

RETHINKING SURVEILLANCE AND COUNTER-SURVEILLANCE IN THE  
ERA OF BIG DATA: THE CASE OF CYPHERPUNKS

A THESIS SUBMITTED TO  
THE GRADUATE SCHOOL OF SOCIAL SCIENCES  
OF  
MIDDLE EAST TECHNICAL UNIVERSITY

BY

AHMED M. R. AL-MADHOUN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS  
FOR  
THE DEGREE OF MASTER OF SCIENCE  
IN  
THE DEPARTMENT OF INTERNATIONAL RELATIONS

SEPTEMBER 2025



Approval of the thesis:

**RETHINKING SURVEILLANCE AND COUNTER-SURVEILLANCE IN THE  
ERA OF BIG DATA: THE CASE OF CYPHERPUNKS**

submitted by **AHMED M. R. AL-MADHOUN** in partial fulfillment of the requirements for the degree of **Master of Science in International Relations, the Graduate School of Social Sciences of Middle East Technical University** by,

Prof. Dr. Sadettin KIRAZCI  
Dean  
Graduate School of Social Sciences

---

Prof. Dr. Özgehan ŞENYUVA  
Head of Department  
Department of International Relations

---

Prof. Dr. Pınar BEDİR HANOĞLU  
Supervisor  
Department of International Relations

---

**Examining Committee Members:**

Assoc. Prof. Dr. Şerif Onur BAHÇECİK (Head of the Examining Committee)  
Middle East Technical University  
Department of International Relations

---

Prof. Dr. Pınar BEDİR HANOĞLU (Supervisor)  
Middle East Technical University  
Department of International Relations

---

Assist. Prof. Dr. Özgür NARİN  
Ordu University  
Department of Economics, Ünye Faculty of Economics and Administrative Sciences

---



**I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.**

**Name, Last Name:** Ahmed M. R. AL-MADHOUN

**Signature:**

## ABSTRACT

### RETHINKING SURVEILLANCE AND COUNTER-SURVEILLANCE IN THE ERA OF BIG DATA: THE CASE OF CYPHERPUNKS

AL-MADHOUN, Ahmed M. R.

M.S., The Department of International Relations

Supervisor: Prof. Dr. Pınar BEDİRHANOĞLU

September 2025, 164 pages

This thesis rethinks the relationship between surveillance and technologist counter-surveillance in the era of Big Data and advanced Algorithms. It does so by studying the case of the Cypherpunks, as a movement that uses technology as the primary strategy to counter surveillance. The analysis is done through the lens of psychopolitics in the information regime as articulated by Byung-Chul Han. It demonstrates that counter-surveillance is a complex and multifaceted phenomenon. The thesis argues that technologist counter-surveillance is of a dual character, both disruptive of and reinforcing of power relations in the era of Big Data and advanced algorithms. Moreover, the efficacy of technologist counter-surveillance is limited to the extent it is intimate with the information regime.

**Keywords:** Surveillance, Counter-Surveillance, Big Data, Cypherpunks

## ÖZ

### BÜYÜK VERİ ÇAĞINDA GÖZETİM VE KARŞI GÖZETİMİN YENİDEN DÜŞÜNÜLMESİ: CYPHERPUNKS ÖRNEĞİ

SOYADI, Adı

Yüksek Lisans,Uluslararası İlişkiler Bölümü

Tez Yöneticisi: Prof. Dr. Pınar BEDİRHANOĞLU

Eylül 2025, 164 sayfa

Bu tez, Büyük Veri ve gelişmiş algoritmalar çağında gözetim ve teknoloji uzmanı karşı-gözetimi arasındaki ilişkiyi yeniden ele almaktadır. Bunu, gözetime karşı koymak için temel strateji olarak teknolojiyi kullanan bir hareket olan 'Cypherpunks' örneğini inceleyerek yapmaktadır. Analiz, Byung-Chul Han tarafından dile getirilen 'bilgi rejimi'ndeki psikopolitika merceğinden yapılmaktadır. Karşı-gözetimin karmaşık ve çok yönlü bir olgu olduğunu göstermektedir. Tez, teknoloji uzmanı karşı-gözetiminin, Büyük Veri ve gelişmiş algoritmalar çağında güç ilişkilerini hem bozan hem de güçlendiren ikili bir karaktere sahip olduğunu savunmaktadır. Dahası, teknoloji uzmanı karşı-gözetiminin etkinliği, bilgi rejimiyle iç içe olduğu ölçüde sınırlıdır.

**Anahtar Kelimeler:** Gözetim, Karşı Gözetim, Büyük Veri, Cypherpunks

*To my family and to the people of Gaza*

## ACKNOWLEDGMENTS

I am forever grateful to my supervisor Prof. Dr. Pınar BEDİRHANOĞLU. Without her support, guidance and patience this thesis would have not been possible. She is a true mentor and a great person. I am also grateful to Assoc. Prof. Dr. Şerif Onur BAHÇECİK and Asst. Prof. Dr. Özgür NARİN, for accepting to be on my jury and for their insights, comments and knowledge.

I would like to also extend my gratitude to Prof. Dr. Feride Pınar ACAR. Her support and kindness during a time of extreme difficulty only shows her exceptionally kind and brilliant personality. I am forever grateful to her.

I would never be able to properly thank my parents–Mahmoud and Rania. Without their love, support, encouragement, and trust I could have never done anything–let alone being here writing this acknowledgement for my master’s thesis. I love them so much and I am grateful to them beyond what words can express.

My beloved sister, Ejoo, has been with me all along, with her love, support and beautiful spirit. Since our reunion she has made my life full of joy and happiness. She will always be special in my heart. My brothers –Abboud and Hammoud- have always made my life much more beautiful, with their love and jokes–that never fail to make me laugh and that never cease to make my day every time I speak with them.

I want to especially thank my friends, who have been my comrades along the way during this journey–Ulyas, Yalei, Asya, Mohammd, Zein and Amr. Our shared memories, love and support shall forever have an unwavering place in my heart.

## TABLE OF CONTENTS

PLAGIARISM .....	iii
ABSTRACT .....	iv
ÖZ.....	v
DEDICATION .....	vi
ACKNOWLEDGMENTS.....	vii
TABLE OF CONTENTS .....	viii
CHAPTERS	
1. INTRODUCTION.....	1
1.1. Problem Statement .....	5
1.2. Research Objectives .....	6
1.3. The Case Study and Methodology .....	6
1.4. Theoretical Framework .....	10
1.5. Main Argument .....	15
1.6. Thesis Structure.....	16
2. SURVEILLANCE AND CONTROL IN THE BIG DATA ERA .....	17
2.1. Introduction .....	17
2.2. Surveillance in the Era of Big Data and Advanced Algorithms .....	17
2.3. Surveillance and Control.....	25
2.4. Counter-Surveillance.....	40
2.5. Conclusion.....	54
3. THE SURVEILLANCE REGIME AND PSYCHOPOLITICS.....	56
3.1. Psychopolitics.....	56
3.1.1. The crisis of Freedom.....	56
3.1.2. The Transition To Psychopolitics .....	57
3.1.3. Psychopolitics.....	61
3.1.4. Emotionalism and Gamification.....	65
3.1.5. The Information Regime: A Second Enlightenment.....	77
3.2. Games.....	81

3.3. Countering Surveillance and Collective Action.....	87
4. TECHNOLOGIST COUNTER-SURVEILLANCE AND THE CYPHERPUNKS.....	95
4.1. The Cypherpunks: A Technologist Movement of Counter-Surveillance .....	100
4.2. The Cypherpunks: A Force for the Information Regime .....	110
4.3. Conclusion .....	123
5. CONCLUSION: THE TECHNOLOGIST COUNTER-SURVEILLANCE IN THE INFORMATION REGIME.....	126
REFERENCES.....	131
APPENDICES	
A. TURKISH SUMMARY / TÜRKÇE ÖZET .....	150
B. THESIS PERMISSION FORM / TEZ İZİN FORMU.....	164

## CHAPTER 1

### INTRODUCTION

A little anecdote before we start. “But be careful what you say there; don’t share private or intimate content; nor should you share personal pictures; they spy on you and collect your data.” That was my first encounter with Facebook Messaging, which was the talk of the time, being the latest popular development of its kind. The discussion continued about the issue among various family members. There was a kind of ‘folk theory’ (Moran et al., 2022) established, based on lived experiences. Being a Palestinian, the sentence did not bring up any fears, nor was it of any surprise; after all, the warning was not something new, that is simply a voicing of how things are supposed to be on the internet—or on the phone.

Despite some inaccuracy, the sentence expresses the sentiment that was widespread in Palestine in relation to the surveillance system people have to face on a daily basis in the Occupied Territories. This sentiment can be seen through various accounts of Palestinians, and is deeply entrenched in the Palestinian collective imagination. Indeed, as Zureik (2013) points out, Palestinians have witnessed the highest degrees of hierarchisation through surveillance tools like population counting and spatial monitoring. But the real concern was state surveillance conducted by Israel, the Occupying power, which has been maintaining a surveillance apparatus all over the historical Palestine since before its establishment, and which brought up new concerns with every new technological advancement being applied (Zureik et al., 2013; Loewenstein, 2023). At that particular point in time, concerns in relation to “surveillance capitalism” (Zuboff, 2019) were not as strong.

Surveillance has intensified with the emergence of the digital era. Nowadays, advanced algorithms (including AI, Natural Language Models, Machine Learning,

and Deep Learning) and digital data infrastructures (including, Big Data and Small Data; regardless of form, structure, source or type) govern all aspects of life. These technologies are essentially technologies of surveillance. They seek to collect information and data, to process them for control purposes, either political domination, domestically or between states, and more importantly for profit by big technology companies, like Alpha, Meta and Amazon, among others. Indeed, Zuboff (2019) proposes the concept of “surveillance capitalism” to grasp the implications of this development in all walks of life as these technologies govern and shape the reality of the present and the future: from economics to public administration, and from human behaviour (individually and collectively) to the production of knowledge. Moreover, they are present everywhere in public discourse, even out of context. In addition, they have been associated with much excitement as well as anxiety; with passionate advocacy as well as feverish scepticism.

Despite the historical ubiquity of surveillance (Weller, 2022), in the ‘information regime’ surveillance has assumed new roles and has grown in breadth and depth, as explained below. Thanks to computer networks, Big Data infrastructure and advanced algorithms, surveillance is now pervasive externally, in terms of application and institutions, and unprecedentedly intrusive internally, in terms of the psyche of the subject. These technologies enable technology companies to build prototypes, ‘subject doubles,’ of individuals’ behaviours and what was considered the intimately private sphere of a community or a family. Furthermore, digital technologies and the development in data infrastructures has led to new forms of social surveillance including lateral (external) surveillance or *sousveillance* (that is, surveillance done by citizens, rather than government or corporation) with new behaviours associated with surveillance, like ‘underveillance,’ where the distinction between the subject and agent of surveillance is further blurred by the fact that traditional agents of surveillance are not the only ones enacting surveillance—and have also become the objects of surveillance.

This has been particularly the case after what is termed the ‘data revolution’, referring to the widespread application of various data infrastructures (Big Data or Small Data alike) with the spike in the development of advanced algorithms to

manage, store and process the collected data. Information regime, which is a form of domination via technology, exploits data and information to mold and shape the behaviour of individuals and collectivities (Han, 2022). In the information Regime, information/data and advanced algorithms for processing information have a decisive influence in politics, economics and society.

Issues concerning control and emancipation and the harmful impacts of computational technologies emerged shortly after the development of the first computers. They developed in parallel with camps emphasising the control potential of these technologies while others emphasising the emancipatory, democratic potential of such technologies. Discussions and attempts to understand and deal with this rapidly growing apparatus/paradigm proliferated in an unprecedented pace and fashion.

Antagonism is inherent in any sort of power relation, and so is the case with the emergence of the information regime. The ubiquity and the immense impact of digital technologies (and with it, the technologies of surveillance) led to more such antagonisms, as people feel the impact of these technologies more; although the reverse is also possible, as some cases show. With the data revolution, this affective aspect of the digital has brought with it novel forms, perceptions and sentiments of resistance.

These computational technologies enabled novel forms of resistance as well, which have been historically unprecedented. They have enabled various forms of antagonisms. Indeed, a quick look into instances of resistance in the digital era reveals multiplicity, complexity and interconnectedness between different actors as well as between various forms, tactics and strategies of resistance. These include the use of digital means as well as more conventional means of resistance, or a mix of both. Moreover, there is a multiplicity in terms of the targets these initiatives have in sight; they can target the digital infrastructure itself or other less-technical institutions like bureaucracy due to the unjust use of Big Data algorithms or other injustices. Mostly however, they seem to combine different elements and objectives, being multi-modal in their approach; both enacting and drawing from earlier modes and tactics of resistance.

For example, the well-known Anonymous has assumed different faces and roles in time such as those ranging from online trolling for political purposes to mobilising campaigns and conducting organising hacking operations; some of these activities have had elements found in intelligence organisations. They have targeted various state, religious, and corporate targets. On one hand, Anonymous has enacted tactics that are considered to be conventional modes of resistance such as journalism and street protests. On the other hand, they have enacted tactics that are distinctively digital in nature, like DDoS (denial-of-service) attacks. Furthermore, they are still proliferating.

Countering surveillance has hence become itself a buzzword found everywhere, attracting great academic attention as well. Various scholars problematise the impact of these instances of resistance in the context of the information regime and the ubiquity of these technologies both theoretically and empirically. Various categories of resistance emerge from this body of literature, ranging from a focus on every-day resistance to focus on social movements, and from those concerned with proactive to passive counter-surveillance.

One approach to counter-surveillance, is the adoption of these technologies of surveillance with the aim to make a democratic change, or to counter the information regime. Technologist counter-surveillance refers to the strategy that emphasises the importance and the primacy of digital technology itself as the principal means and strategy of resistance against the information regime. It shapes the tactics, modes and forms of resistance, centering them around developing novel technological tools or altering/obfuscating existing ones. Furthermore, it assumes different characters, with a diverse collection of actors covering technology experts, journalists, and capitalists.

Examples of technologist counter-surveillance are numerous and varying, and its applications are used by a cohort of individuals and collectives. Salient examples include the Cypherbunks, who advocated and developed technologies, primarily Strong Encryption as the central means for countering surveillance. +KAOS is another example which focuses on the development of alternative data infrastructures to counter the dominant data infrastructures in the information regime. Technologist

resistance includes many smaller initiatives and projects that seek to directly counter surveillance by developing various software, like the open-source InformaCam. InformaCam provides users with the ability to control meta-data attached to their visual contents before sharing them, thus obstructing surveillance and data mining attempts through shared footage. Moreover, it has faith in technology in terms of developing software technologies, but also in terms of developing hardware tools, like open-source 3D printed gadgets or open-source personal computers, from which devices that usually collect data are removed or adjusted.

In contrast to ‘technical counter-surveillance,’ there are also a number of other strategies, including ‘artistic counter-surveillance’ where works of art are adopted as the principal means of countering surveillance in order to disrupt the ‘police order’ of surveillance. In addition, ‘pedagogical counter-surveillance’ emphasises the educational element and increasing awareness. Moreover, ‘legal counter-surveillance’ counts on the power of law to limit the harmful impact of these technologies of surveillance and to instate justice and equality. Other strategies include violent resistance or refusal and disengagement, as will be discussed below.

Indeed, the history of information and digital technologies shows that ‘technologist resistance’ has a longer tradition in the history of counter-surveillance, which develops at each point when a new information technology is developed and applied. However, the emergence of infocracy, with unprecedented developments in data infrastructures and advanced algorithms have allowed this strategy of technologist resistance to grow both in breadth and depth, while its ideological assumptions, tactics and modes are adopted at a large scale globally. This is why the technologist counter-surveillance is the focus of this thesis.

## **1.1. Problem Statement**

There is however a dilemma at the heart of the technologist approach to countering surveillance. Technologist counter surveillance practices are an intimate part of the technologist information regime which they seek to oppose, yet at the same time they have been a disturbing force that significantly caused ameliorative outcomes and has

had a pivotal emancipatory role. Using the parlance of Jacques Ranciere, they have been a force of both ‘democracy’ and ‘police’, of both ‘consensus’ while bringing about ‘dissensus’. At times they have reinforced power relations of domination and at other times they have been forces of emancipation. This dilemma in relation to technologist counter-surveillance is the concern of this thesis.

## **1.2. Research Objectives**

This thesis attempts to understand this dilemma at the heart of resisting the ‘information regime’ in general by investigating the Cypherpunks as an exemplary case of technologist counter-surveillance. It identifies the following objectives:

- I. To explore what technologist counter-surveillance is, manifested in the case of the Cypherpunks, as a strategy of resistance in the information regime;
- II. To understand the relationship between surveillance and counter-surveillance as they take place within the contemporary information regime;
- III. To reflect upon the potential efficacy of technologist counter-surveillance vis-a-vis the control of the information regime.

## **1.3. The Case Study and Methodology**

This thesis chooses Cypherpunks as the case study, as they are an exemplary case of technologist counter-surveillance.

Andy Greenberg (2024) a senior writer for WIRED Magazine, a technology-focused magazine specialising in cybersecurity and surveillance, writes the following before reporting his interview with Meredith Whittaker (the president of the most secure communication, non-profit software application-- Signal) on the 10th anniversary of the application: “Since that July in 2014, Signal has transformed from a Cypherpunk curiosity—created by an anarchist coder, run by a scrappy team working in a single room in San Francisco, spread word-of-mouth by hackers competing for paranoia points—into a full-blown, mainstream, encrypted communications phenomenon.”

WIRED, in its second edition, established the first link between the Cypherpunks (crypto-anarchism) on the one hand, and Libertarianism, on the other. The cover of

this issue (Issue 1.02 of May/June 1993) featured the founders of the Cypherpunks, Timothy C. May, Eric Hughes, and John Gilmore masked and holding the flag of the US, with a text reading “Rebels with a Cause (Your Privacy)”. Twenty years later the cover of the 22.09 issue of Wired depicted Edward Snowden, the renowned whistleblower and contractor of the US National Security Agency (NSA). Whistleblowing is a significant contemporary issue that draws much attention. It represents a central aspect of the Cypherpunk vision.

The Cypherpunks were founded in Silicon Valley in 1992 by Timothy C. May with Eric Hughes and John Gilmore. A group of 16 people started gathering every Saturday in an area for tech start-ups. After a short while they created a mailing list, unmoderated, free, and anonymous. According to Jarvis (2021a) the Cypherpunks envisioned four strategic goals. The first goal concerns free access to cryptographic technologies for citizens. This is the basis for their other goals, the second of which concerns anonymous communication. The third objective emphasises the freedom to conduct anonymous economic interactions without interference by government. Finally, whistleblowing and leaking platforms should be developed as a means to reduce the state's power.

Despite precedents in history, whistleblowing in the digital world took a new turn and exerted unprecedented reach, volume and impact. The impact of Wikileaks, since its first publication in December 2006, was most likely unprecedented in history. As an original contributor to the Cypherpunk mailing list, Assange's ideas are in line with the general ideology, modus operandi and imaginary of the movement. Timothy C. May proposed the use of cryptologic technology for whistleblowing as early as 1988, and spoke of it as a principal application for crypto tools. He also encouraged the establishment of different whistleblowing platforms. Another issue of significance in contemporary times is Cryptocurrency. The issue dates back into the early days of the group, particularly the works of David Chaum on digital cash. Freedom of anonymous economic transactions (Jarvis, 2021a) is a primary objective of the Cypherpunks and a central aspect of their strategy. Moreover, the cyberwars are still going on (Jarvis, 2021a), with the ideas around

both whistleblowing and cryptocurrencies still drawing on the heritage and ideologies of the Cypherpunks.

The continued influence of the Cypherpunks, within the context of the crypto-wars, is one reason for the selection of the group as a case study. According to Beltramini (2021), the Cypherpunks are “perhaps the single most effective grassroots organization in history dedicated to protecting freedom in cyberspace” (101). This is the motivating spirit and the core of the ideology of the Cypherpunks, but also of the majority of the groups and organisations that sprouted in the United States and beyond in that era, particularly in allied countries in Western Europe and Asia. This ideology or vision, albeit in different variations, continues to exert significant influence on contemporary initiatives, discourses and imaginaries about Artificial Intelligence (AI), Big Data, and computer technology in general, by those carrying the flags of different contesting “Frontiers”, or “Revolutions”. Moreover, the Californian ideology exerted influence beyond the United States reaching other geographies in Western Europe and Asia, appealing to the digerati of the virtual class there, who were in fact closer to their Californian peers than to the working classes in their societies. This is so despite the fact that the ideology was a result of a particular group of people with particular socioeconomic environment and within a particular technological context.

Another important reason is the fact that the group is American in its approach. For one thing, this makes it important in the context of what Bigo (2006; in Stevens, 2025) calls the ‘state of unease’ propagated by conceptions of global insecurity, led by ideas emerging from the United States, in the aftermath of 9/11. Moreover, in terms of hegemony, the United States and American Big Technology companies dominate the world when it comes to surveillance through technology, in a systematic and structural manner (Kwet, 2019). This makes it important to investigate technologist counter surveillance from within this hegemonic context. According to Barbrook & Cameron (2001), the Californian ideology has flourished at a critical juncture of historical, economic and technological developments in the context of the emerging information society and information economies in the US and without any rivals capable of countering the narrative of its proponents. “At this

crucial juncture, a loose alliance of writers, hackers, capitalists, and artists from the West Coast of the United States have succeeded in defining a heterogeneous orthodoxy for the coming information age—the Californian Ideology.” (365).

Moreover, and more relevant to the topic of this thesis, is the technologist approach of the movement against the surveillance regime; or what is sometimes also called ‘technocracy’ or technocratic totalitarianism. Surveillance and privacy are essential elements in the Cypherpunk ideology/conceptual framework, and the Cypherpunks emphasise in their documents and speeches that the effective solution is the use and development of technology (especially strong cryptography), not law (unlike, for example legal approaches of counter-surveillance). Moreover, all individuals, according to the Cypherpunks, are supposed to learn at least the basics of cryptography, if they wish to be truly free. The Cypherpunks ‘write code’ and this code is what shapes their strategy, tactics and discourse for countering the information regime of technological authoritarianism. This reason, in light of other reasons, makes the Cypherpunks an exemplary case worth studying in light of the proposed framework and research objectives discussed above.

Another justification is the relationship between the Cypherpunks, as a technologist counter-surveillance on one hand, and the system they attempt at dismantling on the other. The language and the imagination of the Cypherpunks reveal an intimate relationship with that of their rivals in the digital paradigm, despite their opting to “turn [the technology] on the likes of its paymasters” (Assange 2006, 2). Moreover, the Cypherpunks are accused of complacency, that is deeply rooted in, and not just a by-product of, the line of thought and the temperament they possess (Barbrook & Cameroon, 2001). In fact, some would consider them as an international threat, as a haven for global criminals and terrorists, that demands an international approach, based on nothing but delusions (Denning, 1996, 2001). While this neglects the positive impacts of the movement, it is important to understand this relationship between counter-surveillance and surveillance, without simply relegating it to oppositionality, for a meaningful understanding of technologist counter-surveillance in the era of the surveillance regime.

What is more important in this regard, as a justification for the selection of this case study, is the tensions present within this movement. This case study demonstrates the tension between individual and collective action in resistance— between individual resistance and social movement’s resistance. It blurs the lines between various ideological positions, present as a mix of various ideas, often with conflating aspirations. At once it is both and neither. This position, which some observers might call self-contradicting, can only be the result of such an ideology, with a firm technological determinism.

In the light of the above-mentioned justifications, this thesis will investigate the Cypherpunks and their faith in cryptography (within the context of the Crypto-wars). The case is meant to exemplify and demonstrate the discussion about technologist counter-surveillance in the information regime, with its data infrastructure and advanced algorithms, to reach the research objective of this thesis.

The study falls under qualitative, interpretive social research. It will build on present literature on the history and ideology of the Cypherpunks. Moreover, it will utilise documents published by the Cypherpunks and prominent figures in the group or associated with them. It will take this approach to substantiate the argument that technologist counter-surveillance takes place necessarily as a force for the information regime which it tries to counter. It is of a dual character, as both progressive and reactionary; disruptive and reinforcing. Furthermore, as such, its efficacy in countering surveillance is limited to an ameliorative impact, to the extent that it is intimate with the regime it seeks to counter.

#### **1.4. Theoretical Framework**

This thesis builds on the analysis of the philosopher Byung-Chul Han. In particular, his work on psychopolitics and the information regime. Han’s analysis will be developed in detail in Chapter 3 of this thesis. The information regime refers to a new form of domination effected on the social, political and economic fields by information—that is, through the collection, storing, and processing of data and information (Han, 2022). The information regime works along the imperatives of

psychopolitics—which seeks to influence the behaviour of individuals and masses on a pre-reflexive level. At the same time, the information regime reinforces and propagates psychopolitics.

An example of psychopolitics in operation is micro-targeting. Micro-targeting works by personalising messages on the basis of data collected on the behaviour of an individual. The political message or commercial advertisement no longer targets a population with a variety of personalities, ideational positions and desires. They are now tailored to influence the particular individual receiving it. In fact, the kind of content he or she repeatedly encounters is altered to the end of behaviour control.

Before moving on, it is important to note the relationship between ‘information’ and ‘surveillance’ in the work of Han. Han implicitly differentiates between the information regime and the surveillance regime, in a manner akin to that proposed by Fuchs (2010), by arguing that an information regime is not necessarily a surveillance regime. Nevertheless, Han sees the current information regime as a surveillance regime, and formulates it in terms of the information regime. The information regime and the surveillance regime are coinciding in the neoliberal era. Thus, both concepts are used interchangeably (see, Han, 2022).

Han starts by observing what he calls the crisis of freedom. Under neoliberal psychopolitics, freedom, which is supposed to be the antithesis of domination, is being exploited and utilised as a form of control (Han, 2017a). Freedom produces coercion. This is part of a grand transformation in history—from industrial capitalism to information capitalism. Here we observe a new mode of production, a mutation in capitalism, rendering it fundamentally different from the capitalism of the 19th century. We are living in a novel, immaterial, networked, post-industrial mode of production, which overcomes the limitations for increasing productivity and efficiency, found in the earlier modes of production. Capitalism in the present time is one of high-order production—rather than production, which is often sent for the Third World to accomplish. It is a capitalism not of production but of products, that is, it seeks to buy the finished products and wants to sell services and buy stocks. What emerges is a society of control (Ibid.; Han, 2017b).

