in democratic or authoritarian states, political and economic elites seek to maintain the status quo and anyone who challenges it is regarded as a threat and must be controlled. The accumulation of power and wealth is the ultimate motive of controlling "from above" beliefs, behaviors and actions and eventually dictating what is acceptable and how we should think and act.

In general, both democracies and autocracies engage in widespread indiscriminate mass surveillance of their citizens. They take advantage of the opportunities and capacities that the digital landscape offers so as to control, shape or deter actions and opinions which threaten their power and stability. Nonetheless, focusing on states as the only actor that conducts mass surveillance is misleading. The private sector, whether Google or the Chinese Baidu, are collaborating with states and often provide them with users' data and surveillance equipment. Corporations themselves conduct surveillance for their own commercial interests and benefit from the legal framework. Every state has been using different systems and techniques. China proposes a high-tech surveillance model, while Russia a low-tech model that is supported by the current legal framework and its disinformation campaigns. The United States and other democracies use more insidious ways or pretexts to justify surveillance. The normalization and institutionalization of such practices enable extensive and more intrusive digital mass surveillance. In both cases, the surveillance alliance of states and corporations aims to eliminate existing and potential threats to the power balance.

The consequences of (digital) authoritarianism as a result of mass surveillance in human agency are gradually growing. Violation of fundamental human rights and

civil liberties are inevitable in a world where every action and thought is closely monitored. The right to privacy, the freedom of expression and the right to assembly are among others under the constant threat of indiscriminate mass surveillance. Surveillance creates a knowledge and power gap between the watchers and those who are being watched, which further exacerbates social inequalities and exclusion. In addition, scholars warn that what is at stake is far more complicated: the erosion of human agency, freedom and self-determination as a result of the abusive power of states –democratic or authoritarian– and corporations.

Future discussion on the topic, I believe, will facilitate the understanding of digital mass surveillance as a socio-political phenomenon, raise awareness and prepare citizens for resistance and rectification of their power to decide about and shape their own lives.

References

Amnesty International. (2015). *Easy guide to mass surveillance.* https://www.amnesty.org/en/latest/campaigns/2015/03/easy-guide-to-mass-surveillance/

Barrenechea, M. J. (2015). Why Information is the New Currency. *Open Text.* https://blogs.opentext.com/why-information-is-the-new-currency/

Bennett, C. J. (2015). Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications. *Surveillance & Society.* Vol. 13 No. 3/4: Surveillance Asymmetries and Ambiguities. https://doi.org/10.24908/ss.v13i3/4.5373

Bibri, Simon, E., & Zaheer, A. (2022). The Metaverse as a Virtual Form of Data-Driven Smart Urbanism: On Post-Pandemic Governance through the Prism of the Logic of Surveillance Capitalism. *Smart Cities 5*, no. 2: 715-727. https://doi.org/10.3390/smartcities5020037

Boghosian, H. (2013). *Spying on democracy: government surveillance, corporate power, and public resistance. Introduction.* San Francisco, California: City Lights Books.

Chester, J. Montgomery, K. C. (2017). The role of digital marketing in political campaigns. *Econstor*. https://www.econstor.eu/handle/10419/214047

Csernatoni, R. (2020). Coronavirus Tracking Apps: Normalizing Surveillance During States of Emergency. *Carnegie Endowment for International Peace.* https://carnegieendowment.org/posts/2020/10/coronavirus-tracking-apps-normalizing-surveillance-during-states-of-emergency?lang=en

Earl, J., Maher, T. V., & Pan, J. (2022). The digital repression of social movements, protest, and activism: A synthetic review. *Science Advances 8 (10)*. https://www.science.org/doi/10.1126/sciadv.abl8198

Egger, P. (2023). Digital surveillance and Authoritarian states. *Freie Universität Berlin*. https://www.fu-berlin.de/en/featured-stories/research/2023/digital-surveillance-authoritaritanism/index.html

Fernback, J. (2013). Sousveillance: Communities of resistance to the surveillance environment. *ScienceDirect.* https://doi.org/10.1016/j.tele.2012.03.003