This society of control is a mutation from the disciplinary society proposed by Michel Foucault. It works along the lines of psychopower rather than biopower. Michel Foucault (1978) observed a transformation in the mechanisms of power from sovereign to disciplinary power starting from the seventeenth century. Disciplinary power was in essence more subtle and precise in contrast to the coarseness of sovereign power—it sought to administer life, rather than subtract it. This power over life evolved in two forms: the anatomo-politics of the human body (or disciplines of the body) and the biopolitics of population (or regulations of the population). With its dual nature, biopower sought to control bodies and energies for the purposes of production and efficiency. Its objective was the ‘docile body’—to shape the individual into becoming an obedient machine, to place on the assembly line. For that, it deployed disciplines. Disciplines restricted, prohibited and placed restrictions, and were deployed in a variety of milieus and environments including educational institutions, the prison, the factory, and the clinic.

Psychopolitics, in contrast, works along the lines of different imperatives. Rather than inhibiting it seduces and encourages, instead of restricting it sets the individual free. Therefore, “[w]e are living in a singular phase of history when freedom itself entails pressure and coercion. In actual fact, freedom represents the antitype of compulsion—period. And yet this same antitype is now bringing forth compulsion and constraint. More freedom amounts to more pressure. As such, it marks the end of freedom.” (Han, 2017b, 48-9). The individual exploits herself. This is a result of seizing the psyche by psychopolitical technologies of power. The biopolitical concerns itself with bodies. The ‘body’ of the individual as well as the ‘race’ as a body, the population are the targets of disciplines. The psychopolitical, in contrast, concerns itself with the psychological; it penetrates the psyche in order to control the subject, now the entrepreneur, on the pre-reflexive, unconscious level. The individual is living under the illusion of freedom, conceiving herself as an entrepreneur—seeking constant optimisation, when in fact what is being optimised is the system, and not the individual. In other words, the liberation of the body does not negate exploitation, rather “our life projects include all kinds of affective, somatic, and visceral dimensions that are prone to exploitation.” (Wyllie, 2024, 16).

An example of platform workers, in the case of Uber, illuminates this situation. In this case, as Salter and Dutta (2023) show, there exists a paradox concerning knowledge and practice. Despite existing and felt exploitation, the platform business model and algorithms enables an ideological fantasy of the rule-breaking entrepreneur. This way the workers are caught in the web of this business model. Despite being conscious of exploitation, precarity and injustices, workers continue to work for the platform, rather than seeking a different alternative, driven by this ideological fantasy of the rule-breaking entrepreneur. This psychopolitical gamification of work is the reason for this situation in which workers adopt contradictory, irrational positions against their interest.

Furthermore, psychopolitics is intertwined with digital technologies. Psychopolitics enables and is dependent on the digital paradigm. It draws on and entrenches the surveillance regime. Without the computer device and computer networks the ability to penetrate into the psyche of the individual is impossible. Moreover, the utopianism of the early days of the digital age is simply illusionary (Han, 2017b). Instead of a force for emancipation, we have a new form of domination—the ‘information regime’ (Han, 2022).

Through Big Data and advanced algorithms, the information regime is able to provide ‘psychographical’ charts of the individual and the population alike. It is in this way that psychopolitics is able to penetrate the psyche on a pre-reflexive level and to influence the behaviour of people—either their commercial purchasing choices or political decision making and voting. This is a form of smart power, unprecedented in history. The social, political and economic impacts of this manipulative smart power is far reaching. For example, in the contemporary scene of social media platforms, algorithms and analytics, politics and the public sphere have changed dramatically. The post-factual politics of fake news, adopted by Trump (the first Twitter president) is only possible under the information regime, with its Big Data and advanced algorithms. Conspiracy theories also thrive under these conditions with the crisis of truth and representation as well as with the fundamental and widespread distrust (Han, 2022).

This relates to a situation in which the surveillance Big Brother becomes a ‘friendly’ one. Now surveillance takes place voluntarily. People engage in self-exposure and self-illumination. Lyon (2017) observes the emergence of an unprecedented culture in relation to surveillance. He proposes the concept of ‘surveillance culture’ to capture it. There are two main aspects of it. The first concerns the compliance with surveillance that is widely present in contemporary society. The second main aspect of the surveillance culture is the fact that generally the population is no longer the mere target or object of state or corporate surveillance. People have become active participants as they not only engage with surveillance but also initiate it.

For Han, this is explainable through emotionalism and gamification that are essential technologies of power in the neoliberal psychopolitical form of domination. Emotions are elicited and hailed as the expression of liberated subjectivity—for the exploitation of this very ‘expressed,’ ‘communicated’ subjectivity. This sudden boom, according to Han, erupts above everything else from an economic process—the emergence of ‘a new, immaterial mode of production’. It is in our times that “[e]motions have become a means of production” (Han, 2017a, 45). The obedient ‘docile body’ of biopolitics was denied emotions—it should not have. Emotions were seen as a disruptive force in biopolitical disciplinary society. In control society, emotions are elicited for exploitation. As a power, compared to biopolitics, “emotion affords a highly efficient medium for psychopolitically steering the integral person, the person as a whole.” (Han, 2017a, 48)”

Moreover, the totality of life and communication is ‘gamified’ in the information regime. Thinking takes two forms. The first is thinking at work, with the other being thinking at play. Games are supposed to be part of the unproductive—the opposite of labour. This novel mutation of capitalism invests and assumes playing into the realm of labour for exploitation for productivity. Gaming and labour coincide—the totality of life falls under the exploitable (Han, 2017a).

Emotionalisation and gamification have particular temporalities that are not suitable for political reflection and collective action. Moreover, the control of population at a pre-reflexive unconscious level results in psychological maladies that further render

a reflective and collective action unlikely. One important such pandemic is the Information Fatigue Syndrome (IFS), the symptoms of which include attention deficits and gradual deterioration of humans' analytical capabilities. In addition, they gradually lacked the ability to accept responsibility (Han, 2017b). The necessary temporal and mental conditions are unlikely, for an effective collective action—that is capable of questioning and disturbing power relations. Instead of a mass with a political identity, what the information regime brings about are 'swarms'—volatile, fleeting and short-term gatherings. Swarms lack the unifying spirit and duration necessary for effective political action (ibid). The significance of Han's work derives primarily from his analysis of the dynamics of psychopolitical control and the elements present therein. His analysis is relevant to understanding the regime of surveillance in the era of Big Data and advanced algorithms—its characteristics and dynamics. Moreover, it is important to understand the context in which technologist counter-surveillance takes place, and the objects of its resistance—in order to examine its efficacy and to understand the dilemma presented in the problem statement of this thesis. Han's account delves deeper into its dynamics, providing a synthetic repertoire of analytical tools, relevant to the issue of this thesis.

The analysis of Han, and the context of technologist counter-surveillance, will be discussed in detail in Chapter 3 of this thesis. Furthermore, this thesis will make use of recent theoretical developments and empirical results from Surveillance Studies and Resistance Studies, in order to enrich the theoretical framework that draws on the philosophy of Han. Discussions on the history and nature of surveillance will inform the discussion on the relationship between surveillance and control. In addition, Resistance Studies will be informative in setting the context of technologist counter-surveillance as a phenomenon of complexity, multiplicity and dynamic directionality.

### **1.5. Main Argument**

By studying the Cypherpunks as an exemplary case of technologist counter-surveillance in the information regime, the thesis attempts to make the following argument:

Technologist counter-surveillance takes place necessarily *within* the information regime, as proposed by Han, which is the same regime it tries to counter. It is of a dual character, as both progressive and reactionary; disruptive of and reinforcing. Furthermore, as such, its efficacy in countering surveillance is limited to an ameliorative impact to the extent that it is intimate with the regime it seeks to counter.

## **1.6. Thesis Structure**

The thesis is composed of five chapters. After this introductory chapter, Chapter 2 looks firstly into the relationship between surveillance and control. In addition to this, the chapter looks into counter-surveillance in the information regime of Big Data and advanced algorithms.

Chapter 3 delves in detail into the context of counter-surveillance, and the mechanisms and dynamics of the information regime. It gives a detailed discussion of the analysis provided by Han, against which the following chapter examines the case study. Chapter 4 investigates the Cypherpunks as a case of technologist counter-surveillance against the background of the earlier discussions. The final chapter concludes the thesis and presents the argument of this study.

## CHAPTER 2

### SURVEILLANCE AND CONTROL IN THE BIG DATA ERA

#### 2.1. Introduction

In contemporary times words and terms like AI, algorithms and data are encountered all over the public sphere, in policy statements, in public discourse through different media channels and in vernacular everyday talks, even out of context. It is undisputed that these technologies govern and shape the reality of the present as well as the future. They affect all aspects of life, from economics to public administration, and from human behaviour (individually and collectively) to the production of knowledge (See e.g., Kitchin, 2014a; 2014b).

These technologies have been the source of both great jubilation and immense trepidation. Nevertheless, such jubilation and trepidation have been an essential characteristic of the digital paradigm, or the information regime (Han, 2022; Weller, 2022). These traits have been a persistent feature of the information surveillance society. The history of technology has shown celebration and scepticism accompanying every technological development (Weller, 2022). Anxieties and social panics in such conditions have precedents in history. Moreover, they have also produced justifications and calls for increased surveillance (ibid) while at the same time they have led to calls and initiatives antagonistic to that particular emerging technological regime.

#### 2.2. Surveillance in the Era of Big Data and Advanced Algorithms

Advanced algorithms (including AI, Natural Language Models, Machine Learning, and Deep Learning) and digital data infrastructures (including, Big Data and Small

Data, regardless of their form, structure, source or type) permeate every aspect of society and politics as well as economy. These technologies shape the conditions and possibilities of life. They have changed the way governance works, so much so that some scholars argue for a new emerging governance rationality. The ‘digital governmentality,’ where statistical individuation and predictive algorithms on the basis of collected data has become the primary process of governance, producing digital subjects and discarding human rationality—a shift in the rational neoliberal governmentality. Governance here takes place through desire rather than pleasure, and language is treated as behaviour (Barry, 2019). This results in uncertainty as the character of knowledge, similar to what Bigo (2006; in Stevens, 2025) calls the ‘state of unease’ propagated by conceptions of global insecurity, led by the United States in the aftermath of 9/11. Morison (2016) follows this line by discussing ‘algorithmic governmentality’, which renders people both present and absent at once through datafication and continual update.<sup>1</sup> This is even the case in the management of diseases in the realm of health. As Roberts and Elbe’s study of three online syndromic surveillance systems (2016) suggests, the emergence of algorithms has been the central logic with credibility within global health surveillance and control. All this is the result of a sweeping epistemic shift (Barry, 2019; Morison, 2016, Roberts and Elbe, 2016; Flyverbom et al., 2017; Han, 2015, 2017, 2022). Roberts (2019) attracts attention to “an epistemic *break* from previous strategies of risk management” with emerging “new rationalities to regulate yet unforeseen public health emergencies” (p. 95, emphasis added).

Under Big Data and advanced algorithms, all the dimensions of the analytics of government (Flyverbom et al., 2017; Dean, 2009) –namely, the fields of visibility, technes and epistemes of government–, revealing the conditions of existence of regime practices are fundamentally altered. Even scholars who reject the rise of a new governance rationality demonstrate the centrality of Big Data and advanced algorithms in governance.<sup>2</sup>

---

<sup>1</sup> See also, Rouvroy & Stiegler, 2016; Rouvroy, 2020; Rouvroy & Berns, 2010, 2013; Bellanova, 2017.

<sup>2</sup> See Introna, 2016; Aradau and Blanke, 2017; Cheney-Lippold, 2011; Musiani, 2013; Latzer & Festic, 2019; Katzenbach & Ulbricht, 2019.

The contemporary (wo)man produces amounts of data that are unprecedented in human history. Data are gathered from a range of actions that are as important as trivial from data out of medical profiles to data gathered from clicks of one's mouse; and perhaps more importantly, data what is known as meta-data or “data about data” such as IP address, the identity of the contact, the location of calls or messages and the duration of the contact” (Lyon, 2016, p.257). It is the age of Big Data with abundant amounts of data. According to Kitchen (2014a), “A data revolution is underway, one that is already reshaping how knowledge is produced, business conducted, and governance enacted” (xv). Big Data, in short, refers to “massive data sets having large, more varied and complex structures with the difficulties of storing, analysing, and visualising for further processes or results” (Sağiroğlu & Sinanç, 2013). The massive volume, the wide variety and high velocity necessitate novel algorithms and methods, statistical and otherwise, to gather, analyse, present, and make meaning out of the collected data. In addition, new fields of inquiry, notably “data analyses” and “data science,” emerged.

Data infrastructures and databases should not be seen only from a technical vantage point. These technologies are not mere technical means for collecting, storing, and communicating data and information as a neutralist approach to technology and data would assume. They are complex sociotechnical systems with diverse and immense impact as they are located within an institutional milieu consisting of a multiplicity of actors including corporations and governmental agencies as well as intellectuals, experts and dark data markets. As such, data infrastructures are essentially impactful on the fields of governance, economy, and knowledge production (Kitchen, 2014a).

Similarly, advanced algorithms, including AI and its derivative systems, are also socio-technical assemblages, which should be situated within the broader milieu within which they exist. As defined by McQuillan (2022), AI is a “layered and interdependent arrangement of technology, institutions and ideology” (p.1), operating as a structuring structure and existing as a form of meta-politics. It is the result of a historical social process. Advanced algorithms are entangled with a social matrix, consisting in data. It inherits the ideological and philosophical assumptions and worldviews of the actors and institutions developing them, and as such

reinforcing these ‘logics of the master,’ (Salter & Dutta, 2013) and perpetuating present inequalities. They reproduce a form of ‘race science’ (McQuillan, 2022), a technology of power that produces a form of racial science that, in the contemporary world, is the ideology of ‘whiteness’ (Katz, 2020).

This reality is obscured, nonetheless. At one level, the ‘black box’ of algorithms renders attempts to understand the harms resulting from AI and the biases in data fed to them difficult, if not altogether impossible to detect and solve—beyond mere claims of ‘technical solutionism’. AI itself is nebulous, malleable, contested, and continually made and dynamic (Katz, 2020). At another, deeper level, AI is a continuation of a longer historical tradition in science. It wears a cloak of absolute, objective science, building on the legacy of statistics and the scientific methods while also pretending to be the solution through solutionism and dataism (McQuillan, 2022). In fact, the advocates of AI and dataism argue for the obsolescence of theory and science based on the scientific process (Anderson, 2008). Instead, knowledge emerges out of data, the more of which we collect the better. Data should be comprehensive. By this neutral appearance and false conscience, AI naturalises and essentialises dividing lines and social boundaries, reinforcing the *status quo* and generating knowledge that privilege particular groups (the already powerful) over others (the already vulnerable). The consequences can be disastrous: intensified inequality and injustices, and condensed forms of structural and cultural violence (McQuillan, 2022).

McQuillan (2022) moves further in identifying the harms of this information regime. As he argues, aside from the more immediate harms of AI and Data Apparatus, the path AI enables towards a full-scale, comprehensive algorithmic authoritarianism is more harmful as it lends itself to fascism, or what others call ‘digital authoritarianism’. In the contemporary world, AI conflates with a coming global crisis and a *status quo*, enabling and empowering fascistic tendencies; and this is not about usage of AI by authoritarians as much as it is about a deeper link, rooted into the nature of technology and the worldview it assumes. Furthermore, the information regime in general and AI in particular are surrounded by a collection of metaphors to naturalise capital accumulation and provide, in effect, justifications for

AI institutions (Katz, 2020). This is done either by the tech advocates and corporations, or by others who seem to advocate for solutions that neglect the realities of this regime, and are rather reinforcing the logic of the master (ibid.; Salter & Dutta, 2023).

The information regime, with data infrastructures and AI, is oriented to serve imperial and capitalist endeavours and interests, which are based on surveillance as the primary apparatus for control—in line with the main argument of this thesis. If one is to meaningfully speak of surveillance in the era of Big Data and Advanced Algorithms, it must be in relation to this digital ecosystem, the information regime, with its primary technologies, which seek to capture everything as data and process it with its advanced algorithms. Indeed, AI is a surveillance technology.

Coming to the relationship between control by surveillance and counter-surveillance, this is one of intimate and interdependent nature. As such, a study of any form of counter-surveillance should take into account the context within which it acts and the targets it sets out to act against. Communication technologies have both enabled and constricted those seeking to control as well as those falling under control, actually or potentially.

Perhaps a detour into the history of technological communication revolutions might serve to demonstrate this point. Since this thesis focuses on technological counter-surveillance primarily using encryption technologies, the examples relate to encryption as well. Throughout human history there has been a quest to ensure the facility, integrity and authenticity (the triad generally known as CIA), in other words confidentiality and availability, of correspondences, for a variety of reasons and out of different motivations. To that end, many communication technologies were developed even though some particular inventions became milestones in the history of communications. To ensure the integrity and authenticity of the transacted message, encryption has been a sort of corollary to such developments in the field of communication.

Encryption has challenged and has been challenged by these developments –with odds favouring one over the other at different times. The question of encryption is at

heart an issue of communication. It involves a perception of an ‘other’—the surveillant agent. Whether it is targeted or untargeted surveillance, encryption is seen as the remedy against surveillance, especially when information is transmitted in an unsecure network of communication, like the internet. The history of communications and the technological revolutions that have taken place within it demonstrate this tendency that each technological or methodological development has an impact for surveillance as much as it has for counter-surveillance. This is the case despite the asymmetry that reflects the networks of power relations within which it exists, an asymmetry relational to the locus of the agent in power relations. As such, counter-surveillance as such is an integral part of the power ‘game’; it is at once both an act of surveillance and of resistance. With coded bias/inequality there is coded resistance/antagonism, but this coded resistance can at the same time be serving the powerful hegemonic oppressors as much as the oppressors are serving resistance.

There have been a number of revolutions in the development of communication technologies since the finding of the alphabet by early Phoenicians and with the widespread of literacy. These technologies had enabled the citizenry to ensure the integrity and authenticity of their messages, while the state was further enabled to intercept these messages with more facility and alter them when officials desired, threatening the integrity of the message. The surveillance capabilities increased as the literacy rates increased. Literacy, being a positive development, is now enabling further state surveillance. Using the ‘arms of the master’ as proposed by many counter-surveillance initiatives and individuals, and the ethos of technological resistance have been re-used by the same masters, who invest in these developments, repurposing them so as to serve their control (or administration, as they might call it) aspirations further.

With the invention of the Gutenberg press and later developments in printing technology, counter narratives were facilitated in terms of the reach of their message and the prolificity. Yet at the same time, the state (and the Church in this case), with all its apparatuses, power and capabilities was further enabled to intrench its presence, narrative and become more culturally hegemonic and capable of justifying

itself for using coercion, as the sole monopole of such power. At earlier times, it was owned mainly by the state and the powerful, yet with the further ‘democratisation’ of such technologies, counter narratives spread and the predecessors of journalism emerged (Matykiewicz-Włodarska, 2023). At the same time states were now able to have a better grasp on their ideological character and more, what is called the ‘print wars’, where politicisation was high, with polemicists started applying their persuasion in writing (Debbagi Baranova). These were the early seeds for the first generation of open-source intelligence (OSINT), with practices of analysing newspapers of enemy countries and domestic oppositional groups. These facilities were furthered with the advent of postal service, which reduced the costs of sending letters for the citizenry with the integrity of the contents being relatively higher. Yet at the same time this centralisation resulted in an augmentation of surveillance capabilities and methods by the state for tampering with correspondence; and where interception became more transparent, it became a common policy for states to censor and read letters.

The technological developments accompanying advancement in electromagnetics, which gradually became in use like the telegraph and the telephone, further intensified the surveillance capacities of the state. While transmission was taking place at historically unprecedented speeds, the communications were primarily unencrypted and the actors involved in making such correspondences possible at the sender and the receiver ends of the transaction. The processes were owned or heavily regulated by states, even though some people used to incorporate codes, in contrast to cyphers. It is perhaps with the telephone that this kind of electromagnetic communication has taken a global dimension. It provided the ability to organise dissent and communicate with people who were not easy to reach before. At the same time, the intrusive ears of the state were more intrusive in the sense that gradually, in a targeted or untargeted manner, home conversations were taped and greater levels of details were accessible to the state and surveillance eye/ear. This might be a cusp point where surveillance apparatuses had started growing tremendously in terms of capabilities in both breadth and depth.

Computer networks bring this historical curve into a different direction. Computer networks, especially the internet, are perhaps the most significant of all revolutions

in the realm of communication and in relation to the pervasiveness and intrusion of surveillance. Other computational technologies are intimate to surveillance as well. In the digital era, surveillance relies essentially on the internet and advanced algorithms. The internet allows for mass surveillance, and surveillance by internet-based platforms enables the collection of data sought by state agencies (Lyon, 2022; See also, Srnicek, 2016) and corporations, among other actors. Issues concerning control and emancipation and the harmful impacts of computational technologies have emerged since shortly after the development of the first (public) computers. They developed in parallel with camps emphasising the control potential of these technologies while others emphasising their emancipatory, democratic potential. Discussions and attempts to understand and deal with this rapidly growing apparatus/paradigm proliferated in an unprecedented pace and fashion.

Despite its historical ubiquity (Weller, 2022), surveillance after the digital revolution has taken a new dimension. Surveillance has grown in both breadth and depth. This has been particularly the case after what is termed the ‘data revolution’, referring to the widespread application of various data infrastructures (Big data or Small Data alike) with the spike in the development of advanced algorithms to manage, store and process the collected data. The ‘electronic eye’ (Lyon,1994) is now gazing over spheres that were out of reach for previous surveillance technologies, and in terms of depth, being able to build prototypes of individuals, their behaviours, and what was considered to be the intimately private sphere of a community or a family.

Indeed, surveillance has become a lucrative market in itself with the digital revolution being the driving force behind it. Moreover, digital technologies led to the intensification of state surveillance, leading to the contemporary “information state” (Weller, 2012). Furthermore, digital technologies and the development in data infrastructures has led to novel forms of social surveillance, including lateral surveillance, sousveillance, social surveillance and self-surveillance, with new behaviours associated with surveillance. Surveillance under the information regime, based on Big Data and advanced algorithms, has become a global archipelago of a complex variety in actors, tools and domains (Laurent, 2022).

A principal premise for this thesis is the postulate that surveillance is the primary apparatus of control and domination in the era of the information regime. Historically, surveillance has an intimate relationship with control as domination. Surveillance is not the mere act of seeing or watching. Surveillance in essence pertains to the implicit laws and covenants which connects the social, and renders individuals compliant with the frameworks within which they are located (Zayid, 2013, 14). Such surveillance can be in the form of state surveillance, private corporate surveillance in the work sphere, or social surveillance that seeks to ensure and enforce conformity with the ethics of a particular society. The following section looks into the relationship between surveillance and control.

### **2.3. Surveillance and Control**

The study of surveillance has increased drastically in the past 30 years. This suggests the scale to which surveillance has reached and the centrality it has assumed in contemporary times. Within the interdisciplinary field of surveillance studies, surveillance is conceptualised in a variety of ways. Surveillance is a highly (and an essentially) contested concept and, moreover, it is an inherently critical concept (Lyon, 2022). Lyon (2022) identifies four senses of surveillance, namely the etymological meaning of surveillance as observation, surveillance as sorting of population, digitised surveillance and dataveillance. Moreover, surveillance is a multidisciplinary concept. It is connected and conflated with other concepts like monitoring and spying, and is intimately linked to concepts like privacy and internet freedom, which are themselves essentially contested concepts.

This leads to an important issue in relation to the conceptualisation and definition of surveillance. Should surveillance be tied necessarily to control, or is it a neutral social phenomenon that can be of positive and negative depending on the social and political context within which it is deployed and utilised? Scholars diverge on whether surveillance is a negative or a neutral phenomenon. As such, on the one hand, some scholars view surveillance as a means and instrument of control, analysed from variety of perspectives, including political economy and class relations (Lyon, 2022; Zuboff, 2019; Srnicek, 2016; Fuchs, 2010, 2012, 2017), or

race and colonialism (Lyon 2022; Benjamin, 2019; Browne, 2015; Choi et al., 2021), or gender (Abu-Laban, 2015).

On the other hand, some other scholars find such conceptualizations and narrow definitions that only focus on the negative aspects of surveillance, in terms for control, to be lacking, inadequate and severely limited (Marx, 2015; Marx, 2012; Haggerty, 2006). According to these scholars, adopting such a narrow definition consciously opposes the beneficial outcomes of surveillance technologies (Lyon et al, 2012; Haggerty, 2006). According to Haggerty (2006), Surveillance Studies replicate a normative orientation involving a hermeneutics of suspicion. This casts a negative light on new developments, which are seen by such authors to be leading to the intensification and the expansion of surveillance as an instrument of control. As such, surveillance initiatives are located in opposition to civil libertarian rights. One such reason for this tendency, according to Haggerty, “relates to the fact that surveillance scholars are trained in a tradition of critique. Acknowledging and emphasizing the potentially positive uses of surveillance practices risks moving the analysis from critic into advocate and claims-maker on behalf of the system itself.” (2006, 36)

Examples given as to the positive impacts or applications of surveillance include disease control and parenting (ibid.; Marx, 2016). Marx (2016) goes further to associate surveillance with ‘responsibility’ which gives surveillance a positive denotation, in opposition to, say, indifference or carelessness. With such association being an example for the neutrality of surveillance as a phenomenon, he suggests that the conventional definition of surveillance, as necessarily involving hierarchy and social control by watching over, is inadequate. Even families involve power differences, for purposes other than control as domination, which include protection or entertainment. Such cases include an element of reciprocity in surveillance, with a bi-directionality, despite the asymmetry or lack thereof, and despite the inequality within or the quality of such reciprocity. For example, in democratic societies both the states and the citizenry surveil each other despite differences in form or degree. In authoritarian regimes, however, surveillance is non-reciprocal and unidirectional (Marx, 2012; 2015). This reciprocity between governments and citizenry can be one

of three broad possibilities: the ratio favours government, favours citizens, or relatively equal (Marx, 2016), including sousveillance. This reciprocity of surveillance for Marx is important for understanding and capturing the phenomenon of surveillance, and one of the bases of his ‘neutralist’ position on surveillance. Furthermore, by making the distinction between strategic and non-strategic surveillance, Marx strips the purposiveness from the act of surveillance, rendering the intentionality within surveillance dependent on context and occasion.

Marx goes further to contend that surveillance can facilitate the protection of privacy as can be seen through biometric identification and audit trails, or video cameras, filming operators with access to sensitive data. At the same time, according to him, privacy can protect surveillance, as seen in the example of undercover police officers using fake identification cards. Privacy protects surveillance as much as it can nullify it; for example, through encryption. Hence, “[p]rivacy for whom and surveillance of whom and by whom and for what reasons need to be specified.” (Marx, 2016, 23; 2015).

Scholars on this camp prefer to conceive of surveillance as a neutral concept and phenomenon. They emphasise that possible positive and negative implications of surveillance provide Surveillance Studies with a normative orientation, meaning that “surveillance is capable of being used for both desirable and detestable things” (Lyon et al, 2012, 03). For Marx (2015), “at the most basic level, surveillance is simply a way of discovering and noting data that may be converted to information.” (736). A central thesis for Marx is that “*surveillance by itself is neither good nor bad, but context and comportment make it so.*” (Marx, 2016, 10, 284, 320. Italicised in the original text in the three instances; see also, Marx, 2012; 2015).

Surveillance, from this perspective, is, at its core, merely the generic social practice of collecting data; even when it involves social sorting and profiling. Surveillance does not aim to control nor does it inherently possessive of any directionality, since it includes a variety of purposes and objectives where control is but only one possible purpose, or even an outcome of surveillance, and since it can be bidirectional, horizontal or vertical; up-down or bottom-up (Marx, 2015). Furthermore,

surveillance is a natural, universal and fundamental character and process of society; it is a practice that “cut[s] across institutions; individuals in interaction; the interaction of organizations with each other; and the public and private sectors.” (2012. xxi)

In fact, Marx (2012) contends that, unlike the common tendency in critical surveillance studies, the initial question should not be as to whether surveillance is good or bad. The departure points for investigating the phenomenon of surveillance should be a construction of a conceptual map to capture the main structures and process of surveillance and to categorise the diverse settings and technologies. Only afterwards, according to him, can one ask questions relevant to values, facts, and contemplate possible ways to distinguish between appropriate and inappropriate uses. In fact, he conceives of such conceptual map as the core of his project, since this is the way to resolve the value conflicts present everywhere, since, for instance, while legal means can reduce harms and contain the inappropriate use of surveillance, it can potentially expand the use of such tools, and, for example, the watchers might also be watched by the same technologies they use (Marx, 2012).

Such a tendency to conceive of surveillance from a value-neutral, ‘scientific’ lens is found in the literature of surveillance studies. Some accounts can radiate ambivalence, nonetheless, as to the negativity or positivity of surveillance, or at least display some vagueness. On the other hand, there are those who emphasise the necessity of making surveillance a negative, alienated concept. Christian Fuchs (2010) argues for the necessity of defining surveillance with a negative light, and not as a positive, self-evident or natural social phenomenon. Negatively conceptualised, the concept of surveillance highlights the negativity of power structures in heteronomous societies, and identifies and denounces domination. He advocates for a society without surveillance, an emancipated society.

In a negative theory, surveillance is a negative concept that is inherently linked to information gathering for the purposes of domination, violence, and coercion and thereby at the same time accuses such states of society and makes political demands for a participatory, co-operative, dominationless society that is not only a society where co-operative modes of production and

ownership replace classes and the exploitation of surplus value, but also a society where care and solidarity – in one word: democratic socialism – substitute surveillance. (5)

At its core, surveillance is not the mere collection of data/information; rather, it is “an expression of instrumental reason and competition because it is based on the idea that others are watched and data on their behaviour, ideas, look, etc. are gathered so that they can be controlled and disciplined and choose certain actions and avoid others that are considered as undesirable.” (Fuchs, 2010, 11). Fuchs builds on the assumption of what he later calls Radical Digital Humanism (Fuchs, 2022).

Fuchs identifies a number of assumptions present within that neutral concept of surveillance. They speak of the positive aspects of surveillance, surveillance has two faces (Janus-faced, ‘perhaps even better, octo-[faced]’, Marx, 2016, 10). They have at least one of the following assumptions: that there are positive aspects of surveillance; that surveillance is both enabling and constraining; that surveillance is a natural social phenomenon present in all social formations; that surveillance is a necessary process for social and political organisation; and that surveillance refers to any form of systematic information gathering.

Fuchs does not deny the positive potentials, and does not efface the potential for a transformation in society with positive visions. Yet, contemporary society is heteronomous and he rightly notes that “we cannot assume that the pros and cons of information technology are equally distributed, the negative ones are automatically present, the positive ones remain much more latent, precarious, and have to be realized in struggles” (2010, 14). It is necessary “to make surveillance a strange concept that is connected to feelings of alienation and domination. For doing so, it is necessary to alienate the notion of surveillance from its normalized neutral usage.” (15).

Fuchs moves forward to discuss four reasons for opposing the neutralist conceptualisation of surveillance. In summary these are: the etymological reason, theoretical conflationism, the difference between information gathering and surveillance, and normalisation of surveillance. The first reason concerns the

etymological origin of the word surveillance. The connotations of the word 'surveillance' have always been negative, implying hierarchies that have to do with domination and coercion, whether actual or potential. The 'over' ('sur') in 'watching over' (sur + veiller) state a directionality going top down, as 'an "expression and instrument of power" used "to control human behavior"' (Gilliom 2001, 3, in Fuchs, 2010, 13). Nevertheless, this argument neglects the fact that linguistic signs are never stable, especially as they travel through time, the signifier never signifies the same signified constantly. From another philosophical perspective, words belong to families of meaning, some connotations have positive meaning, like monitoring (which Fuchs, 2010, proposes as a more democratic alternative) or observation, depending on the context and sitting within which they take place. A relevant case to point in this discussion is the word 'data' itself, which has lost its original Latin meaning today, changing from its original meaning (to give) to the contemporary meaning (to take) (Kitchin, 2014a).

Another reason is the difference between surveillance on the one hand, and information gathering, on the other, which neutralist definitions seem to emphasise, or even reduce surveillance to this act. Fuchs points out that if surveillance amounts to systematic information gathering, then Surveillance Studies is merely the same as information society studies, and surveillance society is nothing but the information society. For him, however, information processes, and by extension, surveillance society are broader, more general categories, within which surveillance takes place. The surveillance society is heteronomous information society, in which surveillance represents the negative processes of information gathering in this society, and the impacts and harms therein are dependent on other contextual factors. "It is opposed to the notion of a participatory, co-operative, sustainable information society." (2010, 14) In opposition, he proposes solidarity, which enables a categorical separation between the negative and positive aspects and outcomes.

This is indeed an important and necessary distinction, that is needed due to the complexities of 'new surveillance' (using the parlance of Marx, 2016). This is important also in consideration of the following reason Fuchs presents: the normalization of surveillance. According to him, if surveillance is merely a

fundamental aspect of social life, and is something that is present everywhere, and if everything is surveillance, then the outcome of such conceptualisation is passive acceptance of the phenomenon of surveillance. It becomes a normalised phenomenon that renders criticism of the coercive and violent processes of information gathering difficult; especially after 9/11, when repressive surveillance witnessed intensification and extension. This normalisation, furthermore, allows for an ideological justification of means of oppression, by policy and powerful actors, presenting it as inevitable and necessary.

Moreover, in accordance with his political and normative assumptions, Fuchs contends that such conceptualisations leave no space that is outside surveillance, and we might say, no room for resistance, or the process of neutralisation of surveillance. On this account however, it is doubtful whether the cause-effect relation is in the manner Fuchs presents. The effect of such normalisation, and its causes, might not be so straightforward, and the role of neutralist conceptualisations are not as presented. Indeed, this is a difference in positions about the role of theory in reinforcing or changing the *status quo*. But under the information regime, the pervasiveness and penetration of surveillance structures, processes, and means necessitate a different approach to this problem regarding the conceptualisation of surveillance. Whether neutralist positions are the cause of the information regime or a by-product of it is a different, though a worthwhile, question; and it might not be answerable in a straightforward manner.

The final reason, and perhaps the most important among the four reasons, presented by Fuchs against defining surveillance in a neutral way (and also for the necessity of the separation he calls for) is conceptual conflationism. Neutralist positions on surveillance advocate that surveillance has positive aspects and goals, which, depending on the context, are necessary. Surveillance can aim at care as much as it can aim at control (Lyon, 2022; Marx, 2016). Examples of such positive and necessary surveillance practices include parents monitoring their children or, for instance, surveillance video cameras in church, used for control and documentation, which later were used to deliver services to the needy unable to attend (Marx, 2016). These are categorised in what Marx (2015) calls ‘role relationship surveillance’ as a

form of ‘non-organisational surveillance’ where family members can surveil children or an anxious spouse, or friends trying to find each other. Surveillance is also seen as a protective of freedom and liberty, as an appropriate vigilance against risks, pandemics, corruption or crime.

Categorizing all such activities under surveillance, as an umbrella term (Marx, 2012) results in a situation where different levels of analysis as well as various practices are conflated and confused, both theoretically and analytically, according to Fuchs. The differences between domination and care would not be distinguished easily. Justification for instruments of control make use of the marginal care potentially provided. The borders between coercive and non-coercive information becomes hard to distinguish and makes it difficult to “categorically fix the degree of coercive severity of certain forms of surveillance. The double definitional strategy paves the categorical way for trivializing coercive forms of surveillance.” (13) To address this issue, he proposes the term ‘monitoring’ in contrast to ‘surveillance’. This distinction is not simply a choice of names, but describes the characteristics of different archetypes and varying social and political phenomena, with different impacts.

There are other important reasons that can be discussed in addition to the ones provided by Fuchs. In consideration of the scale of the harms and negative impact that everyone -even neutralists- accept, treating surveillance as an all-encompassing, umbrella concept, leads to being a form of an apologetic attitude and reinforces the *status-quo*; not least because of the conflation created and the normalisation spoken of by Fuchs. It serves to reinforce the *status quo* and the logic of surveillance capitalism that keeps advertising itself in line with technical solutionism, promising to be the solution for complex social and political problems, in effect crushing democracy and the potential for change. It depoliticizes surveillance, which is inherently a political act, and which is an inherently critical concept (Lyon, 2022).

Nevertheless, what is more important is the logical fallacy that is committed in this line of thought-- *non sequitur* fallacy. There is a (formal) logical gap in going from surveillance as a positive act to the conclusion that surveillance is, or should be neutral. Indeed, the questions “surveillance of whom and by whom and for what

reasons” (Marx, 2012, 23) are important and necessary, both analytically and theoretically, but jumping to state that surveillance is a neutral, universal phenomenon, relegates the question in a depoliticised way and renders it uncritical. Another premise is missing, possibly reading as ‘we have to accept the *status quo* as is’.

Moreover, history shows positive outcomes produced by the most atavistic and oppressive regimes and ideologies as well as discursive and ideological claims of potential positive outcomes. The Third Reich witnessed a significant reduction in unemployment, a reduction that ‘border[s] on the miraculous’ but one ought to ask, by what means and at what costs (Silverman, 1988 ,185).

Colonialism is a case in point. It is proper both in terms of events as well as of knowledge. The (perceived) positive aspects of colonialism (or of capitalism for that matter) can be indeed observed. For example, in British colonised Malaysia the infrastructure was a good development, where highways were paved and a proper railway system was constructed that connected major centres in the peninsula. Major cities, additionally, were equipped with electricity and potable water. This, however, does not lead one into concluding that one should study colonialism as a neutral, or umbrella term, since it had positive outcomes. Important here is the intentions behind such a system, which might inadvertently lead to positive outcomes. The original motives of such developments were to serve the interests of British colonists in Malaya, by facilitating the exploitative projects of mining and plantation, in a context of poverty for the natives and a system of government managed by ‘divide-and-rule’. Such motives can be seen, moreover, by the differences between the various colonial contexts, either by the same or different colonising powers.

In an ‘objective,’ ‘scientific’ universe inhabited by ‘real’ scholars, the motives for imperialist colonialism were at worst ambiguous, mostly benevolent, even at times admired. “There was no essential motive or set of motives that drove the British Empire. The reasons why the British built an empire were many and various. They differed between trader, migrant, soldier, missionary, entrepreneur, financier,

government official and statesman.” (Biggar, 2023, 44)<sup>3</sup>. However, like any other human endeavour there were corrupted vices, but nothing was of systemic or central perversion. This, moreover, is the case in most empires, with exception, nevertheless, like the Nazis, which was the fruit of a single mind, with allies (ibid). The British empire, by its ‘civilising mission,’ (to use a concept employed by French colonisers in Africa) sought “the aversion to poverty and persecution, the yearning for a better life, the desire to make one’s way in the world, the duty to satisfy shareholders, the lure of adventure, cultural curiosity, the need to make peace and keep it, the concomitant need to maintain martial prestige, the imperative of gaining military or political advantage over enemies and rivals, and the vocation to lift oppression and establish stable self-government.” (ibid., 44). Such would be a passionate argument cloaked in objectivity and neutrality in speaking of colonialism.

Casting ambiguity on the motives or the resultant harms of the system of control by surveillance is akin to colonialism being ‘reassessed’, according to some politically passionate academics on the right of the political spectrum. While scholars advocating for a neutral conceptualisation of surveillance are not at the same level as advocates of extensive surveillance, both, in effect, to various degrees, are casting ambiguity on a system of control, the harms of which can be felt everywhere. While the scholars calling for a more neutral conception of surveillance, will not go as far as calling colonialism an all-over positive process, or for reinstating a total comprehensive surveillance system—in fact, most do the opposite. And while they might not reach to make a statement about anti-surveillance like the following: “[i]t is hard to overstate the pernicious effects of global anti-colonialism on domestic and international affairs” (05). Their arguments, in effect, justify the use and expansion of such technologies of power.

Adopting the neutralist logic, it follows that indeed, colonialism can lift oppression as much as it can be oppressive. The leading imperial motive of those ruling Britain at the time was the desire of self-defence (22), after all the East India company discouraged mass migration of Europeans, and had the Ottomans not chosen to ally with Germany in 1914, Britain would have never decided to control Palestine and

---

<sup>3</sup> For a scholarly assessment of Biggar’s book, see Lester, 2023.

Iraq. Indeed, even the Balfour declaration, was only because Balfour was “moved to tears by Chaim Weizmann’s stories of Jewish suffering from antisemitism” (37), yet the wording of the declaration is rather ambiguous on what he meant by a ‘national home’ for the Jews. We might then seek an objective costs/benefits approach, and need to ask what would likely have happened in a context without colonial rule (Gilley, 2017). “But actually existing Guineans may be asking: When are the Portuguese coming back?” (ibid., 06), when they faced the problems of the world, advocating for reinstating colonialism, either directly or indirectly (Gilley, 2017; 2023).

In addition to the logical gap discussed above, a neutral conceptualisation of surveillance fails to contextualise the problem at hand. Surveillance can be voluntary (Marx, 2012, 2016), and colonialism “appears to have been highly legitimate and for good reasons.” (Gilley, 2017, 04). Millions moved closer to areas under the colonial rule, educated and hospitalised, even served in colonial governments and institutions, and even reported crimes to colonial police, “all relatively voluntary acts”. Indeed, the spread of colonisation was with very little force, and the Sultan of Brunei installed James Brooke, an English traveller as the rajah of Sarawak and preferred his rule over the province (Gilley, 2017, 04). While this logic is not commonplace in relation to the subject of colonialism, it is rather commonplace in relation to other matters, such as gender equality or the rights of different sexual orientations, where practices, attitudes and rhetoric of colonialism are still visible in relation the Global South (Lyon 2022; Kwet, 2019). Indeed, failing to understand surveillance in the socio-economic context within which it takes place would only lead to such accounts, and to a reinforcement of such processes and structures of domination and exploitation.

If data is volunteered, it is because of the broader social and cultural context within which the individual is located. Lyon (2019) emphasises the significance of understanding the relationship between ‘surveillance capitalism’ and ‘surveillance culture’. According to him, “[t]he surveillance culture has an intimate and mutually-informing relationship with surveillance capitalism” (Lyon, 2019, 72). It is in such a relational context that people are conditioned to voluntarily hand out data and private

information, non-coercively, as it were. It is a context in which “the dominant aspects of surveillance culture often play into surveillance capitalism, facilitating and normalising it ... [and in which] much of surveillance culture depends on and is nurtured by surveillance capitalism” (72). Surveillance capitalism enables what enables many aspects of surveillance culture, much of which, in turn, reinforces surveillance capitalism.

The individual and the society are located in a regime attributed to the primacy of information, ‘the information regime,’ in which, a new mode of control is present, that is neoliberal psychopolitics, which seduces rather than coerces, and which internalises surveillance rather than forcing from outside (more on this below) (Han, 2017, 2022). Indeed, the Gramscian distinction between hegemony and domination is informative in this discussion. To bring the example of colonialism once more, it is important to note that an objective of colonialism is to bring about the conditions of possibility for the exploitation of the colonised (Ocheni and Nwankwo, 2012). This can take place through both coercive as well as non-coercive means for the end of control for exploitation.

Moreover, such accounts are ahistorical. This ahistoricity is a result of the tendency to bend the definition of surveillance. It renders surveillance meaningless (McQuade, 2018). The history of surveillance points towards an intimate relation between the need to control and dominate the population on the one hand and, on the other, devising, refining, developing and (coercively) deploying surveillance tools. In the case of Egypt for instance, we can witness how surveillance was essentially developed and institutionalised, in both colonial and post-colonial states, as a tool for control and subjugation of the individual and society, and how it was intimately linked with both direct and symbolic violence (Zayid, 2013). Through two central surveillance practices -population count and spatial monitoring, the Palestinians witnessed the extreme levels of hierarchisation (Zureik, 2013). As in British-colonised India, the colonisers needed and developed ‘investigative methods’ to facilitate their imperial project, instrumentalising discursive (ibid.) and manipulation of law (Barakat, 2013). In addition, and in a different context, in early China, in order to maintain a socio-political regime, where people sense the constant gaze of

the state, ancient statesmen and rulers attempted to build comprehensive infrastructures to encompass the entire population and networks of surveillance, from peasants to high officials, to ensure population control and management (Robinson, 2022). Moreover, attempts to resist surveillance of the population or at the workplace (for a variety of reasons), when implemented, suggest the essential purpose of such surveillance systems (Kırlı, 2013; Seewell, 2022).

Since I elaborated on colonialism as a contrastive phenomenon to that of surveillance, one issue must be addressed in this discussion. This pertains to the question as to whether colonialism and surveillance should be considered at the same level of analysis? Whether they can be contrasted legitimately as such. Indeed, such comparison does not assume that the two are parallel nor are they the same phenomena. Rather, the discussion was to demonstrate a logical gap present within a conception of surveillance as a neutral, universal phenomenon. This notwithstanding, as was seen above, the historical realities show the link between colonialism and surveillance, with surveillance as a primary technology of and for power.

That in the era of big data and algorithms, the information regime in the parlance of Byung Chul-Han, surveillance is the primary apparatus for control and domination is the central assumption of this thesis, as the context for technologist counter-surveillance. Surveillance aims at control through the modulation of behaviour, either for profit or political objectives, and so does colonialism which aims at political and economic control, for political domination or economic exploitation. Furthermore, a second objective of domination is “to make possible the exploitation of the colonized country” (Ocheni and Nwankwo 2012, 46), by various processes and techniques of legitimation and oppression. A difference, however, might be in relation to the ratio between hegemony and domination in the quest of control or between the deployment of coercive and non-coercive means. A matter of degree rather than of kind, dependent on the kind of heteronomeity present within a society. “Colonialism was not just a physical act of aggression, it was an ideology formed to justify conquest and pacify resistance.” (Kwet, 2019, 16).

Indeed, artifacts of colonialism are still present today, and colonising activities are still visible. Moreover, these issues are inseparable from matters of race and

surveillance (Lyon, 2022). Surveillance not only enforces racial inequalities but also takes place in an essentially different manner between the Global North and the Global South. “Like the railroads of empire, surveillance capitalists extract data out of the Global South, process it in the metropolitan centre, and spit back information services to colonial subjects, who cannot compete” (Kwet, 2019, 14).

In addition, a number of scholars take this further. In relation to data, the nutrition/oil for surveillance and advanced algorithms, Couldry and Mejiias (2018) propose the terms ‘data colonialism’. Data colonialism aims at appropriating and exploiting both life as well as the individual. They observe striking parallels between data colonialism and historical colonialism, which sought to appropriate and exploit territories and resources. Data colonialism is a novel mode of colonialism, which “combines the predatory extractive practices of historical colonialism with the abstract quantification methods of computing” (337). For the authors, it sets the preconditions of a new stage of capitalism, the nature of which is yet to be comprehended, revolving around data. It is a new social order, based on social quantification and the commodification of social relations; turning them into data relations. The ‘social’ is reproduced for capital, that is ready for appropriation as data, that is capital, through continuous surveillance, collection, and categorisation. To that end, the authors argue, the rationalities underlying data extraction are naturalised through legal, philosophical, ideological works, and data are constructed as raw material that is just out there to be used, through discursive moves. “The extraction of data from bodies, things, and systems create new possibilities for managing everything. This is the new and distinctive role of platforms and other environments of routine data extraction.” (p. 343). Moreover, it is real human beings, not the statistical “data double” of the algorithms, which are to face the discrimination of the knowledge produced, and what is at stake is the reality of the self as a self. The continuous tracking of life, they add, renders it dispossessed, and the first stage of resisting this new mode of governance and control is by identifying it as data colonialism as well as its absolute-universalist rationale of extracting data and controlling humans through data.

Kwet (2019) investigates what he calls ‘digital colonialism’ in South Africa, as a case within the Global South, which describes a form of structural domination. In

this new form of colonialism Big Tech companies (GAFAM: Google, Alphabet, Amazon, Facebook, Apple, and Microsoft) and intelligence agencies are the ‘new imperialists’, with immense political, economic and social power by maintaining centralised control and ownership by a small number of US multinationals of/over the digital ecosystem—with its three core pillars, i.e. software, hardware, and network connectivity. Like architecture in the colonial era where critical infrastructure and labour were controlled and designed by the colonialists, the digital ecosystem is designed to not only serve the interests of these new imperialists, but also to maintain such monopoly and control over the Global South-- through rent and surveillance, by owning and controlling software, hardware and network connectivity. “This allows them to accumulate profits from revenues derived from rent (in the form of intellectual property or access to infrastructure) and surveillance (in the form of Big Data). It also empowers them to exercise control over the flow of information (such as the distribution of news and streaming services), social activities (like social networking and cultural exchange), and a plethora of other political, social, economic and military functions mediated by their technologies.” (08).

What is at stake here is the assimilation enforced by these technological companies. Within this process, the United States leads the twenty-first century form of colonisation by assimilating the technological products, digital models and associated ideological discourses. This takes place to the detriment of local and strategic development, much as was the case in traditional colonialism. As Kwet (2019) underlines, “foreign corporations undermine local development, dominate the market, and extract revenue from the Global South, with power obtained primarily through the structural domination of digital architecture, which leads to more general forms of imperial control.” (07)

Importantly, Kwet shows how another element of digital colonialism intensified, that is state surveillance, through the intimate relationship between local states, the USA, and these Big Tech corporations -what others have called, the surveillance-industrial complex. This domination of the digital architecture by the Global North, resulted in a global surveillance capitalism, in which the Global South is not merely at

disadvantage with their critical infrastructures dispossessed, but also “[i]t is nearly impossible for Global South firms to compete with these established giants” (03).

In conclusion, surveillance is an apparatus for control as domination. It is intimately linked with attempts by states and corporations to control populations for population management and profit. Furthermore, surveillance is the central apparatus of control in the era of Big Data and advanced algorithms, that is the information regime. In order to understand technologist counter-surveillance in a meaningful way, and in order to see the possibilities for its efficacy in relation to democratic change, one must see surveillance in this context, as it is the target of this form of resistance. That is, in order to understand the dilemma of technologist counter surveillance, there is the need to contextualise it by questioning how technologist counter-surveillance attempts to engage with and target the power relations inherent in the information regime and infocracy. With surveillance being the central apparatus of domination and control, it becomes of no surprise that the technologist counter-surveillance arises primarily to dismantle the surveillance industry complex for democratic change, through the use of various tactics and strategies. Before moving to discuss and examine technologist counter-surveillance in the next chapter, we now look into how counter-surveillance is a corollary of surveillance.

#### **2.4. Counter-Surveillance**

Control and domination always entail resistance. Hegemony results in counter-hegemony. The introduction of a new surveillance system has always been accompanied with attempts to render it futile or at least to reduce the effects of the surveillance system through a variety of tactics and strategies. For instance, communist resistance to assembly line surveillance at the Stollwerck Chocolate Factory in the 1920s highlights the limits of this form of surveillance in relation to workplace surveillance. Surveillance was subverted by employing the same tactics of the factory (Sewell, 2022), employing the ‘arms of the master’, in the parlance of the modern Cypherpunks. In the information regime, where surveillance is perhaps of unprecedented centrality, the relation between surveillance and counter-surveillance might not be straightforward, and the efficacy of the later to reduce the harms, or

annul, the former might not be without serious limitations. To this end, recent insights from resistance studies would help the endeavour of this thesis.

A quick look into resistance events in the digital era reveals a complexity and interconnectedness between the different actors as well as between the various forms, tactics and strategies of resistance. These include the use of digital means as well as more conventional means of resistance, or a mix of both. Moreover, they can target the digital infrastructure itself or other less-technical institutions, like bureaucracy, for the unjust use of Big-Data algorithms or other injustices. Mostly however, they seem to combine different elements and objectives, being multi-modal in their approach—both enacting and drawing from earlier modes and tactics of resistance.

For example, the well-known Anonymous assumed different faces and roles, from online trolling for political purposes to mobilising campaigns and conducting organising hacking operations, some of which had elements found in intelligence organisations. On the one hand, Anonymous enacted tactics that are considered conventional modes of resistance, like their emphasis on journalism and street protests. On the other hand, they enacted tactics that were distinctively digital in nature, like DDoS (denial-of-service)<sup>4</sup> attacks. In fact, many such movements emphasise such a combination as a necessity to achieve efficacy and to expand the reach of their actions, as could be seen in the cases of Anonymous, the Cypherpunks, and +KAOS, the latter of which had intimate relations with more reaching political parties in Italy (Maxigas, 2015).