Franks, M. A. (2017). Democratic Surveillance. *30 Harv. J. L. & Tech.* 425. https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech425.pdf

Frantz, E., Kendall-Taylor, A. & Wright, J. (2020). Digital Repression in Autocracies. *Varieties of Democracy.*

Gamal, N. (2020). The private sector's role in internet governance: east and west, two sides of the same coin. *CSSII*., p. 6, 9. https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2020_Sayed_Gamal.pdf

Giroux, H. A. (2014). Totalitarian Paranoia in the Post-Orwellian Surveillance State. *Cultural Studies*, *29*(2), 108–140. https://doi.org/10.1080/09502386.2014.917118

Glasius, M., & Michaelsen, M. (2018). Authoritarian Practices in the Digital Age| Illiberal and Authoritarian Practices in the Digital Sphere — Prologue. *International Journal Of Communication*, 12, 19. https://ijoc.org/index.php/ijoc/article/view/8899/2459

Hadjimatheou, K. (2013). Ethics and surveillance in authoritarian and liberal states. *European University Institute*. https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.4-Ethics-and-surveillance-in-authoritarian-and-liberal-states.pdf

Hintz, A., & Milan, S. (2018). Authoritarian Practices in the Digital Age| "Through a Glass, Darkly": Everyday Acts of Authoritarianism in the Liberal West. *International Journal of Communication*, 12, 21.

House of lords. (2009). *Overview of surveillance and data collection.* https://publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm

Jiang, J. (2020). The Eyes and Ears of the Authoritarian Regime: Mass Reporting in China. *Journal of Contemporary Asia*, *51(5)*, 828–847. https://doi.org/10.1080/00472336.2020.1813790

Kabanov, Y., & Karyagin, M. (2018). Data-Driven Authoritarianism: Non-democracies and Big Data. In: Alexandrov, D., Boukhanovsky, A., Chugunov, A., Kabanov, Y., Koltsova, O. (eds) Digital Transformation and Global Society. DTGS 2018. *Communications in Computer and Information Science, vol 858. Springer, Cham.* https://doi.org/10.1007/978-3-030-02843-5_12

Kendall-Taylor, A., Frantz, E., & Wright, J. (2020). The Digital Dictators: How Technology Strengthens Autocracy. *Foreign Affairs, 99(2)*, 103–115. https://www.jstor.org/stable/26892668

Khalili, L. (2020). Digital Authoritarianism, China and C0VID. *Lowy Institute for International Policy.* http://www.jstor.org/stable/resrep27665

Königs, P. (2022) Government Surveillance, Privacy, and Legitimacy. *Philos. Technol.* 35, 8. https://doi.org/10.1007/s13347-022-00503-9

Kovacs A., & Hawtin D. (2012). Cyber security, cyber surveillance and online human rights. *Global Partners Digital.* https://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf

Kuehn, K., & Salter, L. (2020). Assessing Digital Threats to Democracy, and Workable Solutions: A Review of the Recent Literature. *International Journal Of Communication, 14*, 22. https://ijoc.org/index.php/ijoc/article/view/12959/3082

Laidler, J. (2019, March 4). High Tech is watching you. *The Harvard Gazette.* https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/

Lamensch, M. (2019). Authoritarianism has been reinvented for the digital age. *Centre for International GovernanceInnovation*. https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/

Laperruque, J. (2019). The history and future of mass metadata surveillance. *Project on Government Oversight*. https://www.pogo.org/analysis/the-history-and-future-of-mass-metadata-surveillance

liu, Z. (2023). How Technology Changes Authoritarian State Surveillance: Evidence from China. *SocArXiv*. https://doi.org/10.31235/osf.io/3zpcj

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society, 1(2)*. https://doi.org/10.1177/2053951714541861

Lyon, D. (2017). Digital Citizenship and Surveillance| Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity. *International Journal Of Communication, 11, 19.* https://ijoc.org/index.php/ijoc/article/view/5527/1933

Mantellassi, F. (2023). Digital authoritarianism: how digital technologies can empower authoritarianism and weaken democracy. *GCSP.* https://www.gcsp.ch/publications/digital-authoritarianism-how-digital-technologies-can-empower-authoritarianism-and