Moreover, despite being digital in nature, and sometimes acting for purely digital objectives, these movements involved individuals with varying kinds of expertise. As was seen in relation to the Cypherpunks, the Californian Ideology<sup>5</sup> was the result of collaboration among hackers, but also writers, capitalists and artists. Influential

---

<sup>4</sup> DDoS refers to Denial of Service Attacks. These attacks overload the server computers of the targeted website or organisation, with the services and the systems crashing down. This prevents legitimate users from accessing the online services of the targeted organisation, and can lead to huge economic losses. One example is the attacks against Paypal, Master Card, and Visa Card as a response to their stopping any donation transactions made for Wikileaks.

<sup>5</sup> For the far-reaching appeal and power of the Californian ideology, see Curtis, 2011 for example.

original contributors to the Cypherpunk mailing list also included journalists, lawyers, and even architects and medical students. In relation to this, it is worth noting that architecture in particular is quite involved in digital resistance, in particular in conjunction with Open-source intelligence, data mining and methods like geolocation. Another example is the Demoscenes of Central Europe hacking scene, promoting exhibition of computer capabilities and digital art, and later organising groups for ‘cracking’<sup>6</sup> software and sharing pirated versions.

In relation to this and concerning the technical abilities, an important point is worth noting. There is, within Anonymous and similar digital resistance movements, a mix in the technical abilities that members or contributing individuals possess. Many, if not most, of those involved in hacktivism operations had little technical knowledge. Coleman (2015) notes that within Anonymous there was a tension between those who are hackers, with technical knowledge of computers and computer networks, who thought of DDoS attacks as lame priding themselves for being real hackers, on one hand, and ‘script kiddies’ (or skids, skiddies)<sup>7</sup>, who lacked proper technical knowledge. Some hackers dismissed Anonymous on the basis of it being a collective of trolling script kiddies, with others within Anonymous insisting on being real hackers and hacktivists. Skare (2018) makes a similar point concerning a particular hacktivist group in Gaza, called Hacker-Gaza, which despite having a clear organisational hierarchy the many of the contributing individuals were lacking in terms of technical knowledge. This notwithstanding, the impacts of both Anonymous and Hacker-Gaza were noticeable and far-reaching, and the groups were capable of mobilising tens of thousands, at least in the case of Anonymous, from all over the world, without necessitating more than the ability to mouse-click.

Moreover, as will be discussed in relation to the case of Cypherpunks, such groups usually do not align with any particular (traditional, or hard) ideology, and can be

---

<sup>6</sup> Cracking a software refers to bypassing or removing the protection measures companies install into the software for copyright purposes, rendering the software available for free use by the users.

<sup>7</sup> Script kiddies is a derogatory term used to describe computer users who pretend to be hackers without having the necessary knowledge and skills of a computer or network hacker. They are capable, however, of using software tools which hackers developed, and by doing so they can exert serious harms on targets.

seen to be ideologically malleable, as it were. This is clear in the case of Anonymous. In the case of Hacker-Gaza, despite being a small group and limited in terms of resources and geography, they possessed, as Skare (2018) notes, an ideology which mixed elements of Qawmiyya (Arab nationalism), Wataniyya (Palestinian nationalism) and Islamism in a particular way, while deploring other Palestinian parties and movements (some of which can be close to them ideologically). An important point as to the latter case is that Hacker-Gaza do not see themselves acting in a distinct and digital mode of resistance (as some other movements would, especially in the United States and Central and Western Europe). Rather, they conceive of themselves as acting within a broad condition of resistance, merely using the tools and affordances of the digital era.

Furthermore, the tension between individual and collective action, which will be seen in the Cypherpunk case, and the interconnectedness between the two forms of action adds to the complexity of resistance in the digital era. One could argue that, despite being present throughout history, this particular inter-connectedness (and interdependence, as some scholars would argue) intensified in the digital era.

Aside from the restrictions and the domination of the surveillance assemblages, the digital era provides the conditions of possibility for every-day, individual actions; whether visible or hidden. Digital media algorithms allow the enactment of ‘small acts of engagement’ through mundane acts, such as commenting on social media or reposting, which needs little investment and intention, yet allow for an expression of agency by individuals (Kapsch, 2022).

Additionally, the digital era provides groups with more opportunities to resist in situations where organised collective action cannot be taken. For instance, Chinese delivery drivers try to resist exploitation of delivery digital platforms and their algorithms by developing complex systems of resistance including both individual and collective tactics for solidarity and resistance (Yu et al., 2022). Moreover, the different modes of resistance can instigate and evolve into one another (Baaz et al, 2023; Lilja et al, 2017, Lilja, 2020). The interaction between the three different modes of hacking identified by Coleman & Golub (2008) is one example of how

different approaches to resistance instigate one another and how one form evolves out of another.

For example, the Free/Open Source movement, for example, and the hacker underground (specifically here) enacted different approaches to resistance against software monopoly, constructive and disruptive modes respectively. Yet, both shared elements and impacted the development of one another (as well as impacting Software companies, which later tried to adopt the free software ethos, and governments which funded the development of such projects, like the important TOR project). The Pirate Bay and the Pirate Party, in Sweden, is an interesting case of such overlapping of the two different modes of action against monopoly and copyright manipulation; by the same individuals at the same time.

In addition, social media campaigns can be seen as attempts to organise collective actions through the affordances these platforms provide. Feminists in Latin America sought to achieve visibility, which is a significant challenge for non-commercial social movements, through two configurations: platform vernaculars and algorithmic resistance. Individual activists collaborated by first adopting the vernaculars of social media platforms to reach a wider audience, and later the activist, through algorithmic resistance, organised the actions of users to challenge the quantitative, commercial visibility regime. Additionally, collective action can be organised through these digital affordances. The Egyptian and Tunisian cases in 2011 are exemplary cases. Alternatively, the natives of Australia, for example, collectively and strategically were able to disrupt the 'colonial algorithm', established by mainstream media for centuries, and instated their narrative, wrestling discursive power with noticeable effectiveness (Fredericks et al., 2022). As another example, and in spite of not being strategic or organised, migrant construction workers in Singapore managed to make their precarities visible through short videos on TikTok (Kuar-Gill, 2023).

Resistance in the digital age takes place as a combination of various digital and conventional modes, tactics, and discursive and ideological positions, and it also draws upon its historical precedents, as could be seen from the various existing cases. Moreover, the relationship between individual-based and collective acts of

resistance is a central issue, and the tension within it is arguably intensified in the digital context. In addition to these issues, other issues are pertinent to the question of resistance, which intensified with the advent of the digital era and in relation to the pervasiveness of the information and surveillance economy. Such issues include those about the intentionality, visibility and volition of resistance.

These issues are essential to understand resistance as it exists in the digital era, and how it evolved with the evolution of the latter. As mentioned earlier in examples, and especially in relation to the pervasiveness of surveillance, visibility of resistance (or lack of visibility) is a central concern for users and activists; either by trying to stay hidden to avoid moderation on social media (e.g. Moran et al, 2022) or to avert sacrifices and prosecution (e.g. Magalhaes, 2022; akin to more conventional hidden everyday resistance) or by trying to achieve maximum visibility, as in the case of Palestinian social media activists or the above mentioned Latin American feminists.

Moreover, and at a different level, the issues of historical context and economic development are critical factors that must be analysed. As will be seen in the case of the Cypherpunks, the evolution of the group and its mode of action was tightly related to the context of American liberalism and the emergence of the Californian ideology. This can be seen more clearly in comparison with other contexts like that of the Soviet Union. For example, the opposing attitudes towards cybernetics, until the mid-1950s, directly impacted the development of computer technologies in both countries (Gerovitch, 2002), and one can make the argument that this can partly explain the emergence of different digital (resistance) cultures.

Furthermore, their ideas and demands were the result of their immediate reality. For example, while the Cypherpunks, and the digerati were generally utopian, individualistic and elitist, their ‘counterparts’ in the Southern European hacking scene were integrated in grassroots social movements, and unlike the Cypherpunks, they were not highly visible (Maxigas, 2017). In the latter case, hackers did not face strong response by the state, and thus did not resort to the underground or assimilate into the mainstream spaces of action (Maxigas, 2017). On the other hand, those in the United States were oppressed on a number of occasions with severe legal

consequences. Additionally, Western European hacking circles emerged at the same time as that of the United States. Furthermore, and in contrast, the disparity in economic development, as well as the cultural and historical contexts of the global south provided the conditions of possibility for a different course of evolution of resistance in the digital era and resulted in the enactment of different conceptions, modes, tactics, and objectives of resistance in the digital era (Pereira et al., 2022; Nashif, 2017).

A group of researchers called the Resistance Research Group (RESIST) (Baaz et al, 2023; Lilja et al, 2017, Lilja, 2020) propose a synthetic new approach to study resistance. This framework is supposed to be a tentative guide for an analysis of resistance that is comprehensive in terms of accounting for the different forms of resistance that take place in a particular case, which earlier scholarship has overlooked due to their focus on different aspects of the phenomenon. The scholarship on resistance has primarily focused on either one of two aspects: everyday resistance or organised resistance. Everyday resistance research focuses on individual and primarily hidden acts of resistance, while organised resistance research focuses on social movements mobilisation and open, collective resistance. According to this group of scholars, both can be viewed as subfields within Resistance Studies, and each alone is not sufficient for a proper grasp of resistance not for accounting for the inter-connectedness and interaction between the different forms and acts of resistance.

Moreover, they emphasise the fact that not only power relations impact the enacting of resistance, but also other contextual elements, such as the prevalent knowledge regimes in a particular case of resistance. Furthermore, resistance is not necessarily oppositional, and resistance can create power as much as power creates resistance or reinforce power relations.

The authors provide a number of examples to demonstrate these points. As to the latter proposition, they mention the example of ‘counter hegemonic bloc’ introduced by Antonio Gramsci, whereby hegemonic power relations are opposed by creating new forms power that seek to address exploitation, or in a different way when

anarchist or feminist radical groups create informal elites with less visible power while attempting to oppose formal hierarchies.

In relation to the digital era this can be seen in many examples from the sphere of social media activism, where particular individuals assume (partly thanks to the media algorithms themselves) leadership roles and seek to instate particular power relations, to hacktivism where some hackers are deemed to be elites and representative of hacker culture. This was seen in the case of the Cypherpunks, not only through their documents but also through the changes they adopted in response to reaction by the state. For example, while Anonymous enjoys much recognition in the media and more concern by states, other groups like the Italian Autistici Inventati or +KAOS are barely known in comparison to Anonymous, despite building alternative (and perhaps rather more effective) digital infrastructures (like data and internet infrastructures) which proved effective in resisting oppression and surveillance and which Anonymous itself used in some of its largest operations.

While research that focuses on infrapolitics (or everyday resistance) focuses on individual, hidden and dispersed acts of resistance, it overlooks other instances of resistance. For example, there are individual instances that are not hidden and are rather highly visible, like self-emolition. Other everyday acts of resistance do not seek to merely avoid oppression but also seek to challenge power and are contentious in nature. In relation to the digital era, while many people resort to disengagement as a mode of resistance against surveillance (a choice that is individual and hidden), the revelations by Edward Snowden in 2013 were individual acts, yet they were not hidden, seeking maximum visibility with impacts that no collective action could have achieved. These were pivotal points that reshaped our perception of power relations in the context of surveillance and data politics. Yet, despite the significance of such cases, collective approaches to resistance do not give sufficient attention to these modes and forms of resistance.

Moreover, whistleblowing as a resistance tactic (which is central to the strategy of the Cypherpunks) has led to other forms of resistance, by journalists, academics and civil activists, to reconstruct the discourse about surveillance, encryption and internet

freedom and privacy. In addition, it had resulted in a number of initiatives that adopted a more constructive mode resistance resulting in a number of technological tools to avoid surveillance and disrupt the algorithms of power, like the open-source software InformaCam which provides users with the ability to control meta-data attached to their visual contents before sharing them, thus obstructing surveillance and data mining attempts through these footages.

The authors of this research group provide an alternative categorisation as the basis for a more comprehensive approach that is capable of capturing and grasping the different instances and tactics of resistance and their intricacies. They propose a tentative framework with three categorisations: (1) Avoidance Resistance, (2) Breaking Resistance, and (3) Constructive resistance. While some of these are more relevant to counter-surveillance than others; they are all present in the quest to counter-surveillance; as will be seen in the case study and the other examples mentioned.

*Avoidance Resistance* by its name avoids power relations and oppression by disguise and hiding from detection. This quest to be under the radar is shared with ‘everyday resistance’. However, unlike the category of everyday resistance, ‘avoidance resistance’ does not need to be informal, individual or taking place on a daily basis, rather it can be organised and collective. They bring the example of Maroon communities of runaway slaves, who created communities in jungles or mountains. In the digital era, they use the example of using P2P (peer to peer) technology to share files on the internet, to avoid copyright regimes and detection by legal authorities. This avoidance is enacted by millions of people all over the world, and in some contexts, organised and lobbied for. Moreover, this kind of resistance can be seen among communities who refuse to use digital media or among groups active on the Deep Web, for various purposes and reasons.

*Breaking resistance* operates with a different logic. It seeks to directly and publicly challenge power relations, as a form of ‘contentious politics’. While it can be in the form of collective and organised social movements, as in the case of the Cypherpunks or the Electronic Frontier Foundation, it can also be individual and

informal, as in the many cases of whistleblowing or hacking. Finally, *constructive resistance* primarily rests on the assumption that resistance is not only about opposition and disobedience. Ettliger (2018) as was discussed proposes 'proactive resistance' as a broad category of resistance in the algorithmic era, and traces its various modes and tactics. Nevertheless, she conceives of productive resistance as essentially oppositional and frames its tactics in terms of 'antagonism of strategy', relationally with power relations, and which targets various nodes of power.

In constructive resistance, on the other hand, resistance need not be oppositional to a particular form of power, and it undermines power by instating alternative models and lifestyles that do not necessarily seek to break or avoid power. In this case of resistance, the authors highlight that this kind of resistance can take place easily in the digital era. For example, within a particular historical conjuncture, the involvement of thousands of developers and computer tech-savvy individuals created alternatives that made it possible to run a computer with totally free and open software, and social movements can easily produce their own versions of such software at will, with even states contributing to these endeavours as a result of the impact of this movement.

Resistance and attempts to counter-surveillance are complex, including the various forms of resistance mentioned above, all at once. They can be against different targets within the 'information regime', as well as blur the borders between individual and collective action-- as can be seen from various examples. Furthermore, we can see such insights about resistance in relation to surveillance. Firstly, the application of surveillance tools, methods and systems incites resistance and attempts to counter this system. This can be against surveillance itself or against the tools perceived as enabling surveillance, like big data or platform algorithms. Moreover, digital applications meant for surveillance have actually enabled not only counter-surveillance initiatives and movements, like social media platforms, but also helped some resistance actions, which have actually toppled down oppressive regimes.

An example might help illustrate these points. The case of Tunisia is exemplary in relation to this issue. The pre-2011 Tunisian state was an example par excellence for

a police state which developed a solid and comprehensive surveillance apparatus. Beside the institutional surveillance, done by internal intelligence and policing agencies (with one security deputy for every 60 citizens, between 1998 and 2004), and beside informants (mainly partisans of the ruling party), the Ben-Ali regime developed new methods for surveillance. What was called ‘vigilantism/watchfulness committees’ (Lejan al-Yaqadha), which was formed by the various branches of the ruling party and its youth, was turning in daily reports to both the party’s leadership and from there directly to the presidential cabinet. In addition, in 1997 a presidential decree innovated a new informal vocation called the ‘surveillant/vigilante citizen’ (al-Muwaten al-Raqeeb). The stated objective of this new vocation was to facilitate citizens to deliver their grievances to the highest authorities, through this ‘vigilante citizen,’ but, in reality, worked as a surveillance informal institution and represented the omnipresent power of the state. In addition, surveillance over intellectual activities was comprehensive insomuch as that higher education institutions were to report to the Ministry of the Interior about any academic events with lists of participants and the texts of their participations (Khabash, 2012; Tunisian labour communist party, 2005).

Tunisia was one of the first Arab countries to spread the use of the internet, starting from 1997 with a presidential decree, accompanied with campaigns reaching even small or neglected cities teaching how to use the internet, and reducing the subscription fees for the internet. This was partly to serve the image of the regime as a modern state, and partly as a ‘circus and bread’ scheme (through the virtuality of the internet). Soon, however, the regime started a process of extreme surveillance and control over the internet, with advanced surveillance tools. Internet Cafes were legally responsible for reporting user’s visiting of censored or banned websites; the users had to show I.D. cards and record the visiting dates. Later in 2009, internet cafes had to install ‘Publisoft’ software which recorded users’ surfing activity in detail. The ‘Internet police’ even conducted ‘phishing’ attacks to surveil Tunisian Facebook users (ibid).

Nevertheless, despite other factors the internet (including international assistance by hacktivists) was a primary reason for toppling down a regime, the destruction of

which went against all the indicators. Aside from the use of the internet during the Tunisian Revolution, it had a history which starts with the introduction of the internet in the Tunisian society. Lecomte (2011) identifies 3 periods of the development of the internet as a tool of resistance in the Tunisian context; which correspond to 3 generations of ‘cyber-dissidence’. The era from the end of 1990s until mid-2000s witnessed the first generation of cyber dissidents, who were generally isolated from the public, and who, however, were the pioneers and led the evolution of cyberactivism. From mid-2000s, the Tunisian blogosphere started to grow, with users being individuals and yet linked together, with a tension between the different generations on crossing the political red lines, leading to what is called cyberbalkanization, where the Tunisian cyberspace was made of separate differing spheres. Evading discussions of what is political. However, soon debates broadened (even indirectly), in response to arbitrary censorship by the cyberpolice, and the new measures taken (see also, Khabash 2012). The third period, a few years before the revolution of 2011, coincides with the popularity of social media platforms. By January 2011, the number of Tunisian users of Facebook reached approximately 1 million 800 thousand users—indicative figures; forming the third generation, which allowed for further de-compartmentalisation of online criticism, down to the revolution. The internet, in addition, allowed for the communication between Tunisian activists and international Hacktivists, including Anonymous and Arab hacking groups, which significantly led to the downfall of the Ben Ali regime. In this example, we can see the various elements of breaking and constructive resistance, in addition to the accompaniment of individual and collective actions, beyond territorial borders (either by expatriates or international sympathizers).

Another example, which relates more closely to the information regime, and which traditionally, at the purview of intelligence services and state institutions, is open-source intelligence (OSINT)—that is, the collection of intelligence on the basis of publicly available information, and the processing of such information, for intelligence ends. It uses surveillance technologies for counter-forensics, such as breaking or constructive resistance. The rapid growth of big data along with the plethora of digital tools and algorithmic advancements allowed for OSINT to become a significant phenomenon in the ‘digital age’. While as a tradition OSINT

existed at least since mid-19th century in the United States, (and even some intelligence historians would say it can be traced back to 16th century Italy) within states' institutions (Block, 2024), the number of actors collecting, analysing, and using OSINT tools (to variant degrees of effect), as well as the number of purported claims as to the reasons of employing OSINT has surged dramatically in the age of Big Data and advanced algorithms. These actors include state agencies, NGOs, activist groups, as well as individuals, with a variety of intentions that may be emancipatory or reactionary (and different patrons lying behind the scene). In addition, of importance here is the scale and the reachability. As such, OSINT involves a number of differing, contesting actors, as well as constituting a space with abundance of 'grey areas' and blind spots; despite the 'open' in it.

In many cases where OSINT investigations constituted instances of resistance, either by individuals or organisations. For example, when the Israeli Mossad, on its X account, attempted to claim that the massacre in the Al-Ahli hospital of Gaza was caused by a failed missile launched by the Palestinian Islamic Jihad, it published a video as evidence to support its 'thorough analysis' of the incident. Shortly after, however, individuals, using OSINT tools, traced back the video, thought hard to find online, to an incident which happened more than two years ago. In the same context, 'Forensic Architecture', using OSINT, Data Mining, and other data-related methodologies, investigates the deliberate destruction of the medical infrastructure in Gaza by Israel (Forensic Architecture, 2023a). Moreover, such investigations go beyond mere documentation and publication to intervene and affect legal procedures, such as in the case of the ICJ case South Africa vs. Israel, where 'Forensic Architecture' scrutinised, and exposed the misrepresentation of, evidence provided before the court by the Israeli legal teams, using OSINT as one methodology (Forensic Architecture, 2024). Numerous similar cases, in other contexts, exist, involving various actors.<sup>8</sup> Moreover, in some cases they can also be in direct opposition to Tech companies and their data surveillance regimes (Forensic Architecture, 2021, 2020b).

---

<sup>8</sup> For a variety of examples, see Forensis, 2023, 2024; Forensic Architecture, 2017, 2022, 2023b, 2020a; Gonzales, 2024.

Furthermore, OSINT can be an oppositional response, a resistance mode against the data regime, and in particular the data episteme. Its collective projects can be a mode of productive resistance, which includes different elements from other modes, like ‘civic hacktivism’ and ‘platform cooperatives’ (as described by Ettliger, 2018). It can indeed be a form of ‘counter-forensics’ (van der Velden, 2018). In addition, using OSINT to extract data and then rendering it visible in a variety of ways (notable among them are interactive visual platforms), it can be an act of ‘artivism’ (Suárez Val et al., 2023), and it can disrupt and obfuscate the logic of ‘data colonialism,’ which naturalises the exploitation of people through data (Couldry & Mejias, 2019). It constitutes a response, and opposition to the ‘colonial algorithms’, a form of wrestling back discursive power and the potential of opening new alternatives and possibilities for theory and praxis, using the same data regimes and technologies. It is an attempt to reach an ‘equality of arms’, in the words of the lead developer of InformaCam (van der Velden, 2015).

Nevertheless, conducting OSINT requires resources and technical knowledge. Moreover, States, corporations, groups and individuals are all involved in OSINT, making use of big data and algorithms, with different intentions and on the basis of different assumptions. As such, OSINT can be reactionary as well as emancipatory, a positive endeavour as well as an endeavour with detrimental consequences. It can oppose the ‘colonial algorithm’ and alter power relations, or it can reinforce them. Furthermore, even when the claim is to empower the public or the oppressed, there are issues as to what entities fund a particular project, what alliances a particular organisation has, and, perhaps more importantly, what rationales form the basis of an OSINT investigative organisation; among others similar issues. Arises also the question as to the character of actors involved in OSINT and where do they lie on the power relations network. Hence, OSINT is an arena of grey areas and blind spots; and it is so in a stark way, reflecting the complexities of resistance, particularly in the digital era, and in its relation to power relations. One can also argue that it is also an arena reflective of the contemporary power asymmetries; and that it might be devoid of any genuine potential for effective resistance.

In conclusion, resistance in the digital era is a complex phenomenon, involving a mesh of forms, tactics, and strategies. Under the information regime, instances and

movements of countering surveillance include forms of avoidance, breaking, and constructive resistance, and blur the separating borders between traditional lines separating between, for instance, individual and collective acts. This is a necessary starting point in studying technologist counter-surveillance, drawing from insights in recent Resistance Studies, in relation to Surveillance Studies. These insights will be clear in the case study of this thesis-- that is, cryptography-based technologist counter-surveillance.

The examples above as well as the different cases and examples, and types/tactics/strategies found in the literature, hint at two issues. The first is the dilemma of technology as a restrictive as well as an emancipatory tool. The second, which is the concern of this thesis, and which is inherently entangled with the first issue, is the dilemma of countering surveillance in the information age. To understand this dilemma we need to understand the kind of regime within which this dilemma takes place. Here, we make use of the theoretical insights from the works of philosopher Byung-Chul Han.

## **2.5. Conclusion**

The contemporary times are characterised by the prevalence of Big Data and Advanced Algorithms—impacting and shaping all aspects of life, in the present as well as in the future, from economics to public administration, and from human behaviour (individually and collectively) to the production of knowledge. The history of technology has shown celebration and scepticism accompanying every technological development. These technologies are technologies of surveillance. There arise questions about the relationship between surveillance and control, as well as questions about counter-surveillance in this era. This chapter sought to discuss these issues, before moving on to study the characteristics and dynamic of the contemporary surveillance regime—in the following chapter.

A principal premise for this thesis is that surveillance is the primary apparatus of control and domination in the era of the information regime. Historically, surveillance has an intimate relationship with control as domination. Surveillance is

not the mere act of seeing or watching. Surveillance in essence pertains to the implicit laws and covenants which unifies the social and which ensures compliance with this social framework (Zayid, 2013, 14). Furthermore, surveillance is the central apparatus of control in the era of Big Data and advanced algorithms, that is the information regime.

Moreover, with surveillance being the central apparatus of domination and control, it becomes no surprise that different forms of and approaches to counter-surveillance arise. Counter-surveillance is a complex phenomenon, involving a mesh of forms, tactics, and strategies. Under the information regime, instances and movements of countering surveillance include forms of avoidance, breaking, and constructive resistance, and blur the separating borders between traditional lines separating between, for instance, individual and collective acts.

This complexity and the variety of form, tactics and strategies of counter surveillance, hint at two issues; first: the dilemma of technology as a restrictive as well as an emancipatory tool. The second, which is the concern of this thesis, and which is inherently entangled with the first issue, is the dilemma of countering surveillance in the information age. To understand this dilemma we need to understand the kind of regime within which this dilemma takes place. This regime marks a special transition in history possessing distinct features with implications for counter-surveillance, and for resistance in general. This is the subject matter of the next chapter.

## CHAPTER 3

### THE SURVEILLANCE REGIME AND PSYCHOPOLITICS

#### 3.1. Psychopolitics

##### 3.1.1. The crisis of Freedom

Han starts with an observation of a crisis—the crisis of freedom. In the information regime, freedom is exploited for economic gains. He states that: “We are living in a singular phase of history when freedom itself entails pressure and coercion. In actual fact, freedom represents the antitype of compulsion—period. And yet this same antitype is now bringing forth compulsion and constraint. More freedom amounts to more pressure. As such, it marks the end of freedom.” (2017b, 48-9). He is concerned with a paradox where, under the neoliberal regime, freedom has become an instrument of domination. Freedom produces coercion.

Freedom here is proved to be an interlude—a phase that is sensed during the transition from one way of living to another. The subject residing under this kind of domination deems itself free, feeling freedom, with forms of liberty (including play, emotions and communication) are exploited. In reality, the subject is a slave. Moreover, and more importantly, the subject is an active participant in this subjugation directed against him/her. The subject is at once both the subject and object of exploitation, serving the capitalist interests (Han, 2017a). Informed by the Gramscian distinction between hegemony and domination, Han states that “[t]oday, exploitation is possible without any domination at all.” (2017b, 13).

It is a condition where allo-exploitation (that is exploitation by an Other) yields to auto-exploitation (self-exploitation), and in which freedom is in such a crisis. This

condition is rooted in a foundational social transition. It is a transition representing a mutation, and intensification of capitalism. Under neoliberalism the mode of government is psychopolitics. Instead of controlling through direct oppression, restriction, and inhibition, psychopolitics controls by seizing the psyche and emotions on a pre-reflexive level, to influence action and behaviour (Han, 2017a). This foundational transformation, proposed by Han, results in a society of control, operating in accordance with the imperatives of psychopolitics.

An example of psychopolitics in operation is micro-targeting. Micro-targeting works via personalising messages, on the basis of data collected on the behaviour of an individual. The political message or commercial advertisement no longer targets a population with a variety of personalities, ideational positions and desires. They are tailored to influence the particular individual receiving it. In fact, the kind of content he or she repeatedly encounters is altered to the end of behaviour control. Cambridge Analytica is a well-known case in regard to political influence. Another example, in the field of e-commerce, is Amazon's recommendation algorithms. Amazon's recommendation algorithms, through the collection of large amounts of behavioural data, influence the behaviour of individual customers with its "item-to-item collaborative filtering". In a larger scope, Google's PageRank algorithm imposes a hierarchy of visibility, determining what could and what could not be seen in the search results—possessing the potential to shape political and social priorities (Musiani, 2013).

### **3.1.2. The Transition To Psychopolitics**

Neoliberal psychopolitics of the control society is a mutation from the biopolitics of the disciplinary society that was the form of domination in the era of industrial capitalism. Michel Foucault (1978) observed a transformation starting from the seventeenth century. This concerns a transition in the mechanisms of power—from sovereign power to disciplinary power. Since ancient times the 'sovereign' was able to control and dominate through the 'sword', which was emblematic of the 'power of life and death'—that is the power to 'take' life and 'let' live. The sovereign was the possessor of the privilege, albeit not necessarily in absolute, arbitrary terms, to kill or

refrain from killing. This form of power operated by means of deduction and seizure, that is by means of appropriation of wealth, bodies, time, and ultimately life.

Here punishment assumes a theatrical presence; it becomes a spectacle that has as its object the flesh, the corporeal body of the convicted. Punishment becomes a ceremony with spectators gathered in public arenas and squares, to watch the process of torture and execution (Foucault, 1977). Later, however, the body becomes an intermediary, an instrument. The physical pain of the body is no longer the punishment itself. “The body, according to this penalty, is caught up in a system of constraints and privations, obligations and prohibitions” (ibid., 11). Starting from the late 18th century, the theatricality of pain was excluded from the punishment and the spectacle was gradually disappearing (ibid.).

This transformation was rooted in the transformation in the form of power—the transformation into disciplinary power. Disciplinary power was in essence more subtle and precise in contrast to the coarseness of sovereign power. According to Foucault (1978), starting from the classical age, ‘deduction’ as a ‘technology of power’ was becoming merely one form of power, to be used when necessary. Biopower, of the disciplinary society, sought to administer life, rather than to subtract it; it sought to “invest” life. It gradually started to concern itself with ensuring, maintaining and developing life. Power assigned itself the task of administering life. This pertains to the life of both bodies and races, of the individual as well as the species. Once this became the function of power, the death penalty was increasingly difficult to enact. “One might say that the ancient right to take life or let live was replaced by a power to foster life or disallow it to the point of death.” (138).

This power over life evolved in two forms: the anatomo-politics of the human body (or disciplines of the body) and the biopolitics of population (or regulations of the population). Both forms constitute two poles on the spectrum of ‘biopower’, administering life. Biopower is both, at once, an individualising and totalising form of power.

The anatomo-politics of the body, targets the body envisaged as a machine—to discipline it, to optimise it, to improve its performance and enable its integration into

‘efficient’ control systems. ‘Disciplines’ ensure the production of the ‘docile body’. The body is to be made useful and utilisable in order to serve the interests of industrial capitalism. Disciplines mean to render the process of control more efficient and economic. These disciplines were deployed in a variety of milieus and environments, including educational institutions, the prison, the factory, and the clinic. The subject, here, is akin to a stock of organic resources (Stoneman, 2024).

The second form of power concerns itself with the ‘race’, the population at large. It operates at the level of the body of the ‘species.’ This body serves as the basis of the biological processes of birth, life-expectancy, health and death, and impacting conditions governing such processes. This is a power of intervention and regulation. Biopolitics of the population concerns problems including migration, birth rates, and housing. A significant consequence of this form of power pertains to the ‘norms’, the ‘normal’. As such, it seeks to control and affect distributions around the norm; rather than drawing lines between obedient subjects and enemies of the sovereign. It seeks to control society by ‘normalising’ it, by “investing the body, health, modes of subsistence and habitation, living conditions, the whole space of existence.” (Foucault, 1978, 143-4)

These two forms of power are based on calculation for the management of life—for the subjugation of individual and social bodies. In fact, according to Foucault (1978), speaking of biopower amounts to speaking of the forces that rendered life and its dynamics within the realm of explicit calculation. At the time, statistics was the mode of calculation for biopower. It enabled the capturing of population in a manner that enabled such administering of life and control of the population, around a norm—as opposed to the outsider, the singular, the abnormal. Worth mentioning for later discussion is the issue of ideology. Ideology played a role of coordination, as an abstract discourse coordinating these two technologies of power—the anatomo-politics of the human body and the biopolitics of population—to be joined together at the level of concrete arrangement. Hence, rather than being simply a speculative discourse effective in thought, it—that is, in operation, as a mechanism of control, rather than in thought.

Biopower was a necessary mutation for the development of capitalism. Foucault states that “[capitalism] would not have been possible without the controlled insertion of bodies into the machinery of production and the adjustment of the phenomena of population to economic processes.” (1978 141). As techniques of power, biopower serves to preserve the effects of hegemony and the relations of domination.

Later, in the early 1980s Foucault started to focus on “the history of how an individual acts upon himself” (Foucault, 1988,19; in Han, 2017a, 27)—that is ‘technologies of the self’, as different from ‘technologies of power’ discussed earlier. In other words, technologies of the self (or ‘arts of existence’) refer to the efforts individuals make in order to change their approach to life and set themselves codes and rules of conduct. They refer to the techniques individuals deploy to transform themselves in accordance with certain values and criteria. Important aspects of these techniques, as identified by Foucault (1985), are the intentionality and voluntariness present in their employment by the individual. Nonetheless, this is not to suggest that technologies of the self are separate from, or immune to technologies of power. These ‘arts of existence’ have lost part of their autonomy through the influence of religious power and later other types of doctrines, including hegemonic educative, medical and psychological practices. Disciplines and norms impact on how the subject seeks to act upon itself.

Han sees a further transition, a further mutation in capitalism, in which the mode of control is no longer in line with the biopolitics of the disciplinary society, but rather in line with the psychopolitics of control society. The disciplinary society yields to the control society. The form of power transforms from biopower to psychopower—from biopolitics to psychopolitics.

The main criticism Han brings against Foucault is that the latter has not seen the change in the relationship between technologies of the Self, on the one hand, and technologies of power, on the other. Han states that the blind spot in the analysis of Foucault is that he “did not see that *the neoliberal regime utterly claims the technology of the self for its own purposes: perpetual self- optimization*” (2017a, 28,

italicised in the original). In other words, under neoliberalism we only have technologies of power, in the sense that what constituted the technologies of the self in the liberal disciplinary society of biopolitics has become assumed under, and incorporated in, the technologies of power. The neoliberal regime renders the technologies of self into technologies of power.

The ‘intentional and voluntary’ efforts of the individual to transform him- or herself are being invested, impacted and captured by the neoliberal regime for its purposes. The ‘arts of existence’, that is the technologies of the self, are heavily influenced by the various control mechanisms of the neoliberal regime, along the line of psychopolitics, on a pre-reflexive, unconscious level. As such, the individual exploits itself, that is, it ‘modulates’ itself and shapes its art of existence, not so much intentionally and voluntarily, but rather out of a market compulsion which invades all aspects of his or her life. It is a market compulsion, that merges the realm of play with the realm of work, rendering all aspects of one’s life exploitable. The subject, through perpetual self-optimisation, becomes a project rather than a subject. The liberal subject is more of a project, an achievement subject. Han agrees with Foucault about the efficiency of power—that power is always in the quest to increase its efficiency (Wyllie, 2024).

### **3.1.3. Psychopolitics**

Before going into how the psychopolitical regime operates, and how it impacts collective action (especially against surveillance) it is imperative to look into what characterises this regime, and the control society it brings to being. Han here builds on, and goes beyond Gilles Deleuze’s discussion of the control society (as different from the disciplinary society), in the latter’s short article “Postscript on the Societies of Control” (Deleuze, 1992).

Deleuze identifies a crisis of the institutions, by which he means the introduction of a progressive and dispersed novel regime of domination. For this new regime he uses the name ‘societies of control’. This society of control evolved from the society of disciplines—that is, from capitalism of concentration. The disciplinary society is

characterized by institutions, that is by discrete, discontinuous enclosures. The exemplary model is the factory. All institutions, including the family, the school, and indeed the prison, despite being discrete, work ‘analogically’, as variations of the factory. Institutions represent disciplinary enclosures. Enclosures are ‘molds.’ They cast into a mold, to capture the subject, who is always starting again as (s)he moves from one institutional enclosure to another—from the family to the school, then to the army or the factory, for the purposes of efficient control.

In the societies of control, on the other hand, unlike disciplines, controls are a ‘modulation’. The mold, the cast, is ever self-deforming, continuously in change and re-molding. Instead of schools, we have perpetual training. Instead of factories we have corporations, which divides individuals within, opposing them against one another, rather than molding them as a single body. Control is continuous and limitless, it is of short-term and rapid rates of change. Disciplines, however, are of long temporality, they are infinite, discrete and discontinuous. “The family, the school, the army, the factory are no longer the distinct analogical spaces that converge towards an owner-state or private power-but deformable and transformable-of coded figures- a single corporation that now has only stockholders.” (6)

Capitalism in the present time is one of high-order production—rather than production, which is often sent for the Third World to accomplish. It is a capitalism not of production but of products, that is, it seeks to buy the finished products and wants to sell services and buy stocks. Money, in the societies of control no longer referred back to the gold standard, like the case in the society of disciplines, but rather relates to floating, fluctuating rates of change. This crisis of milieus of confinement, this closedness and rigidity, and the continuous calls for reform, arise out from the fact that the older formations of control are no longer suitable for the immaterial, networked, post-industrial mode of production in the information age. The limitations need to be overcome for more capital production.

Deleuze uses the simile of a mole now becoming a serpent. The animal of the disciplinary society is the mole—that of neoliberalism is the serpent, the snake. The

mole digs a discrete network of burrows. The snake on the other hand, “makes space by means of its own movement.” (Han, 2017a,18). It represents a new form of movement—it is not confined spatially or temporally to the network of the burrows, but rather, it develops novel forms of movements, to bypass the limitations for productivity presented by the earlier regime. The mole, according to Han’s (ibid.), extending the metaphor, represents the labourer, the subjugated subject, which has always to move from one milieu of confinement to another. The transformation of the individual from a mole to a snake, represents its transformation from a subject under the liberal, biopolitical disciplinary society, into an entrepreneur, into a project under the neoliberal, psychopolitical regime of control. This subject is an “amorphous, shapeless, and flexible, an adaptive and self-starting entrepreneur” (Wyllie, 2024, 18).

The biopolitical concerns itself with bodies. The ‘body’ of the individual as well as that of the ‘race’, the population, is the target of disciplines. The psychopolitical, in contrast, concerns itself with the psychological, it penetrates the psyche in order to control the subject, now the entrepreneur, on the pre-reflexive, unconscious level. An example of platform workers, in the case of Uber, illuminates this situation. In this case, as Salter and Dutta (2023) show, there exists a paradox concerning knowledge and practice. Despite existing and felt exploitation, the platform business model and algorithms enables an ideological fantasy of the rule-breaking entrepreneur. This way the workers are caught in the web of this business model. Despite being conscious of exploitation, precarity and injustices, workers continue to work for the platform, rather than seeking a different alternative, driven by this ideological fantasy of the rule-breaking entrepreneur. This psychopolitical gamification of work is the reason for this situation in which workers adopt contradictory, irrational positions against their interest.

The significance of Han’s work derives primarily from his analysis of the dynamics of psychopolitical control and the elements present therein. When compared to the sovereignty regime, biopolitics exerts a positive influence on life (Foucault, 1978): it operates, nonetheless, through ‘negativity’—through restriction and inhibition. It is repressive. Psychopolitics, in contrast, is permissive, indeed inciting and

encouraging. It is here where the crisis of freedom lies. Psychopolitics operates within and brings about a society of ‘positivity.’

The liberation of the body does not negate exploitation, rather “our life projects include all kinds of affective, somatic, and visceral dimensions that are prone to exploitation” (Wyllie, 2024, 16). These represent other ways in which the body can be exploited, and which Foucault did not foresee. Han agrees with Foucault on the premise that power is constantly in the quest to achieve efficiency for domination (Wyllie, 2024). As such the objective of psychopolitics is to overcome the limitations present in the disciplinary society. This leads to the discussion of the nature and dynamics of the society of control working along the lines of psychopolitics. Prior to that, and essential to psychopolitics, is a discussion of the ‘machine,’ characterising this society of control.

According to Deleuze (1992), each type of society has associated with it certain types of machine as these machines express the social forms which generate and utilise them; this is an expressive relationship not a deterministic one. In the society of sovereignty, simple machines prevailed (such as levers, clocks). The disciplinary society was characterised by machines involving energy (such as the steam engine). In the societies of control a different type of machines emerge—computers (1992). Han also writes that despite the fact that the transition from subject to project has been in development before the advent of digital technology, digital media is now completing the process. “[I]n critical phases of its existence, the prevailing form of being or life pushes for modes of expression that attain completion only in a new medium” (2017b, 45).

In other words, psychopolitics is intertwined with digital technologies. Psychopolitics enables and is dependent on the digital paradigm. It draws on and entrenches the surveillance regime. Without the computer device and computer networks, the ability to penetrate into the psyche of the individual is impossible. Moreover, the utopianism of the early days of the digital age are simply illusions (ibid.). Instead of a force for emancipation, we have a new form of domination—the ‘information regime.’

Instead of having “raised ourselves up from a submissive, subjective position” (Flusser, 1997, 188; in Han, 2017b, 45) through what Flusser calls the ‘digital turn’, we are now subjugated in a wholly new form of domination—the information regime. The information regime (or rather, in different terminology, the surveillance regime) refers to a novel form of domination in which the decisive influence on the social, political and economic fields is exerted by information—that is, through the collection, storing, and processing of data and information (Han, 2022). What defines power here is not necessarily the owning of the means of production, as the case under the disciplinary regime, but rather the ownership of, and the capability to access and retain data and information. Data and information are the target of exploitation here, rather than bodies and energies (ibid.).

It is in this manner that the regime of psychopolitics is optimized and made to approach completeness and efficacy of control. Surveillance works along the lines of psychopolitics to predict, control, and influence behaviour. The information regime is intimately tied to information capitalism, which is the intensified development, mutation of capitalism under neoliberalism. Under the information regime, communication and control coincide to become one and the same (Han, 2017a). “Surveillance and control represent inherent features of digital communication” (Han, 2017b, 72). Under the information regime of big data and advanced algorithms, the Big Brother becomes a ‘friendly’ Big Brother (Han, 2017a). Information is not taken, rather it is voluntarily given by the eager self-exposing individual. In fact, everyone is both at once the big brother and a prisoner, a situation in which Bentham’s panopticon is efficient and complete (Han, 2017b).

#### **3.1.4. Emotionalism and Gamification**

Hans' analysis links up with Lyon’s concept of surveillance culture (Stoneman, 2024). Lyon (2017) observes the emergence of an unprecedented culture in relation to surveillance. He proposes the concept of ‘surveillance culture’ to capture it. While the word culture is in the singular, it refers to multifaceted and complex phenomena present in late-modernity, that is the digital modernity. There are two main aspects of it.

The first concerns the compliance with surveillance that is widely present in contemporary society. Surveillance is accepted as a given and resisting surveillance is rather limited to certain groups of people and confined to particular settings, while the majority of the population comply with surveillance as a given state of being without questioning it. He explains this through other factors: surveillance has become a familiar dynamic as it is normalised and domesticated; fear and uncertainty has become a prevalent sentiment especially in the post-9/11 world; and finally, through the integration of fun and seriousness, entertainment and serious life, which are increasingly becoming two aspects of the same thing. The second main aspect of the surveillance culture is the fact that generally the population is no longer a mere target or object of state or corporate surveillance. People have become active participants, as they not only engage with surveillance but also initiate it. These two aspects motivate the analysis of surveillance culture along with other concepts, including the ‘surveillance state’ and surveillance society.’

The components of the surveillance culture as proposed by Lyon are: (surveillance) social imaginaries, and surveillance practices. Social imaginaries refer to the commonplace norms, expectations and understandings about daily-life visibility. They emerge from engagement by people with surveillance but also from news and popular media. They provide the people with a sense of the dynamic of surveillance as well as a sense of how to engage with and evaluate surveillance. Surveillance practices refer to ‘responsive’ as well as ‘initiatory’ activities revolving around surveillance. Responsive activities relate to being surveiled, and include actions like using encryption tools or wearing particular clothes to limit camera surveillance, or purchasing goods and services using cash instead of bank cards. Initiatory actions on the other hand relate to modes of engagement with surveillance. Examples include surveiling others on social media platforms or installing a dash-cam or utilising health-related surveillance applications.

Lyon emphasises that the two components of the surveillance culture, while analytically distinct, are inseparable. “[surveillance social imaginaries] provide a capacity to act, to engage in, and to legitimate surveillance practices. In turn, surveillance practices help to carry surveillance imaginaries and to contribute to their

reproduction” (ibid., 829). Moreover, Lyon (2019) emphasises the significance of understanding the relationship between ‘surveillance capitalism’ and ‘surveillance culture’. According to him, “[t]he surveillance culture has an intimate and mutually-informing relationship with surveillance capitalism” (Lyon, 2019, 72). It is in such a relational context that people are conditioned to voluntarily hand out data and private information, non-coercively, as it were. It is a context in which “the dominant aspects of surveillance culture often play into surveillance capitalism, facilitating and normalising it ... [and in which] much of surveillance culture depends on and is nurtured by surveillance capitalism” (72). Surveillance capitalism enables the elements which enable many aspects of surveillance culture, much of which, in turn, reinforces surveillance capitalism.

The divergences between the two analyses of Han and Lyon of cultural surveillance include the position they take on surveillance and its outcome. Whereas the account of Lyon is neutralist regarding how it views surveillance (or at best ambivalent, see Fuchs, 2010), the account offered by Han is rather bleak. However, at the centre of Han's concerns are the two main issues Lyon identifies as the main aspects of the surveillance culture: the compliance of and the participation by the same objects of surveillance. Nonetheless, what distinguishes Han is that his analysis goes beyond mere cultural transformation to investigate a rather grander transformation of the prevailing domination system. Moreover, Han's account delves deeper into its dynamics, providing a synthetic repertoire of analytical tools, relevant to the issue of this thesis. This allows us to understand surveillance beyond the mere act of surveillance, either by the subjects or objects of surveillance. More importantly it allows us to understand the efficacy of counter-surveillance in the light of the characteristics and dynamics of this new form of control and in relation to it.

To begin with, Lyon (2017), as discussed above, proposes an explanation to the issue of the widespread compliance with surveillance through three concepts that relate to ‘emotions’—to reiterate, these are, familiarity, fear and fun. Han addresses a sudden boom in interest in emotion in recent humanities and social sciences as well as in popular discourse. In this context, human beings become creatures of sentiment instead of being creatures of merely reason and rational calculation. This sudden

boom, according to Han, erupts above everything else from an economic process—the emergence of ‘a new, immaterial mode of production’. It is in our times that “[e]motions have become a means of production” (Han, 2017a, 45). We face emerging in our times, what is called ‘emotional capitalism,’ in which “[t]he neoliberal regime deploys emotions as resources in order to bring about heightened productivity and achievement” (ibid., 45). Rationality is the medium of engagement in the disciplinary society. In the psychopolitical society of control, the limitations for production are overcome by ‘emotionality’; accompanied by an incited feeling for liberty (as to be free is defined, under this system, in terms of enabling and setting free emotions).

The purpose of disciplines in the disciplinary society was to ‘function’, to ‘produce’ and in such milieu emotions represent a disturbing force. The ‘docile body’ of the disciplinary society can be seen as an ‘unfeeling machine’—at least within the enclosures, the milieus of confinement. In contrast, in the control society of the information regime, emotions are elicited and hailed as the expression of liberated subjectivity—for the exploitation of this very ‘expressed,’ ‘communicated’ subjectivity.

This represents a shift in the temporality of the regime of control. While rationality is conceived in terms of objectivity, generality and steadiness, emotionality, on the other hand, is defined in terms of subjectivity, situatedness and volatility. As such emotionality represents the opposite of rationality. Rationality is nurtured in stable conditions, with duration, consistency and regularity, unlike emotions which prefer change and shifts in perception. Rationality is slow, contemplative, meanwhile emotions demand acceleration. It is in this context that the neoliberal economy pressures for the acceleration of communication and promotes the emotionalisation of the productive processes. It rests on instability to enhance productivity.

Emotions are nowadays more consumed than any other goods or services, and can be consumed on end. Emotions, thus, transcend value in relation to consumption. Under emotional capitalism new fields of consumption are ‘opened up’, which are novel and limitless. Emotions are ‘raw materials’ exploited for the purpose of corporate

optimisation. It is in this novel and immaterial mode of production, which banks on freedom and communicative interaction, that sociality, communication and subjectivity can be, and are, exploited. This should be seen, furthermore, after effacing the conceptual conflation between different responsive elements of the psyche.

Han observes a conceptual conflation existing in the provided accounts related to emotions. Han distinguishes between feelings on the one hand, and emotions and affects on the other. This is important in relation to how psychopolitics becomes able to penetrate the psyche beyond the body to exploit subjectivity on a pre-reflexive level for control. These distinctions mean different temporalities, intentionalities and different states of being—indeed different objectives.

Feelings are characterised by duration and lack intentionality. They are constative and lack an objective. On the other hand, emotions are short-lived and fleeting— affects are even limited to a single moment. While feelings represent a static state of being, emotions are on the other hand dynamic. Emotions, unlike feelings, are performative—directed towards action. “As inclinations, [emotions] represent the energetic- the sensory, or even sensuous-basis for action” (Han, 2017a, 47). Feelings, as such, cannot be exploited as they are static, enduring and lacking intentionality. Emotional capitalism exploits the dynamism and performativity of emotions. Affects are, however, eruptive, lacking performative directionality, nevertheless they constitute a significant part of digital communications, on the basis of their temporality and the expression of subjectivity.

Feelings, due to their stability and temporality, have narrative qualities (see below on the crisis of narrative). Feelings can be ‘re-counted;’ emotions and affects, in contrast, can only be ‘counted.’ Emotions cannot give an account. In the information regime of today, “the narrative theatre of feelings is yielding to a clamorous theatre of affects” (ibid., 42). Social media are exemplary in this regard (Andary&Auza, 2025; Wand&Pal, 2015; Ruensuk et al., 2020; Guo et al. 2019). To reiterate, as such, emotions are the sensory base of action, they “form the pre-reflexive, half-conscious, physico-instinctual level of action that escapes full awareness” (ibid., 48). Thus, in

this way, through exploiting emotions and affects, neoliberal psychopolitics is able to penetrate and modulate the psyche -beyond the docile body which biopolitics could not penetrate- in order to overcome the limitations present in the disciplinary society.

It is a technology of power—the coincidence of the technologies of power and the technologies of the self—exploited for control and optimisation of the production process. As a power, compared to biopolitics, “emotion affords a highly efficient medium for psychopolitically steering the integral person, the person as a whole” (Han, 2017a, 48).

This relates to the concept of ‘shock’. According to Naomi Klein, the shock is a means of control in the neoliberal age through which the psyche is wiped through shock to be re-conditioned again. Disaster traumatises and paralyses, rendering people ready to accept the imperatives of neoliberalism. Han (2017a) criticises Klein's theory of shock as a biopolitical measure of coercion, predating the neoliberal regime. Shock therapy is a disciplinary technique, which counts not as a psychopolitical technology of power, but rather as ‘psycho-disciplines’, orthopaedic in nature. It does not encourage, incite and is not positive in nature. It is negative, working through paralysing and annihilating the contents of the psyche.

Neoliberal psychopolitics, unlike psycho-disciplines however, work instead through positive stimuli. The ‘bitter medicine’, the shock, yields to the incitation of the ‘liking.’ Instead of paralysing the psyche and erasing its contents, psychopolitics flatters the psyche, preempting it instead of confronting it. It protocols emotions and desires instead of inhibiting them. “By means of calculated prognoses, it anticipates actions-and acts ahead of them instead of cancelling them out” (ibid., 36).

Moreover, according to Han (2017b), shock (which represents the response to cinema, according to Walter Benjamin), is no longer the emotive response found today, rather what is found resembles ‘disgust’. Images trigger disgust instead of shock. Shock, in the parlance of Han, represents a feeling, which takes the place of ‘contemplation’ (in context of the emergence of cinema). Disgust on the one hand is an emotion or an affect. To be exploitable, what is to be incited is disgust, since even

repulsive content is meant to entertain, that is to be made consumable. Shock is an immunoreaction; as such it impedes communication and the circulation of information—the essential mechanism of the information regime. As said earlier, emotional capitalism however necessitates the acceleration of communication. In addition, the lower the threshold of immunity the more acceleration the circulation of information gains. Dulling the sense, in this context, relies not on shock, but rather on the over-triggering of affects and emotions.