Marshall, R. (2013). Liberty, liberalism and surveillance: A Q&A with Quentin Skinner. *OxPol.* https://blog.politics.ox.ac.uk/liberty-liberalism-and-surveillance-a-qa-with-quentin-skinner/

Michaelsen, M., & Glasius, M. (2018). Authoritarian Practices in the Digital Age—Introduction. *International Journal Of Communication, 12, 7*. https://ijoc.org/index.php/ijoc/article/view/8536/2458

Miyamoto, I. (2020). Surveillance technology challenges political culture of democratic states. In A. L. Vuving (Ed.), Hindsight, Insight, Foresight: Thinking About Security in the Indo-Pacific (pp. 49–66). Daniel K. Inouye Asia-Pacific. *Center for Security Studies.* http://www.jstor.org/stable/resrep26667.9

Nafisi, A. (2015). Surveillance States. *The New York Times.* https://www.nytimes.com/2015/06/14/books/review/surveillance-states.html

National Intelligence Council. (2022). *Digital Repression growing globally, Threatening Freedoms.* https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/3691-digital-repression-growing-globally-threatening-freedoms

Nurik, C. L. (2022). Facebook and the Surveillance Assemblage: Policing Black Lives Matter *Surveillance and society*. https://doi.org/10.24908/ss.v20i1.13398

Ortiz Galindo, R. (2016). Social cybermovements: a review of the concept and theoretical framework. *Communication & Society*, 29(4), 165-181. https://doi.org/10.15581/003.29.35813

Padden, M. (2023). The transformation of surveillance in the digitalisation discourse of the OECD: a brief genealogy. *Internet Policy Review, 12(3)*. https://doi.org/10.14763/2023.3.1720

Polyakova, A., & Meserole, C. (2019) . Exporting digital authoritarianism: The Russian and Chinese models. *Brookings Institution. United States of America*. https://coilink.org/20.500.12592/rwbp8q

Privacy International. *Mass surveillance.* https://privacyinternational.org/learn/mass-surveillance

Privacy International. Who they target. https://privacyinternational.org/learn/who-they-targ

Robles, J. M. Córdoba-Hernández, A. M. (2018). Commodification and Digital Political Participation: The "15-M Movement" and the Collectivization of the Internet. *Palabra Clave,* 21(4), 992-1022. http://www.scielo.org.co/scielo.php?pid=S0122-82852018000400992&script=sci_abstract

Sahin, K. (2020). The West, China and AI Surveillance. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/geotech-cues/the-west-china-and-ai-surveillance/

Schleusener, J. (2019) The surveillance nexus: Digital Culture and Surveillance control. *In book: REAL Yearbook of Research in English and American Literature*. Volume 34 (pp.175 - 201).

Shahbaz, A. (2018). The rise of digital authoritarianism. *Freedom House*. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Stoycheff, E., Burgess, G. S., & Martucci, M. C. (2018). Online censorship and digital surveillance: the relationship between suppression technologies and democratization across countries. *Information, Communication & Society, 23(4)*, 474–490. https://doi.org/10.1080/1369118X.2018.1518472

Surveillance Studies Network (2006). *The Surveillance Society, London: Information Commissioner's Office.* p.3. https://ico.org.uk/media/1042391/surveillance-society-summary-06.pdf

Wirth, J., Maier, C., & Laumer, S. (2019). Justification of Mass Surveillance: A Quantitative Study. *Wirtschaftsinformatik*.

Xu, X. (2020). To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance. *American Journal of Political Science*.

Zayani, M. (2019). Social movements in the digital age: change and stasis in the Middle East. *European Institute of the Mediterranean*. https://www.iemed.org/publication/social-movements-in-the-digital-age-change-and-stasis-in-the-middle-east/

Zuboff, S. (2020). Surveillance capitalism. *Project Syndicate*. https://www.project-syndicate.org/magazine/surveillance-capitalism-exploiting-behavioral-data-by-shoshana-zuboff-2020-01