Moving back to Lyon (2017), he states that entertainment and serious life are increasingly becoming the aspects of the same thing. Han delves deeper into this and conceives of this ‘gamification’ as an essential and necessary part of this shift towards immaterial modes of production—an essential power of technology in psychopolitics, working along with emotions (2017a). For Han, the contrast is between games/playing and labour, between *homo ludens* and *homo laborens*. Gaming, that is the ‘other’ of Work, is exploited. Life and working are gamified to the end of increasing productivity. Thinking takes two forms. The first is thinking at work, with the other being thinking at play.

The game operates with a particular temporality which is characterised by an instant sense of reward, delivering an immediate experience of success. This, in turn, delivers higher performance, and stimulates further motivation—emotion. The *homo ludens* is being emotionally invested, made to work in a manner that surpasses the way the *homo laborens* engages with/in labour. “The gamification of work exploits *homo ludens*. The player subjugates him- or herself to the order of domination in the very act of playing” (ibid., 49-50). Moreover, through social media, communication is also subjugated to the logic of the game. This gamification of communication entails commercialisation—destroying human communication. This brings up again the issue of freedom. Freedom is associated with play—that is, freedom belongs to the other of the work, it takes place outside the realm of labour. It belongs to the unproductive, to a mode of living that is not a mode of production. It is outside the realm of necessity. However, with the gamification of labour and the totality of life, the emancipatory potential of play is expropriated. In short, this novel mutation of capitalism invests and assumes playing into the realm of labour for exploitation for

productivity. Gaming and labour coincide—the totality of life falls under the exploitable.

The psychopolitics of the information regime, thus, enacts a form of ‘smart power’. This power is permissive rather than repressive, works by stimulation rather than inhibition. As such, it is more powerful and efficient in comparison to disciplinary power. Moreover, and what is important in relation to the crisis of freedom, as articulated by Han, is that psychopolitics commands a different mode of appearance, further invigorating and fortifying its power. It takes place as ‘it just happens’ without drawing attention to itself. Its technologies of power escape visibility. Furthermore, the context of domination is hidden and thus the subject dwells in the illusion of liberty, thinking it is free, to the effect of participation in its own exploitation. The second main phenomenon of the ‘surveillance culture’ proposed by Lyon (2017), is the fact that subjects are no longer merely the targets and objects of surveillance by a higher and detached surveilling subject, rather they are active participants, not only engaging with surveillance but also initiating it. This, according to Han, emerges as a result of this particular smart power—it is an effect of the crisis of freedom. “Today’s crisis of freedom stems from the fact that the operative technology of power does not negate or repress freedom so much as exploit it. Free choice (*Wahl*) is eliminated to make way for a free selection (*Auswahl*) from among the items on offer” (2017a, 15). Only a negative regime of power becomes visible, and as such elicit resistance.

Moreover, unlike disciplinary power, psychopolitical power does not seek to make people ‘compliant’, but rather ‘dependent’. As such it does not require energy and force as much as disciplinary power does. It pleases, seduces, fulfils and meets the individual half-way, guiding their will to its own interest. It does not impose silences, it urges expression and communication, of opinions, desires and wishes. Under the information regime, “people subjugate themselves to domination by consuming and communicating” (ibid., 15). The efficacy of the smart power of psychopolitics under neoliberalism is unprecedented and its economic mode of production is the root cause of the crisis of freedom. ‘It simply happens’, and through Big Data and advanced algorithms it reads, predicts and evaluates our both conscious and

unconscious thoughts. Indeed, as Lyon (2017) states, this is not to say that resistance does not exist, rather, the majority of the population are compliant with surveillance (that is in Han's analysis, 'dependent') on the information (i.e. surveillance) regime.

It is through these technologies of power that the Big Brother of the Orwellian society becomes a 'friendly' Big Brother, even when the awareness of it exists. In fact, everyone is both at once the Big Brother and a prisoner, a situation in which Bentham's panopticon is efficient and complete (Han, 2017b). It is a Big brother that does not erase words from the lexicon it seeks to multiply them endlessly; instead of erasing the word of 'freedom' it works to intensify it.

It is important to distinguish between psychopolitical technologies of power and psychotechnical methods—as was mentioned earlier, in relation to shock. The biopolitical panopticon of Bentham, while invisible it is sensed, and in this being sensed lied its efficacy as to ensure discipline and compliance with the rules of the institution. The inmates interiorize the panopticon's Big Brother. This Big Brother operates by psychotechnical methods, including solitary confinement, constant surveillance, or the power of norms and disciplines. The digital panopticon, however, penetrates and molds the psyche, by being stealthy and non-sensed. It is invisible and as such it is not interiorized but rather the subject is modulated around it. It seeks not to cast into a mold, rather to morph and modulate. Here, to repeat, negativity yields to positivity, repression to stimulation. Confession is not obtained, it is given (data, in the original sense of the Latin word—'to give') and voluntarily disclosed.

The Ministry of Truth yields to predictive algorithms, that instead of rewriting the past according to the present, it seeks to influence the future through the tools of predictive algorithms and the collection of data (Han, 2017a). It is important to reiterate the following point in this context: the digital panopticon is not internalised in the sense that it was in the panopticon, rather what is at stake is that the 'arts of life', or the technologies of the self, are subsumed into technologies of power—under psychopolitics, both coincide. It is in this way that surveillance becomes efficient—eliciting general compliance and active participation. In addition, it is in this way that “the dominant aspects of surveillance culture often play into surveillance capitalism,

facilitating and normalising it ... [and in which] much of surveillance culture depends on and is nurtured by surveillance capitalism” (Lyon, 2019, 72).

The digital panopticon thrives on this auto-exposure, leading to self-illumination and self-exploitation. Here emerges the crisis of freedom, without the Big Brother wresting out information from the surveiled (Han, 2017a) and the difference between the Big Brother and the inmates becomes increasingly blurrier through hypercommunication—control and freedom, thus, become indistinguishable (Han, 2017b).

If the psychopolitical regime of control is so efficient, it is because of the emergence of Big Data and the associated advanced algorithms, including AI algorithms, which facilitate the collection, retention, and processing of huge amounts of data. Big Data, in short, refers to “massive data sets having large, more varied and complex structures with the difficulties of storing, analysing, and visualising for further processes or results” (Sağiroğlu & Sinanç, 2013). The massive volume, the wide variety and high velocity necessitate novel algorithms and methods, statistical and otherwise, to gather, analyse, present, and make meaning out of the collected data. This is not simply a matter of collecting excessive points of data on the individual and population, in an unprecedented fashion. Big Data is also identified by an ideology, a set of assumptions that act as the basis of the information regime, as a form of domination with far-reaching implications.

Big Data allows digital surveillance to become aperspectival, unlike any previous analogue optical surveillance system (Han, 2017a). It peers on and into the surveillance object from every and any angle. It eliminates any blind spots into the object of its inquiry. Moreover, it is oriented towards the future, with predictive data analytics. It works in accordance with the imperative of transparency. Transparency here refers to ‘the’ systematic compulsion of the information regime, since everything is to be transformed into information and communication. The information society is a transparency society (Han, 2022). Transparency is a neoliberal dispositive, working along the line of positivity, which deems information as a positive value, by force turning everything into information. Transparency is

required under the demands of the freedom of information and the freedom of circulation. This happens, again, under an immaterial mode of production which equates more information and more communication with the increase of productivity, growth and acceleration. Secrets and otherness are hurdles in the way of efficient, unlimited information and the circulation thereof. Everything is to be datafied. Life is to become completely logged in.

This means that through Big Data and advanced algorithms, the information regime is able to provide ‘psychographical’ charts of the individual and the population alike. In the disciplinary regime, working along the lines of biopower, statistics (the mode of calculation) could only provide demographical charts. As such, subtle psychological intervention was not feasible in that era. Control had to be enacted by confinement, on the body, from the exteriority of the body. Psychic processes were beyond the reach of discipline. In fact, the resources to achieve a decent level of such a psychographic chart does not require much resources. One need not be a resourceful company like Cambridge Analytica. In a presentation on data analytics and micro-targeting, Shivam, a political consultant working with data, demonstrates the facility with which the public discourse can be shaped in the context of Indian state elections. It is easy to collect information on people, much of which is available online, to buy data and to recruit motivated volunteers to do surveillance tasks (Shankar Singh, 2018).

In contrast, the panopticon of Bentham had only a ‘punishment log’—far from being an efficient recording system. It could not have access to thoughts and desires beyond what is expressed. Furthermore, the development of the Internet of Things and wearable devices, turned most of the objects around us into agents of surveillance. Self-surveillance is the motto of the era.

Han builds an analogy with the ‘optical conscious,’ proposed by Walter Benjamin (Han, 2017a, 2017b, 2022). According to Benjamin, the movie camera brings about the ‘optical unconscious’—providing a different gaze to reality, as a result of the new affordances of the movie camera. Han observes the emergence of a ‘Digital Unconscious’. In this analogy, Big Data operates in a manner akin to a magnifying

glass. Data mining renders previously elusive behaviours and micro-actions detectable, quantifiable and recordable, for the purposes of prediction and influencing behaviour, through micro-targeting and other technologies. This also works at the level of collective patterns, presenting ‘collective digital unconscious’. With enough data points, this can be better than our knowledge of ourselves, since it captures micro-actions and desires that escape consciousness. As such, digital psychopolitics would be in the position to take control of mass behaviour on a level that escapes detection” (Han, 2017a, 65).

In this situation Big Brother and Big Business are merging, and “[i]t’s getting harder and harder to tell the difference between economically motivated snooping for data and its use for intelligence purposes ” (Han, 2017b, 73; 2017a). The American company Acxiom collects and stores on almost all the citizens of the United States. It provided the authorities with personal information of 11 suspects in relation to the 9/11 attacks (Han, 2017b). The company possessed more personal data on Americans than the Federal Bureau of Investigation.

Han sees this in connection with Bauman and Lyon (2013), who note that with the panopticon there emerges a ‘ban-opticon’. With the utilisation of Big Data, there emerges a new society of digital classes, based on the utility of the individuals, or rather the data-based doubles of the individuals, both collectively and individually. The ban-opticon serves to exclude the ‘waste’ population—population the data of which yields no economic gains. It is an exclusionary mechanism, to set the boundaries between demographics which are to exist within the regime of control, that is, the demographics that yield economic gains on the one hand, and those demographics which are without economic value on the other. People are classified into categories and “the sole accomplishment of waste is soiling and cluttering up the space that could otherwise be usefully employed” (Bauman & Lyon, 2013, in Han, 2017a, 66). For example, in the realm of video game analytics, players are usually characterised according to their spending on the game’s platform. Whales is the title referring to those who spend too much money to buy game features. Krills are the opposite, they never spend any money while Dolphins are occasional spenders (Quartz, 2018). Such categorisation impacts how the company shapes its policies and

algorithmic engagement with the different categorised demographic for effective manipulation. This also takes place in all aspects of life, reinforcing social injustices and biases.

### **3.1.5. The Information Regime: A Second Enlightenment**

According to Han (2017a), a second Enlightenment has emerged. During the first enlightenment statistics were celebrated as a revolutionary force, which will bring an end to the myth. Han here cites Voltaire, Kant and Rousseau. For Voltaire the Enlightenment and statistics are one and the same. Voltaire contended that through statistics a new historiography will emerge that will revise history and efface all histories, which according to him are all narratives bordering on mythology. Statistics will render history truly philosophical. It is only through statistics that objective knowledge can be derived, since it is based on numbers rather than narration.

The political implications are present in Rousseau's understanding of the general will. Rousseau developed an arithmetic rationality that is possible without communication, as opposed to communicative rationality. The general will 'must' be without communications, as communication and discourse distort it, by exerting influence and mitigating the differences (Han, 2022). It is a matter of statistical averages: there is the 'will of all' and the 'general will', the 'will of all' is the sum of particular will; but if we cancel the opposites "the 'pluses' and the 'minuses' which cancel each other out" (in Han, 2017a, 74, emphasis added)—what's on the other side of the equal sign is the 'general will'. As simple as that! According to Han, Rousseau's represents a biopolitical response to the issue of good governance—a democracy of pure numbers, without discourse or communication (ibid). Even Kant caught the euphoria of statistics: the conduct of individuals might seem arbitrary, however, if we take a look at the free will on a large scale, that is statistically, we might find that human will operates in accordance with the laws of nature. Statistics, thus, was a means to face up to the contingencies of the world (ibid.).

Today, the same euphoria exists in relation to Big Data. It is 'dataism' which has taken the stage, as the new faith of what Han calls the second Enlightenment. Its

imperative; all is to be rendered into information. It fetishizes data and information. Everything that can be quantified, should be quantified. It seeks to make ideology and theory obsolete. David Brooks (2013), in his influential article in the New York Times, keeps unanswered the question as to when to rely on intuitive patterns and when to ignore intuition all together, in favour of relying on data. Nevertheless, he promotes data-ism with its cultural assumptions: “that everything that can be measured should be measured; that data is a transparent and reliable lens that allows us to filter out emotionalism and ideology; that data will help us do remarkable things — like foretell the future.” and celebrating that data can expose when intuition is faulty as well as illuminate unnoticeable behavioural patterns. This is the essence of dataism. “[T]he ideology of dataism shows characteristics of a widespread belief in the objective quantification and potential tracking of all kinds of human behavior and sociality through online media technologies” (van Dijk, 2014, 198).

Datafication and dataism have become accepted scientific paradigms, in relation to understanding social behaviour and relationships. According to van Dijk (2014), dataism resembles a secular belief that relies on problematic ontological and epistemological claims. The first of these claims relates to a widespread misconception that data is objective and that larger datasets yield higher intelligence and insightful knowledge. The second relates to the assumption that data is ‘raw’, given, simply there, and waiting to be collected and processed. Nevertheless, these are myths: the collection of data is nothing but objective. It is rooted in assumptions and implicit questions that guide and frame the process of collecting information. Indeed, raw data is an oxymoron. Data by itself reveals nothing—it is given prior to argument, prior to narration (to use the parlance of Han), yet to be interpreted. Piles of data by themselves “reveals no more information about specific human behavior than large quantities of sea water yield information about pollution” (ibid., 201).

Dataism is compelling, according to van Dijk, for the new scholarly frontiers it promises, on the basis of these assumptions—that mining of data does not have a pre-set context and its analysis does not have a predetermined purpose. Big Data is claimed to efface the subjective arbitrariness in the process of producing knowledge. Moreover, obtaining data renders theory superfluous. Knowledge is to rest on data,

and the more data is collected the more understanding we obtain. ‘Numbers speak for themselves’ (Anderson, 2008).

Knowledge here relies on correlation as the means to producing knowledge. Causation yields to correlation. The advanced algorithms for processing and analysing these huge piles of data, however, work through the operations of abstractions, reduction and representation. These abstractions are reductionist, providing categorisations and descriptions of reality in accordance with pre-set features, which are further reduced within the internal transformations of the algorithms (Mcquillan, 2022). Everything psychological and social is to be captured and transformed into numbers, that is, datafied, in order for it to be processed. Language itself is rendered into numbers and linguistic relations are turned into mathematical functions.

Han, building on Hegel’s logic, states that “*Totalized data-knowledge amounts to absolute ignorance*” (2017a, 70, emphasised in original). Correlation is the most primitive level of understanding. It represents probability—not a relationship of necessity. A higher level of knowledge is causality, distinguished by necessity and explanation. Reciprocity, still, is a more complex relation than causality. A and B are necessarily conditioning each other reciprocally. Still, even at the level of reciprocity, we lack conceptuality. What brings about knowledge is the ‘Concept,’ which is capable of providing the higher context of A and B. “Only from the all-comprehending Concept C is complete comprehension (*Begreifen*) of the correlation between A and B possible.” (ibid., 69). As such, with its reductive abstraction and correlation-only methodology, Big Data in itself produces absolute ignorance. “The absolute knowledge intimated by Big Data coincides with absolute ignorance” (ibid., 69).

As such, dataism and its neoliberal transparency herald a false clarity. To reiterate, this second Enlightenment appeals to information, data and transparency. In the name of reason, the first enlightenment worked as an oppressive force. By a fatal dialectic, the first Enlightenment, in its quest to destroy myths, turned itself into a myth, resulting in barbarism (ibid.). The second Enlightenment risks a similar fatal

dialectic—leading to the barbarism of data. Claiming to be counter-ideology, it has become an ideology itself (ibid.). It buries politics and ideology with the machinic opacity of its advanced algorithms and mathematical models. Moreover, it makes possible the dismissal of alternative perspectives and modes of life, as subjective, intuitive—thus, less worthy (McQuillan, 2022). The effects of such ‘barbarism of data’ are observed in every aspect of life—the biases are experienced and the consequent harms are affecting people at large.

Importantly, it naturalises and essentialises dividing lines and social boundaries, reinforcing the *status quo* and generating knowledge that privilege particular groups (the already powerful) over others (the already vulnerable) (ibid.). It is an ideology that “uses the aura of science to perpetuate the idea that its abstract mathematical models provide a reliable way of knowing, and promotes a reductive definition of truth that is claimed as inherently superior to lived experience” (ibid., 51). Thus, and to repeat, “Neoliberal psychopolitics is a technology of domination that stabilizes and perpetuates the prevailing system by means of psychological programming and steering” (Han, 2017a, 79).

However, these harms and negative side effects make the accompanying euphoria not last for long. In the case of the first Enlightenment of the eighteenth century, it did not take long before resistance to statistical reason emerged. Today, too, resistance is emerging, however, the context and the regime of power against which resistance in the contemporary takes place is fundamentally different. This entails new consideration of the new, or necessary, modes of resistance against this new regime of power, and the efficacy of such modes and tactics. What follows summarizes the discussion so far, before moving on.

Byung-Chul Han essentially observes a paradigm shift taking place with the ‘digital turn’. This is a mutation of capitalism in which a new immaterial mode of production emerges. This mutation of capitalism is fundamentally different from the capitalism of the industrial era of the nineteenth century. To the end of overcoming previous limitations to production and to increase efficiency for economic gains, a new form of power emerges. Instead of biopower working along the lines of biopolitics, we

have psychopower with a psychopolitical form of control. Psychopolitics seeks not to exploit bodies and energies, rather it seeks to penetrate and seize the psyche to influence and control the population. It operates through the imperatives of positivity, rather than negativity. It is permissive rather than repressive. It incites, seduces and encourages expression, rather than inhibiting, disciplining and imposing silences. The milieus of confinement yield to continuous fields of operation. The molded subject becomes an entrepreneur, a project that continuously self-optimises.

The characterising medium of this ‘second Enlightenment’ is the digital medium with its data infrastructures, especially Big Data, and the necessary advanced algorithms of information collection, storing and processing. Dataism is the digital rationality of the information regime. Its imperative is transparency and the free circulation of information, allowing for the datafication of life to the end of economic exploitation.

To make the information regime more efficient, emotional capitalism seizes emotions and affects, after eliciting and inciting them unprecedentedly. Furthermore, it renders life in accordance with the logic of games. As such, surveillance and control are inherent features of this society of hyper-communication, and with its smart power, we witness a friendly Big Brother. Self-exploitation, through self-exposure and self-illumination, is the salient character and dynamic of control in this era, resulting in a crisis of freedom in which the subject dwells in the illusion of freedom while in the act of exploiting itself. Freedom and control, thus, coincide. The dialectic of this second Enlightenment leads to data barbarism, manifesting the biases, injustices it reinforces and reinvigorates, as well as in the resulting harms.

### **3.2. Games**

Perhaps, video games present an exemplary case to illuminate the previous discussions. As was mentioned earlier, dataism and digital utopianism lost the euphoria and enthusiasm of its early days, as the impacts of the information regime have been directly experienced by people in different demographics, especially the impact on marginal and vulnerable sections of society. There is no doubt that

awareness of surveillance and the data regimes have increased, especially after the revelations of former NSA contractor Edward Snowden. Nonetheless, as Lyon (2017) observes the majority of the population complies with surveillance and is an active participant of it. This awareness, however, is limited usually to particular practices and institutions—for example, micro-targeting and platform algorithms, and to corporations like Google and Meta.

The surveillance of video games does not enjoy much awareness and receives less critical engagement in comparison. Moreover, the market of video games has expanded exponentially in the last decades—especially, with relying on monetary micro-transactions within the games themselves (Quartz, 2018). Video games in the information are not exactly games. Needless to say, they have become big industries, and, in addition, they operate within platforms (like Google Play, Steam, or Apple Store) or have become platforms of their own (like Fortnite). Moreover, game engines have grown in complexity, reflecting different policies, business models and ideational positions within the data economy—emerging as platforms themselves as well in some cases (Chia et al., 2020). Video games are everywhere nowadays, an average cellphone is full of various video games, with online cultures revolving around particular games (PUBG for example). They are widely adopted as the most prevalent digital media form and appeal to a variety of demographic groups—interesting is the fact that the largest gaming demographic group in the US is adult women (Egliston, 2020; Quartz, 2018). Moreover, identities have grown to become entangled with the act of gaming—the identification as a gamer or otherwise; the connection with racial, gender and sexual identities (Shaw, 2011).

More importantly, it operates in a position which makes it more intimate and immediate to the psyche. I use games here as an example par excellence for a psychopolitical technology of power. Video Games are essentially systems that transform physical, neurological and cognitive inputs into machine language, producing output the player can comprehend (Egliston, 2020; Cybulski, 2014).

The interest in games emerged for a number of reasons in both state and corporate institutions. For example, NSA documents from 2007 and 2008 reflect this interest

for intelligence, military purposes as well as for interactive influence. This interest is three-fold. Technically, games are easy to produce—especially with the emergence of ‘game engines’, including Unity game engine and platform. Games are popular, especially amongst the population generally targeted for the military, between 18 and 35 years old. Finally, when located within militarized discourses, games serve multiple functions: propaganda; military recruiting, training and simulation; and potentially money laundering and fundraising (Whitson & Simon, 2014).

Another factor inciting such interest is the potential of data collected through games: it far exceeds the potential data collected in, say, online shopping platforms or search engines. Game telemetry relies on collecting biometric data. Eyes and player gaze become a target of datafication. As technical study on developing eye tracking in games proposes: “we can find out so much....we can for example see what parts of the screen he focuses on most, how often s/he checks her/his minerals/gas and how often he looks at the mini-map” which enables teaching an agent something in relation to the game on the basis of this input (Fekete & Hagelbäck, 2012). With the increasing utilisation of virtual reality devices, with eye-trackers embedded in them, and the relatively easy access to facial input, the quantification of ‘engagement’ becomes easier and yield higher efficiency for the optimisation of game systems and micro-targeting advertisement, within and outside games (Rashed et al., 2025). Even health related gadgets, like heart-rate devices, are used psycho-physiological techniques during gameplay, to identify specific psychological states of users during playtime (Nazlina et al., 2012).

The market of game development is highly competitive, and game analytics has been a crucial part and constituent of it. With the field of game analytics, middleware companies emerge selling costly data and analytics to game developing companies and engineers, for various reasons—including, the development of their games, advertisement and micro-targeting (Egliston, 2020, 2021; Sifaa et al., 2018; Whitson & Simon, 2014). More importantly they are used to shape the behaviour of players to elicit profit through addiction and compulsive spending—to make in-game purchases, to continue playing, and to start playing a newly produced game. The business models of many games act in manners akin to gambling platforms—for

example, selling in-game gadgets in a mystery box or drawing lottery (Quartz, 2018). These objectives are not easy to achieve and game analytics companies promise to provide solutions through profiling and deep understanding of players, individually and collectively. Engagement measures and telemetry are used to that end.

Player engagement, thus, becomes a primary goal for companies in this field of game development as well as small game developers. To maintain the right affective experience (the fun) and the cognitive engagement (high concentration and low spatio-temporal awareness), game developers need to understand a complexity of issues, including how to balance between difficulty and player skill, feedback availability and goal clarity. Player engagement takes place on multiple levels—the cognitive, the affective and the behavioural (Rashed et al., 2025). All these dimensions need to be captured to foster emotional attachment and player retention within the game. The state of being of the player needs to be captured.

Telemetry and facial input seek also to capture the behavioural dimension of the player in-game. There are a variety of player engagement estimation models and approaches, capturing various aspects of the gaming process, using a variety of simple and complex techniques (ibid., 2025)—it is a thriving and expanding area of development. “The use of metrics in the game industry directly parallels the hype around Big Data more generally, emphasizing surveillance in the future tense: collecting and collating massive databases of seemingly trivial data in the hopes of inferring hidden patterns and correlations in human behaviour that then can be used to profile subjects, predict their actions, and to act upon them accordingly” (Whitson & Simon, 2014). Thus, surveillance (as a ‘friendly’ Big Brother) is also at the center of the game development industry.

With huge amounts of data points of each player that are highly complex and volatile, behavioural profiling of gamers becomes a solution. It offers the possibility of condensation and modelling, rendering players quantifiable for understanding their modes of playing—in the past, present and future (Sifaa et al., 2018). Indeed, motivation is at the centre of this model of gaming, and can be inferred using automation directly during playing, without explicit requesting of information from the player, with the potential for dynamic adjustment of experience (Yee et al.,

2012). Indeed, some commentators resemble game business models in this era to business models of gambling, for example, selling in-game gadgets in a mystery box or drawing lottery (Quartz, 2018). Ban-opticon, as discussed earlier, is also at play here. Players are usually profiled according to their spending on the game's platform. Whales are those who spend too much money on game features. Krills never spend any money and Dolphins are occasional spenders (ibid.). The personalisation of the game and the objectives of influence depend on the categorization where the profile of the player is located. "[T]he sole accomplishment of waste is soiling and cluttering up the space that could otherwise be usefully employed" (Bauman & Lyon, 2013, in Han, 2017a, 66). The 'Krills'<sup>9</sup> of the game serves to optimize the game's system, to soil the space—in addition to the advertisement potential.

This business model is reflected at the level of technical design of the video games. As said earlier, video games are systems, simulations representing particular milieus and activities. This has an input and output, and the processing and execution takes place through code. According to Cybulski (2014), code architecture is essential in this regard. It is important to understand the flow and direction of information. The video games business models operate on code architectures that are opaque and asymmetrical. Moreover, it facilitates and is dependent on surveillance. The code architecture has two main aspects that contribute to this: data structures and modular coding. First, the data structures are designed to ensure efficient collection, retention and revoking of data in a dynamic manner throughout the programme. Secondly, the code uses modular code, consisting of discrete chunks of code, instead of one complete project. This facilitates the editing of specific functions or methods (that is chunks of code), making the task of fixing code easier. This also makes easier the alteration of the game for a particular user on the basis of their profile and the collected behavioural data—the game is to be altered slightly, to influence in-game behaviour and to maintain the player's cognitive engagement (i.e. high concentration and low spatio-temporal awareness).

---

<sup>9</sup> The word 'krill' refers to marine creatures living in oceans. However, the popular use (from which it entered into the jargon of game analytics) has multiple meanings that are indicative of situations in which the 'krills' exist in the context of games. It might refer to a hustler, or someone who collaborates in a group, hardworking. It might also refer to an underdog, a person or a group with less power and resources in comparison to others in a group.

Even though resistance practices are also present in this digital realm of participatory surveillance and self-regulated governance systems, automatic tools of hierarchical governance undermine any kind of empowerment present in these platforms. For example, Massively Multiplayer Online Games; which operate as surveillance assemblages of corporate governance—rely on automated forms of dataveillance and on contract law to punish players and control them to the detriment of their privacy, effectively curbing any deviant behaviour the guidelines of the platform (Kerr et al., 2014). Even for small game developers, individual or otherwise, commercial viability and visibility depends on their adherence to the internal logic and determined policies of the platform(s) on which they operate (Egliston, 2021).

Streaming is the broadcasting of gameplay by a gamer. It has grown to become a significant part of the ecosystem of video games. Streamers broadcast gaming as a type of creative and communal play. This was soon brought under exploitation through control and surveillance. What Walker (2014) calls “streaming posture” is the stance taken by streamers, in relation to their engagement with the streaming platform characterized by passivity or activity. With an active streaming posture, streaming takes place voluntarily and players exert effort to make streaming possible. They develop a public identity, shaping or playing within communities. With a passive streaming posture on the other hand, streamers subjugate themselves to the logics and rules of the platform on which they play. They rely on the software and hardware resources provided by their respective platform—even their streams become available on the website, without consent. In effect, they are labourers for the platform. Streaming platforms demonstrate that game governance shapes players’ behaviour in a flux, shifting, and adjusting manner (Kerr et al., 2014).

Leisure becomes labour, often lacking the player's explicit consent. This exploitation is often unnoticed—since it is not considered labour. Moreover, it is easy to imagine these players calling themselves entrepreneurs. The power of games also derives from the fact that it also renders serious life, labour, into a gamified version. Another reason for the sudden interest in games is the game’s ability to improve achievement, efficacy and engagement in fields other than leisure games (Yee et al., 2012; Whitson & Simon, 2014; Rashed et al., 2025). Such fields even include health, as in

the case of a project which promotes the development of games that use eye-tracking devices, and the collection of relevant data, to improve vision impairments related to oculomotor training, through games (Arnarson et al., 2021).

### **3.3. Countering Surveillance and Collective Action**

To begin with, the neoliberal psychopolitical regime of the information regime with its hyper-communication and acceleration of the circulation of information, and with it acting at the level of pre-reflexive unconscious realm, results in psychological maladies at the level of the population. These psychological maladies impact the resisting agent and undermines the potential for efficacious collective action. Under these conditions it becomes less likely to stand up and question the *status quo* in an effective manner; thus, the possibility for collective action is limited. This will be discussed in what follows and in accordance with the analysis provided by Byung-Chul Han.

One important such pandemic is the Information Fatigue Syndrome (IFS). IFS was limited to individuals whose work demanded the analysis and processing of huge amounts of information. With intense engagement with information, they suffered from symptoms including attention deficits and gradual deterioration of their analytical capabilities. In addition, they gradually lacked the ability to accept responsibility (Han, 2017b). In today's world of constant networking and circulation of information, and with the expropriating of the entirety of life as labour, the IFS affects everyone in the information regime. This pandemic affects resistance in more than one way. On one level, the analytical capacity is necessary for thinking and reflection. Without it, it is not possible to distinguish and select—the necessary processes in social and political discourse.

The positivity of the achievement society de-interiorises the subject and its capacity for reflection by stripping it out of the negativity necessary for action. Negativity is inherent in thinking, as the latter depends on discerning, selection and distinguishing. It works by excluding certain elements of a discourse, of a world-view, and affirming other elements (ibid.; Han, 2022). As such, the individual is stripped out of the

potential to choose freely, it can only select from the items offered to him or her (Han, 2017a). Free choice yields to free selection from the given options.

The IFS and the consequent symptoms stem from the rationality of the digital era—i.e. dataism—and its imperative, stating that the more information possessed, the more insight, better judgement and decisions one can have—the logic of positivity. However, better judgement and decisions necessitate the process of exclusion, omission—negativity. Less information proves more productive, to deal with social and political problems. Information on its own, without the negativity of theory or ideology, means nothing—it offers no truth, no concepts, no conclusions, it only serves to confuse. Information, after a certain point becomes deformative instead of informative—and communication simply cumulative, instead of communicative (Han, 2017b, 2022).

This society of ‘tiredness’ precludes what is common, the shared—it precludes proximity (Han, 2015b). The eradication of negativity enhances the logic of achievement. It has a different psyche from that of the disciplinary society. It is a psyche which is poor in negativity, a psyche that is constantly working along the lines of ‘can’, rather than ‘should.’ Its subject is an achievement subject, working along the lines of freedom, pleasure and inclination, rather than duty (ibid.).

Bearing responsibility is essential for a productive collective action and it requires particular conditions—mental and temporal conditions. The fleeting, short-term temporality of the information regime, through hyper-communication, promotes non-bindingness and arbitrariness. It scatters time. It seeks to seize the future by optimising the present, rendering time into a mere sequence of disposable presences. This eradicates the potential for actions that give time or necessitate duration. As such bearing responsibility or making promises, obligation becomes unlikely. Moreover, trust becomes impossible under such circumstances, and even unnecessary. The fact that information can be readily accessible renders trust meaningless. With this transparency and the possibility of capturing all aspects of life, the logic of efficiency becomes the mode of operation, in which surveillance and control replace trust (Han, 2015a, 2017b).

Photography, for example, in its basic form, represents a truth. It refers to a particular, constant referent. Digital photography in contrast, with editing tools, calls into question the truth and the referent of the photograph. Furthermore, the excessive amount of data available, and the advance of generative AI that produces high quality images, the crisis of representation is exacerbated. As such, it does not represent, it merely presents. It is self-referential. The political corollary is a situation in which the contemporary political economic regime is self-referential. Politicians and activists are no longer seen as representing a demography but as agents of the system—the referent of the political act is no longer the real referent, the human being. With this self-referentiality of the system, individuals are alienated and isolated. They cannot and are unwilling to act politically or participate in discourse (Han, 2017a).

This brings about a milieu in which communication takes place without a community and makes discourse superfluous (Han, 2022). The digital rationality continues the logic of Rousseau, discussed above. With huge amounts of data and information, we have the chance to capture the complexity of society—mathematically. Understanding how the society works, we can provide technical solutions for problems and conflicts. Indeed, the autonomous human is nothing but a construction emerging out of our ignorance to explain what was not previously explainable due to lack of enough information and the capacity to process it. The individual is merely a behavioural device, by collecting this device we can understand the root causes of its behaviour (Pentland, 2015, Skinner, 1973, in Han, 2022). We can develop social physics through sociometers to mine reality—rendering it predictable and controllable; government and politics become merely the process of optimised planning and conditioning.

Discourse, on the other hand, is slow and an inefficient mechanism of information processing and lacks enough information. As such it is a mechanism of ignorance. Algorithms replace argumentation. Here communication and the public sphere are dismantled (Han, 2022). However, as discussed earlier, advanced algorithms do not think, they count. They do not provide a narrative enabling the explication of the world and offering a worldview, rather they are only additive. Information is merely additive and cumulative; it lacks the higher context within which it takes place. It

adds, and never concludes; it is always open for further addition. Knowledge demands a form of syllogism (that is, in Hegelian terms, a form with a beginning and an end with meaningful relations governing them), a form of coherent narration. Addition, on the other hand, yields no conclusion; it goes on end, and as such, it can only work at the level of correlation (Han, 2017a).

Moreover, the abstractions of advanced algorithms are reductionist, providing categorisations and descriptions of reality based on pre-set features, which are further reduced within the internal transformations of the algorithms. These are mere numbers, with assigned meanings, concealing pre-held ideological assumptions and politics under machinic opacity, while wearing the cloak of scientific objectivity—to the end of social detriment (Mcquillan, 2022). The assumptions and the worldview of AI, as defined above, is the problematic part of the story, leading to the harmful consequences. Furthermore, they inherit concepts developed under colonialism, reproducing them as a form of ‘race science.’ AI puts on the cloak of absolute, objective science, building on the legacy of statistics and the scientific methods, while also pretending to be the solution; through solutionism and dataism. As such, AI naturalises and essentialises the dividing lines and social boundaries, reinforcing the *status quo* and generating knowledge that privilege particular groups (the already powerful) over others (the already vulnerable). The consequences can be disastrous—intensified inequality, injustices, with the existing forms of structural and cultural violence condensed.

Aside from the more immediate harms of AI and Data Apparatus, of particular importance according to McQuillan (2022), is the path AI enables towards a full-scale, comprehensive algorithmic authoritarianism—lends itself to fascism. Fascism is, of course, a result of multiple factors, where multiple crises and discourses confluence. In the world we live in, AI conflues with a coming global crisis and a *status quo*, enabling and empowering fascistic tendencies. This isn’t about usage of AI by authoritarians, but rather a deeper link, rooted into the nature of technology and the worldview it assumes.

Narration adheres to a different temporality than that of the information regime and it depends on negativity as well as positivity. It is slow, recounting, and engages in

selection, affirmation and exclusion. As such it can stand up to such hegemonic assumptions and worldviews. It is capable of producing alternative ways of life and programmes for moving forward and questioning power. In the information regime, narration is destroyed and replaced by data and correlation.

Under conditions of distrust and communication without a community, the potential for collective action becomes unlikely. Eli Pariser (2011 in Han, 2022) argues that algorithmic personalisation is leading to destruction of the public sphere for effective communication. The ‘filter bubbles’ keep users within particular atmospheres of opinions and with other opinions are excluded. The social media user has content before him or her only from a particular worldview—this is a direct threat to democracy, too. Han (2022) criticises Pariser for being reductionist. The issue is not simply a technical matter, the root causes are essentially social. The root cause of this is the ‘eradication of the other’, under the psychopolitical information regime.

Psychopolitics leads to total isolation (Han, 2017a). Under this mutation of capitalism, the worker becomes an entrepreneur, who is an individualist—alienated, isolated and is living under conditions of ‘solitude’. Without an other one’s opinion lacks the discursive character necessary for communicative interaction. It is the voice of the other, the potential countering and challenging of one’s opinion, that makes it possible for this opinion to become part of the process of a truly discursive reflection. Otherwise, an opinion or a proposition is merely self-absorbed and dogmatic.

As such, in the contemporary digital sphere, content creators and followers do not constitute a public sphere (Han, 2022). They are more akin to ‘swarms’—gathering of fleeting patterns, volatile and ludic. A swarm is soulless, and there is no political ‘we’ possible within it (more below) (Han, 2017b). They exist as tribes. These digital communities are, as such, commodified. They lack the capability to act (Han, 2022).

As was mentioned earlier, otherness and foreignness are hurdles in the way of efficient, unlimited information and communication—that is, they are limitations for productivity, growth, and acceleration (Han, 2017a). Thus, sameness is what

characterizes this contemporary society. Transparency demands conformity in order to curb the other, the deviant. Conformity becomes a compulsion. Big Data and advanced algorithms emphasise the likelihood, the average of the collective behaviour. It is blind to the singular, the deviant, the statistically unlikely, and it seeks to eradicate it. With surveillance, and the widespread compliance with it, the resulting effect is conformity. In ‘spectator democracy’ citizens become passive consumers, who consume politics, conforming to the logic of the visible. Reacting passively to politics lacking the will and the ability to engage in communal and political action (ibid.). What ensues in demanding occasions are not political actions, but rather shitstorms—eruptive, short-term communicative fluxes (Han, 2017b). Moreover, politicians and parties treat politics as consumable commodities too, doing anything but a political demand (Han, 2017a). As such, the post-factual politics of fake news, adopted by Trump (the first Twitter president), is only possible under the information regime, with its spectator democracy. Conspiracy theories also thrive under these conditions, with the crisis of truth and representation as well as the fundamental present distrust (Han, 2022).

To reiterate, collective action is undermined and increasingly unlikely. Bearing in mind the crisis of freedom, any revolution distinguishing between the exploiters and the exploited is impossible (Han, 2017a). Along the lines of psychopolitics and the imperatives of the information regime, Han offers a conceptualisation of the collectivities active in the social and political spheres— ‘the many;’ the self-exploiting masses.

Han (2017b) looks into the concept of ‘crowd’ as articulated by Gustav Le Bon in his book ‘The Crowd: A Study of the Popular Mind’. Le Bon conceives of modernity as the ‘age of crowds.’ People emerged as ‘masses’ and the voice of the masses prevailed. It had expressed a new balance of power, constituting the power of the masses, one which disturbed earlier power structure and entailed the crisis of sovereignty. The crowd had a ‘soul’, a ‘we’, that united and gathered them. The mass came into being through this unifying spirit. The individual was assumed into the mass, the features of a mass did not emerge out of its constituent individuals. In other words, the mass is more than its constituent individuals. The individual of the mass is

‘no-body’, who does not claim attention and whose private identity is extinguished, melted into the mass.

The *homo digitalis* in contrast maintains a private identity, as an ‘anonymous’ ‘somebody’, with a profile to be optimized. As a project, an entrepreneur, he seeks attention and is constantly on the act of exhibition and self-illumination. He is melting into a new form of mass—the ‘digital swarm’. The swarm does not have a ‘spirit’ that enables it to develop a ‘we’. It lacks the harmony that unites the crowd. They lack the interiority of assembly. It cannot, thus, morph into an active entity, as it lacks internal coherence. When the swarms gather, they are doing so without assembly. They are isolated and scattered. The spaces in which they assemble, that is the digital media (unlike arenas, or the radio, for example) isolates them, rather than assembling them. When the swarms act, they produce ‘noise,’ rather than demands. Shitsorms erupt, in a fleeting, short-time manner, creating noise that fails, and lacks the ability to question the *status quo* or to confront power. They are ‘hikikomori’ (reclusive individuals) sitting in front of a screen. They cannot form a public sphere. The temporality of its engagement deprives it of the possibility to engage in discourse.

The organised labour, through unions or syndicates, does not take place with a fleeting temporality, it is stable and voluntary. Its formations last and is underpinned by a unifying ideology—it has a directionality, marked by resolve. This enables the masses to face up to domination and embark on a collective action. The mass constitutes a form of power capable of confronting the hegemonic, exploitative relations of power. The swarm on the other hand is marked by volatility, instability and a fleeting temporality. It lacks obligation and bindingness and it is ludic. Its gathering, rather than assembly, represents a carnival. It lacks directionality, attacking everywhere under the illusion of activism, motivated by the logic of platform visibility and the act of scandalisation.

While the crowd is marked by rage as a feeling, in relation to the dominant power relations, the swarm is marked by the emotion of outrage. Waves of outrage are more efficient in catching attention, but their being fluid, volatile and short-term, they

cannot shape a public discourse, let alone utilised to bring power into questioning. They dissipate as soon as they erupt. Rage on the other hand is narrative, because it recounts existing conditions and it speaks of particular actions. As such it possesses the capacity to interrupt the existing condition of which it speaks.

The swarm is an inherent result of the digital age and the psychopolitical form of power. The entrepreneur project of neoliberalism cannot be part of a ‘mass’. He is dwelling in the illusion of individualist freedom, which according to Marx, is nothing but a ploy of capital. By eliminating the other, what is free is Capital, as being free cannot happen in isolation, rather by self-realisation with others—a working community (Han, 2017a).

Nevertheless, as was discussed in the previous chapter, there is increasingly a growth in the various forms of resistance against surveillance and against the surveillance regime in general. Much of these instances and initiatives of counter surveillance make use of the affordances provided by the digital paradigm itself. However, there is a dilemma at the heart of this approach. The following chapter looks into an exemplary case of such technologist counter surveillance—namely, the Cypherpunks. It investigates this case through the lens of the imperative of the psychopolitics of the neoliberal information regime.

## CHAPTER 4

### TECHNOLOGIST COUNTER-SURVEILLANCE AND THE CYPHERPUNKS

As the earlier discussion shows, the digital turn brought about a novel form of control, which was perfected through the advanced developments in the fields of Big Data and computational algorithms. Yet the perfection of a regime of domination does not preclude forms of resistance. Resistance is a corollary of control. As discussed in the second chapter of this thesis, the surveillance regime entails counter-surveillance. Moreover, resisting surveillance is a complex phenomenon, involving a multiplicity of actors, forms and strategies.

The Pirate Party is a Swedish party that evolved out of the Pirate Bay, a prominent name in the global hacker scene. The Pirate Bay was a website that allowed Peer-to-Peer (P2P) file sharing and the indexing of torrent files –that is, from one computer to another without having to upload the file to a third-party server.<sup>10</sup> The Pirate Bay represented a serious challenge to media production companies and to the dominant copyright regime. Through decentralised technologies, the Pirate Party seeks to bring about a digital, real-time democracy. In his discussion of the society of positivity,

---

<sup>10</sup> Networks have two main architectures: Peer-to-peer (P2P) networks and client/server networks. The majority of information and file sharing on the internet takes place through client/server networks. The server is a central computer (configured properly to perform this task) and manages the whole network. The client is the user, trying to access, or share a particular file. The client communicates with the server making a request. In file hosting services, like Google Drive, for example, Bob needs to upload his media file to the servers of Google before sharing it with Alice—who in turn needs to ask Google for access to this file. Google here has the upper hand on managing and maintaining the uploaded file. If the file has a copyright claim, the file can be deleted without Bob's consent or even awareness. In contrast, P2P architecture allows Bob and Alice to communicate directly, without the necessity for a third party to host the file. A P2P is a decentralised network architecture. The file is sent from Bob's computer to Alice's computer. This is usually done using a Torrent file distribution system. A torrent file functions as an index, a table of content, including the meta-data necessary for accessing the desired file. No authority can intervene to delete the file, since it is on the personal computer of the sharing user (although under many jurisdictions an Internet Service provider (ISP) can legally look into the files and stop the sharing flow in such cases).

Byung-Chul Han writes that the Pirate Party is an antiparty. It is a transparency party, a colourless party of ‘opinion’--lacking a narrative. The party depoliticised politics—moving towards the post-political. In this context, politics is transformed into simply a matter of administering social needs. The socio-economic relations are thus maintained and perpetuated (Han, 2015a). Thus, digital, ‘real-time’ democracy is nothing but an illusion that in effect undermines the democratic process, and is built on the premise of a responsible collective. What is at stake instead is nothing but a ‘digital swarm’ far from being a responsible collective—a depoliticised consumer cattle trained by smart influencers. The smartphone subjugates, it is a mobile shop window, way far from being a mobile parliament (Han, 2022).

The Pirate Party (also known as the Piratpartiet) was established in 2006 in Sweden. It then spread into other countries, with Pirate Parties International (PPI) established in 2010, in Belgium (BBC, 2011). It included parties in more than 40 countries, with parliament members in some of these countries (Piratpartiet, website). In May 2006 the Swedish police raided the Pirate Bay and seized the servers of the Piratbyran (the owner of the pirate bay at the time, a Swedish anti-copyright organisation), leading to a shutdown of the website for three days. The growth and the popularity of the party dramatically increased in response to the raid. The raid was ensued by many street protests and assumed international attention (Li, 2009). The raid, and later trials of the owners of the Pirate Bay, were in part a result of the pressure from the United States and the lobbying of the international branch of the Motion Picture Association of America (MPAA) (ibid.).

The Piratbyran (the Piracy Bureau) emerged in 2003 from within the Swedish hacker scene and the integrated Internet Radio broadcasting community (ibid.). In late 2003, the Pirate Bay was created as an anti-copyright, non-profit P2P file-sharing website. In 2009 the Pirate Party’s principal political goals included: “fundamentally reform[ing] copyright law, get rid of the patent system, and . . . [ensuring] . . . that citizens’ rights to privacy are respected.” (Piratpartiet, The Pirate Party Overview, in Li 2009, 289 fn60).

The Pirate Bay and Pirate Party present important cases in the scene of technologist resistance. On their website they state that “Where others use technological

development to control, exploit and divide, we use it to build community, spread knowledge, enable innovation and create quality of life.” (Piratpartiet, website). The party makes clear its faith in technology and its ability to make significant change, for “an open, free and democratic society with freedom of thought and expression and the opportunity for everyone to share and share knowledge and culture”(ibid.). In their Principiprogram (Programme of principles<sup>11</sup>) they start the document stating that “*digitalisation changes everything*”, and as such the party is “born out of the desire to use technological development to improve society, based on libertarian, compassionate values. We are a movement that understands that digitalization changes the conditions and opportunities of politics (Piratpartiet, 2021; emphasis added).

It is this faith in technology which alarms Han, in relation to democracy and freedom. His brief dismissal of the Party as an effective means for democracy stems from his understanding of the party in terms of psychopolitics and as part of the information regime. However, technologist resistance has proven itself important in the contemporary digital era and has led to different positive outcomes. Thus, there emerges a dilemma at the heart of this approach to countering surveillance. At once they are an intimate part of infocracy which they seek to oppose and disrupt, yet at the same time they have been a disturbing force that significantly caused ameliorative outcomes. At times they have reinforced power relations of domination. At other times they have been an emancipatory force.

Resisting surveillance takes a multiplicity of forms, and is initiated with a variety of approaches. One approach to counter-surveillance is *technologist* counter-surveillance. It is the belief in and the utilisation of the technologies of surveillance with the aim to counter the information regime and to prevent its harmful consequences. Technologist counter-surveillance refers to the strategy that emphasises the importance and the emancipatory potential of digital technology as the principal means and strategy of resistance against the information regime. It shapes the tactics, modes and forms of resistance, around the imperative of

---

<sup>11</sup> The document is only available in Swedish, and has been translated with machine translation.

developing novel technological tools or altering/obfuscating existing ones. This approach revolves around technology. It seeks to use the tools of the information regime against the regime itself.

Furthermore, it assumes different characters, with a diverse collection of actors ranging from technology experts, journalists, and capitalists. Examples of technologist counter-surveillance are numerous and varying, and its applications are used by a cohort of individuals and collectives. Salient examples include the Cypherbunks, who advocated and developed technologies, primarily Strong Encryption as the central means for countering surveillance. +KAOS is another example which focuses on the development of alternative data infrastructures to counter the dominant data infrastructures in the information regime. Technologist resistance includes many smaller initiatives and projects that seek to directly counter surveillance by developing various software, like the open-source InformaCam. InformaCam provides users with the ability to control meta-data attached to their visual contents before sharing them, thus obstructing surveillance and data mining attempts through shared footage. Moreover, it has faith in technology in terms of developing software technologies, but also in terms of developing hardware tools, like open-source 3D printed gadgets or open-source personal computers, from which devices that usually collect data are removed or adjusted.

In contrast to ‘technical counter-surveillance,’ there are also a number of other strategies, including ‘artistic counter-surveillance’ where works of art are adopted as the principal means of countering surveillance in order to disrupt the ‘police order’ of surveillance. In addition, ‘pedagogical counter-surveillance’ emphasises the educational element and increasing awareness. Moreover, ‘legal counter-surveillance’ counts on the power of law to limit the harmful impact of these technologies of surveillance and to instate justice and equality.

Indeed, the history of information and digital technologies shows that ‘technologist resistance’ has a longer tradition, which can be traced back historically, which develops at each point when a new information technology is developed and applied. However, the emergence of the information regime, with unprecedented

developments in data infrastructures and advanced algorithms has allowed this strategy of technologist resistance to grow both in breadth and depth, while its ideological assumptions, tactics and modes are adopted at a large scale globally.

The continued influence of the Cypherpunks, within the context of the crypto-wars, is one reason for the selection of the group as a case study. According to Beltramini (2021), the Cypherpunks are “perhaps the single most effective grassroots organization in history dedicated to protecting freedom in cyberspace” (101). This ideology or vision, albeit in different variations, continues to exert significant influence on contemporary initiatives, discourses and imaginaries about AI, Big Data, and computer technology in general, by those carrying the flags of different contesting “Frontiers”, or “Revolutions.” Moreover, the Californian ideology exerted influence beyond the United States reaching other geographies in Western Europe and Asia, appealing to the digerati of the virtual class there, who were in fact closer to their Californian peers than to the working classes in their societies. This is so despite the fact that the ideology was a result of a particular group of people with particular socioeconomic environment and within a particular technological context.

Another important reason is the fact that the group is American in its approach. It is important to investigate Technologist counter surveillance from within this hegemonic context. According to Barbrook & Cameron (2001), the Californian ideology has flourished at a critical juncture of historical, economic and technological developments in the context of the emerging information society and information economies in the US and without any rivals capable of countering the narrative of its proponents. “At this crucial juncture, a loose alliance of writers, hackers, capitalists, and artists from the West Coast of the United States have succeeded in defining a heterogeneous orthodoxy for the coming information age—the Californian Ideology” (365).

Moreover, and more relevant to the topic of this thesis, is the Technologist approach of the movement, against the surveillance regime—Emphasizing repeatedly that the effective solution is the use and developing of technology (especially strong cryptography), not law or legal solutions (unlike, for example legal approaches of

counter-surveillance). The Cypherpunks ‘write code’ and this code is what shapes their strategy, tactics and discourse for countering the information regime of technological authoritarianism. As such they are a proper case to investigate the dilemma stated above, in light of the relationship between the Cypherpunk, as a technologist counter-surveillance, on one hand, and the technologist information regime they attempt to dismantle. The language and the imagination of the Cypherpunks reveal an intimate relationship with that of their rivals in the digital paradigm, despite their opting to “turn [the technology] on the likes of its paymasters” (Assange 2006, 02). Moreover, the Cypherpunks are accused of complacency, that is deeply rooted in, and not just a by-product of the line of thought and the temperament they possess (Barbrook & Cameron, 2001). Moreover, the vision of the Cypherpunks is full of tensions and self-contradictions—including, the tension between individualism and collectivism, tensions between contesting ideological positions and world view, as well as conflating aspirations.

The following discussion seeks to demonstrate that the Cypherpunks as a technologist counter surveillance movement is a complex and amorphous phenomenon. It takes place *within* the information regime it tries to counter. It fosters the illusion of freedom on the basis of technology and shares similar positions with digital rationality. Moreover, it reinforces the logic of gamification of life and operates as a swarm rather than a collective. Yet at the same time, the Cypherpunks seek to counter the imaginaries of the information regime about the free circulation of information by emphasising privacy, and establishing a distinction between the powerful vis a vis the weak in relation to privacy. Moreover, the critique and action of the Cypherpunk targets the structures of power in a holistic way—yet, not an effective way, due to these characteristics. It does so through the lens of the imperatives and dynamics of psychopolitics, as discussed in the previous chapter.

#### **4.1. The Cypherpunks: A Technologist Movement of Counter-Surveillance**

One hundred and forty years after the famous first line of the ‘Communist Manifesto’, another haunting spectre is announced to the world. “A specter is haunting the modern world, the specter of crypto anarchy.” (May, 1988). In response

to requests from other Cypherpunks gathering somewhere in the Silicon Valley, in 1992, Timothy C. May (generally considered to be the brain of the Cypherpunk movement) published 'The Crypto Anarchist Manifesto', in the Cypherpunk mailing list; a manifesto which he had originally written in 1988. In it he foresees an inevitable total anonymity which will emerge because of the developments in strong cryptography, after the Second World War. It will transform the nature of governmental regulations and economic interactions. Eventually state and corporations interference in individual and economic life will become largely, if not at all, obsolete.

This was the motivating spirit and the core of the vision of the Cypherpunks. It is also shared by many groups and organisations that sprouted in the United States and beyond in that era—particularly in allied countries in Western Europe and Asia. This vision, albeit in different variations, continues to exert significant influence on contemporary initiatives, discourses and imaginaries about AI, Big Data, and computer technology in general, by those carrying the flags of different contesting “Frontiers”, or “Revolutions”. The Cypherpunks were founded in Silicon Valley in 1992 by Timothy C. May with Eric Hughes and John Gilmore. A group of 16 people started gathering every Saturday in an area in which tech start-ups were operating. After a short while they created a mailing list— an unmoderated, free, and anonymous list. In a few years the mailing list became global with hundreds of participants.

According to Jarvis (2021a), the Cypherpunks envisioned four strategic goals. The first goal concerns free access to cryptographic technologies for citizens. This is base for their other goals, the second of which concerns anonymous communication. The third objective emphasises the freedom to conduct anonymous economic interactions without interference by government. Finally, whistleblowing and leaking platforms should be developed as a means to reduce the state's power. These objectives might be summed up in the following statement by Appelbaum (in Assange et al., 2021): “What the Cypherpunks wanted to do was to create systems that allow us to compensate each other in a truly free way where it is not possible to interfere” (in Assange, 2012, 91).

Fast forward into the future, an important issue has gained much media coverage and shocked the foundations of some governments around the world—whistleblowing. Whistleblowing refers to an event in which an insider to a public or private organisation exposes unethical, illegal or fraudulent activities of that organisation. Despite precedents in history whistleblowing in the digital world took a new turn and exerted unprecedented reach, volume and impact. Whistleblowing was on the agenda of the Cypherpunks since their early days as an important strategy of resistance against technological authoritarianism.

On July 24th 2024, Julian Assange, the renowned founder of the famous whistleblowing platform Wikileaks and a Cypherpunk, was released from the high-security prison of Belmarsh in the United Kingdom, after years of legal battles in Sweden, the UK, and the USA. The impact of Wikileaks, since its first publication in December 2006, was most likely unprecedented in history. The most significant leaks of the platform included: ‘Collateral Murder’ in April 2010, featuring a classified video of the US army killing 12 civilians in Baghdad, including 2 journalists, with 2 injured children. The footage was a scandal, and shortly after, Chelsea Manning was court martialed for leaking the video. In the same year Wikileaks published the Afghan War Logs (in July), as well as the Iraq War Logs (in October), exposing American war crimes in both countries, in addition to Cablegate (in November) with millions of diplomatic cables of the US since 1966. Many other leaks were perhaps even more significant in terms of intelligence and security, including Vault 7 (beginning in March 2017; considered the largest leak of CIA documents in history and exposing the agency’s cyber warfare and digital surveillance) as well as the Spy Files Russia (beginning in September 2017, containing hundreds of thousands of documents on surveillance and private contractors) (Ali & Kunstler, 2019).

A long-established idea among the Cypherpunks is that technology will (potentially) facilitate a constant, grandiose stream of leaking and whistleblowing. As such, this is not a new idea, for those in, or influenced by the Cypherpunks. It was a desirable and essential strategy of the Cypherpunks, towards their objective of weakening the state as well as the corporate economy—particularly in relation to their interference in

individual life and economic interaction among individuals. Strong encryption technologies and anonymous systems should be developed partly to encourage and facilitate such leaks from within these organisational structures. Strong Cryptography acts as an assurance for insiders against being exposed or becoming the object of retaliation by the organisation. Furthermore, it is partly an important strategy to obtain reliable knowledge of these institutions—which is necessary for countering and resisting the technological authoritarianism, which they constitute.

About the time of publishing the first leak, in December, Assange (2006a) published his ‘Conspiracy as Governance,’ in December 2006. In this text, he puts forth a conception of governance as conspiracy. A conspiracy, according to him, is greater than the sum of its individual conspirators, who are connected together with links of different levels of importance<sup>12</sup>. The conspiracy is “the primary planning methodology behind maintaining or strengthening authoritarian power” (02). Conspiracy is both a functional and cognitive device. The aim, for a resisting agent, is to cleave or throttle it ad infinitum to reduce its ‘total conspiratorial power.’ Alternatively, it should be deceived and blinded so as to distort its outcome—the outcome also being the next action of the conspiracy. Thus, understanding the structure of conspiracy is necessary to that end, and needs to be discovered by various means—which would also induce further resistance. The target is to disable the ‘conspiratorial cognitive abilities.’

In relation to this text, in an exchange on his website later that month (2006b), Assange asks his interlocutors to think about the effects of leaks. The more secretive an organisation, the higher the cognitive ‘secrecy tax’ it will have to pay in cases of leaks—in terms of fears and paranoia, particularly by high-ranking officials. This would lead to ‘consequent system-wide cognitive decline resulting in decreased ability to hold onto power as the environment demands adaption’ (2006b). This is the result since, according to Assange, ‘[a]n authoritarian conspiracy that cannot think is powerless to preserve itself against the opponents it induces’ (2006a, 05). In line

---

<sup>12</sup> The simile is akin to the language used to describe neural networks algorithms of AI. Some parts of his texts are written in a style akin to that of some mathematical or Computer Science texts. This is not strange, because the imaginaries of the Cypherpunks are dominantly drawn from technological imaginaries.

with the legacy and the vision of the Cypherpunks, he adds: “Hence in a world where leaking is easy, secretive or unjust systems are non-linearly hit relative to open, just systems. Since unjust systems, by their nature induce opponents, and in many places barely have the upper hand, mass leaking leaves them exquisitely vulnerable to those who seek to replace them with more open forms of governance” (2006b, n.d.). This is an essential strategy for the Cypherpunks in order to realise their objectives.

As an original contributor to the Cypherpunk mailing list, Assange’s ideas are in line with the general vision, *modus operandi* and imaginary of the group; although for some he represents a change in the character and image of the Cypherpunk from the resistant to the subversive (Beltramini, 2021). Timothy C. May proposed the use of Cryptographic technology for whistleblowing as early as 1988, and spoke of it as a principal application of cryptographic tools. He encouraged the establishment of different whistleblowing platforms from early on—which led to the establishment of the platform ‘alt.whistleblowers.’

Moreover, for the Cypherpunks, whistleblowing is an essential tactic in the strategy of ‘Diffusion, Confusion, and Refusion,’ deployed against technological authoritarianism. It is a process of resistance accomplished by deploying cryptographic technologies at a large scale by the majority of people. This is to be intertwined with other tactics like fake religions, whistleblowing communities, which is meant to be an antidote for shutting down this alternative, dispersed system. The expositions of whistleblowing should be dispersed among other activities—including eliciting media attention, as an element for spreading awareness. Whistleblowing should be encouraged and reinforced in this manner to be effectively “helping to undermine the state by using whistleblowers and anonymous information markets to leak information” (May, 1994a, n.d.).

Moreover, Whistleblowing is an essential part in the strategy for the ideal open society which will become possible (and inevitable) in the digital age. The ideal driving this society is the motto “privacy for the weak, transparency for the powerful.” (Assange et al., 2012, 07). Privacy, for the Cypherpunks, is understood as ‘the power to selectively reveal oneself to the world’ (Hughes, 1993, n.d.). People

can retain memories of their interactions while revealing as little as possible at their will. This is antithetical to a system of surveillance, where one must always reveal themselves. In other words, it is antithetical to the transparency imperative of the information regime. In this open society, one cannot, and should not “expect governments, corporations, or other large, *faceless* organizations to grant us privacy out of their beneficence” (Hughes, 1993, n.d.; emphasis added). “An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy” (Hughes, 1993, n.d.).

Moreover, the idea of dispersion is central to the vision of the Cypherpunks. It is a theme in opposition to which they envision ‘technocracy’ or technocratic totalitarianism (Beltramini, 2021) as a centralised, hierarchical system. It is, importantly, the architecture and the shape of the technological system that is to be created by the Cypherpunks as well as the desired crypto-anarchist society. In the words of May, “Cypherpunks know that a widely dispersed system can't be shut down.” (May, 1994a, n.d.). This is mainly a reiteration of Hughes’ (1993) words in his “A Cypherpunks Manifesto”. In this manifesto, Hughes stresses the indestructibility of software that is capable of moving beyond borders and jurisdictions. Such a system is powerful because it is so widely distributed freely among individuals and software developers, who further develop the capabilities of the software. Essentially, the Cypherpunks ‘write code’ (although that’s not all they do) and they publish it for all to use and play with it.

Privacy can be effectively applied only if everyone is using strong cryptographic technologies and is equipped with the minimum knowledge about using them. In a crypto-anarchist society “*everyone* should learn enough to at least vaguely understand how ‘blinding’ [the surveillance regime] works” (May, 1994a, n.d.; emphasis added). This concept animates many of the technologies developed or advocated for by the Cypherpunks, like Blockchain and Onion Routing technologies as well as cyber virtual communities; to mention a few examples. Indeed, central to the Cypherpunks is an antagonism towards hierarchies and a quest for a decentralised society, but here the element of dispersion becomes a mode of resistance and

struggle, as part of the strategy of “Diffusion, confusion, and refusion” (May, 1994a, n.d.). Dispersion is necessary for a truly decentralised society.

These elements take place together in a holistic manner, and are informed by the technological imaginaries of the Cypherpunks. The mind of the Cypherpunk understands social and political realities in terms of networks, algorithms and imaginaries drawn from science fiction. That is the imaginary of that era since, at least, the rise of cybernetics and the digital paradigm. Yet the Cypherpunks opt for cryptographic weapons as a means to “turn [the technology] on the likes of its paymasters” (Assange 2006a, 02). As could be seen in the works of Assange, for example, (2006a; 2006b; Assange et al. 2012), it is a system with “[a] vast connected network of industries, insiders and cronies.” (2012, 4), that can be depicted as a ‘connected graph’, in different shapes and formulations, with links each of which has its own *weight*, or importance, that carry information through this large cognitive network-device. May (1994b), as another example, considers the issue of surveillance and network visibility in terms of nodes and the links between those nodes, with ‘chemistries’ or ‘algebras’ that shape the transparency and opaqueness of these links and nodes in different states. For instance, in a police state, the nodes and the links in the network between them and between individuals are always transparent for the powerful. This has been a sustained theme/idea through the different generations of the Cypherpunks.

Another prominent issue in the contemporary world is Bitcoin and other cryptocurrencies. These issues in particular raise questions about the visions and claims of the Cypherpunks. Digital cash has always been on the agenda of the Cypherpunks since the beginning. The ability to conduct anonymous economic transactions is one of the primary four objectives of the Cypherpunks; as identified by Jarvis (2021a). Bitcoin tackles a number of issues that are central to their world-view of the Cypherpunks such as anonymity and decentralisation.

The problem of digital cash goes back to the 1980s, pioneered by David Chaum, who developed the first digital monetary systems. Unlike digital currencies developed by Chaum, bitcoin is a decentralised currency. The systems developed by Chaum, while

providing complete anonymity for individuals and their transactions, were centralised. Bitcoin on the other hand is a distributed currency system. It is a hybrid system where the account holders are anonymous while the transactions are completely public. It is a system in which trust is distributed and in which enforcement is not descending from a regulating body. Trust and enforcement emerge from mathematics and technology—through the difficulty of cryptographic computation required for creating a bitcoin and for making sure a transaction has been completed, in which every part of the network is engaged as a manner of proof (Assange, in Assange et al., 2012). Moreover, it is more of a commodity, according to Appelbaum (in Assange et al., 2012), the value of which is determined by the involved people themselves.

In other words and “in non-technical terms, it’s a way for me to send Julian currency and for Julian to confirm it without Andy really being able to interfere or to stop it” (Appelbaum, in Assange et al., 2012, 97). As to anonymity, Bitcoin is not as anonymous as should be, despite the hybridity spoken of by Assange. However, according to Cypherpunks, such issues can be overcome with the help of other technologies like Onion Routing, for anonymous access to the internet and technologies like TOR, which makes onion routing more accessible to a wider group of users. All in all, in the words of Muller-Maguhn (in Assange et al., 2012) “Bitcoin was the most successful attempt to introduce a digital currency for the last ten years” (Muller-Maguhn, in Assange et al., 2012, 99) and it is a step in the right direction in relation to privacy, for which only the wealthy can afford to pay, under current conditions of mass surveillance (Appelbaum, in Assange 2012, 100).

These positions can be challenged nowadays, bearing in mind the growth Bitcoin has witnessed, the legal regulations that sprouted around it, as well the proliferation not only of Cryptocurrencies but of also Blockchain platforms, like Ethereum, which allows for further proliferation of cryptocurrencies with facility and wider accessibility. But this is how the Cypherpunks view such technologies of digital cash and cryptocurrencies. Furthermore, for the Cypherpunks the emergence of underground economies is both inevitable and desirable. Such a system would work as an antidote to the state’s will of raising taxes and would act as a haven for tax

evasion where money could escape the grip of the state, after a certain threshold in the advancement of such technologies (Ludlow, 2001); itself pretty much as inevitable and desirable as crypto-anarchy in general.

Taxation is indeed a significant concern for crypto-anarchists, with tax evasion deemed an effective strategy to get rid of the state—or at least for minimising state interference in economic interactions. Moreover, digital cash with strong cryptography, for example, as ‘credentials without identity’, can potentially inhibit the emergence of a surveillance regime. These positions have been challenged since the early days of their proposition. For example, Denning (1996, 2001) warns against crypto-anarchy as an international threat, as a haven for global criminals and terrorists, that demands an international approach. According to her, the prospects of a state of crypto-anarchy is not only inevitable, but also unlikely. This is mainly due to the capabilities of states and resourceful companies to break the ciphers based on strong encryption algorithms. The inevitability and desirability of digital cash and crypto-anarchy are but delusions of the Cypherpunks.

These issues are at the core of most of the initiatives and movements which concerned themselves with the issue of cryptography in relation to governance and control. They are proposed, among others, as the solutions to the system of technocracy that the early generations of Cypherpunks feared and which the later generations of Cypherpunks witnessed taking control of all aspects of social, political and economic life. They witnessed the emergence of strong cryptographic technologies on the internet, in addition to virtual communities emerging with it. They conceived of these as tools for and of an increased surveillance regime, with tentacles reaching everywhere rendering privacy obsolete. They saw an illiberal path taking place emerging out of modernisation, turning into technocracy (Beltramini, 2021).

According to Beltramini (2021), the Cypherpunks understood a shift in the regime of power that emerged with the digital paradigm. Unlike old authoritarianism where power is abused, technocratic authoritarianism is manipulative and imperceptible. At the heart of technocracy is an apparatus which is the reverse of the panopticon. Their

response was an emphasis on the necessity of the development of strong cryptographic tools for secure communication and economic interaction to avoid surveillance and interference from governments (Beltramini, 2021).

The Cypherpunks, thus, have a holistic approach to counter surveillance. They envision a system of technological authoritarianism operating as a system of control through surveillance. They aimed at countering it through technology, by blinding and disturbing this information regime. Moreover, they sought to develop an alternative regime, using digital technologies—emphasising decentralisation and autonomy of the individual.

The Cypherpunks offer a significant critique of the information regime in relation to the transformation in the nature of power. Power in the era of technological authoritarianism (or the information regime) has become subtle and manipulative—in contrast to earlier forms of authoritarianism. This is an element in which the Cypherpunks as a technologist movement distinct itself from the mainstream of technological euphoria which accompanied the digital turn—the new Enlightenment. Unlike dataism or mainstream cybernetics, the Cypherpunk detected and criticized an authoritarian trend emerging along with the digital paradigm. This criticism locates it in opposition to the information regime as a resistance force with an emancipatory potential.

Moreover, the Cypherpunks make an important distinction in relation to one of the main imperatives of the psychopolitical regime of control—namely the transparency imperative. Transparency is the compulsion to self-expose, enacted upon the individual by the various mechanisms of neoliberal psychopolitics. Privacy here becomes obsolete and undesirable for capital as it hinders productivity and efficiency. Through the development of Strong Cryptographic technologies, and the advocacy for a widespread adoption of cryptographic knowledge and utilization, they stand in direct opposition to the Transparency regime and the information regime. In addition, they make an important distinction between the objects of transparency and the object of privacy, through a lens that acknowledges and seeks to emphasise the power asymmetry present in this regime of control. This distinction is summed up in

the motto “privacy for the weak, transparency for the powerful”—which runs through and forms a basis for the vision of the cyberpunks.

Nevertheless, the vision of the Cypherpunks proved to be an illusion—to say the least. For one thing, Bitcoin has developed in a direction opposite to decentralisation towards a total centralisation. The value of a bitcoin is far from being determined by the people, and the already resourceful have the advantage to mine cryptocurrency. Similarly, a new business model has emerged around whistleblowing, with some companies making profit by encouraging insiders to become whistleblowers. Despite having a rather holistic vision, the Cypherpunks lack the ability to effect a change in the power relation in an efficacious manner.

#### **4.2. The Cypherpunks: A Force for the Information Regime**

The idea of liberty and freedom is at the core of the Cypherpunk worldview. However, freedom is a contested concept and is conceived differently within the group. This is to do with the fact that the Cypherpunk comprised individuals adhering to a variety of political and ideological backgrounds—including radical libertarians, socialists and anarcho-capitalists. Moreover, the group brought together a variety of professional backgrounds—including academics, crypto-anarchists and even industry professionals, along with journalists and lawyers (Jarvis, 2021b). Nevertheless, members of the group, generally, identify themselves as crypto-anarchists, a crypto form of anarcho-capitalism. According to Timothy C. May, in 1993, around 50% identified themselves as “strongly libertarian/anarchist”. An additional 20% were leftists or liberal, and the political background positions of the remaining 30% was unknown (Jarvis, 2021b). A sample analysis of the Cypherpunks Mailing list shows that the most participating members were libertarians (Jarvis, 2021a). Furthermore, the general academic position on the political orientation of the Cypherpunks affirms that they are generally libertarian. The first association between the Cypherpunks and libertarianism, especially that of crypto-libertarianism in particular, was through WIRED technology magazine with the cover of its second issue in 1993.

As such a plausible entry point to understand the Cypherpunks is around the concept of freedom. Beltramini (2021) challenges this established position, which states that the Cypherpunks were libertarians. Rather, he proposes that the Cypherpunks were a group and a movement which was first and foremost against the regime of technocracy (technocratic authoritarianism) and the emerging 'reverse panopticon' of mass and omnipresent surveillance. While they can be read as taking a position closer to the libertarian ideas of Noam Chomsky, they can equally be read as following the ideas proposed by Michel Foucault. Their documents and statements share elements that allow them to be positioned on either camp. Beltramini writes: "if freedom is the freedom to shape one's identity, as an attribute of humanity itself, then freedom means to choose his/her own identity, and the cypherpunks behind the progress of distributed technologies were libertarians. If freedom, however, is far from being a condition that makes humans human, rather a highly fragile construction, they were not libertarians after all." (103). Furthermore, he points to statements by May, in a private conversation, that the latter was influenced by the works of Foucault.

Rather than revolving around freedom, the central struggle of the Cypherpunks was around the "crises of freedom". In other words, the problem for crypto-anarchists was not the state itself, as would anarchists or libertarians generally argue. Rather the problem is with the becoming of the state as an apparatus within an extensive network of social control and domination. The state is problematic only to the extent it interferes in the private life of individuals and in the economic interactions between them. The implementation of the state is the problem rather than the state itself. The problem for the cyberpunks is not a political position against the state per se.

Moreover, under such a crisis of freedom with irremediable democracy and corrupted capitalism, technology rather than law is the tool to which people should resort to protect their privacy and freedom. Nevertheless, this condition is not due to an innate nature of the democratic system, but due to its being broken, which is a necessary consequence resulting from the trajectory of modernisation, or the societies of affluence and post-industrialism.

It is here, according to Beltramini, that anarchy becomes relevant to cyberspace. It is in the light of this deviation against democracy and capitalism, that the autonomy of cyberspace is being declared. Furthermore, while the anarchism of the 1960s was a dreamy, utopian commune anarchism, the punks of San Francisco (the direct ancestor of the Cypherpunks and the geography where, according to him, the group was founded) became explicitly political anarchists, out of a "mix of nihilism and protest, anger and radicalism, disillusion and vitriol, scepticism and resistance and uncompromising opposition" (111).

Their antagonistic position was not only targeted against the neo-liberal technocratic authoritarianism but also against the previous generation, which the punks saw as complacent and cowardly. In relation to this point, Ludlow (2001), explains the reason why anarchy became of interest by the availability of cryptologic technologies, which allow for the perception of the possibility (or even the inevitability, for many Cypherpunks) of anarchist ideals. For instance, digital cash would challenge and undermine the distribution of power and its centres, because enough taxation money (i.e. the nutrition of the state) would eventually escape the net of the state, or would allow the abolishment of the effective monopoly by large corporations. However, in this context, it is important to note that the association between anarchism and the Cypherpunks might be due to the fact that anarchism itself lacks a unitary definition, usually conceived by its proponents as an ethical stand point (Franks et al., 2018). This might also be due to a misconception that the central theme of anarchism is the rejection of state (Amster, 2018) or that liberty is the determining value of anarchist political philosophy (May, 2008). As such, the status of the Cypherpunks as anarchist or libertarian is questionable and should be seen from a different perspective, pertinent to the context within which it emerged.

It is important to point out that the Cypherpunks within this trajectory of the 'crisis of freedom' that goes back to the mid-20<sup>th</sup> century, which led to the rise of the Cypherpunks and which also explains the intellectual lineage of the Cypherpunks. This can be traced back to the problem with modernity. The emergence of the Cypherpunks took place at a juncture under the influences of and convergences and divergences with the Free Speech movement, the student protests counterculture of

the 1960s, with prevalent anti-conformist sentiments, and lastly with the Punks in general, in the San Francisco Bay Area. These share with the Cypherpunks the scepticism of modernisation and the fear of the emerging technological regime of control (Beltramin, 2021). This line of action and (vernacular) ideologies is important to understand the contemporary scene of social movements as related to the digital paradigm or using it, as many contemporary ideas present globally, arguably, draw from that time in the digital era.

Jarvis (2021a) makes a critique of Beltramin's account that there is little evidence to account that the latter gives. In other words, for Jarvis, it is not about the crisis of freedom as Beltramin contends, but about freedom itself. The Cypherpunks were primarily libertarianism, as seen through the sample writings of the individuals of high impact, the typical cases. Moreover, it consisted of some elements of anarchism as well, due to the societal disaffiliation inherited from the counterculture. Their objective was to minimise the role of the state or remove it at all, and not to simply avoid the negative consequence of a course turned deviant. Jarvis points out that the Cypherpunks are drawing from a number of sources of influence that shape the way they operate and think. Politically they are influenced by libertarianism and anarchism. Two other sources of influence are counterculture, with its anti-war stance and protest politics, as well the hacker culture, especially the hacker ethics as written by Loyd Blankenship in 'The Conscious of a Hacker' also known as the 'Hacker Manifesto', published in 1994. Moreover, science fiction literature and cinema of the cyberpunks played a constituting role in shaping the politics, the ideology and the imaginaries of the Cypherpunk movement (Jarvis, 2021a). Indeed, Cypherpunk documents and statements are redolent of allusion and direct referencing to Cyberpunk literature. One example is the seminal essay by May (1994b) in which he states that the called-for combination of strong encryption and virtual community was firstly introduced in cyberpunk science fiction.

Hellegren (2017) makes an important point on the nature of the relationship the Cypherpunks and other crypto (i.e. encryption) discourse communities had with freedom, particularly that of *Internet* freedom. According to her, the crypto-discourse in general emphasises a negative concept of freedom. This negative conception of

freedom removes the responsibility from states and lays it on the shoulders of individuals—if they wish to protect themselves from surveillance and technocratic authoritarianism and to practice their freedom of speech online. This stance, according to Coleman & Golub (2008) is rooted in the liberalism found in the United States. Furthermore, with crypto being a site of struggle where different discourse communities contest its meaning and try to fix a particular notion of crypto. In this way, they exclude positive conceptions of internet freedom and this deepens the democratic deficit. For Hellegren, the principal issue of the crypto wars and crypto discourse revolves around *internet* freedom in particular, which is a practice that shapes relevant public policy over time.

She provides a periodisation, which is important to understand the complexity and contingency of the Cypherpunks and the crypto-scene as a whole, and how it evolved throughout the years. The timeline consists of three periods: the origins, spanning between 1975 and 1990, the crystallisation starting from 1990 till the beginning of the new millennium, and the revitalisation between 2000 up until 2015. This timeline reflects changes in the dynamics of the relationship between the Cypherpunks, as a movement and an ideology, and the state. It also brings into question the relevance of the Cypherpunks' ideas in the light of the evolution of the cryptography scene. For example, Denning (2001) has pointed to the changes in the cryptographic scene in a comment on her criticism of crypto-anarchy, which she wrote in 1996, pointing to how states' capabilities have changed in such a short period of time. Indeed, the timeline demonstrates not only the complexity within a particular discourse community but also the overlapping and interrelatedness between ideas of these different communities (among which are cryptographers, hackers, online rights activists and technology journalists, in addition to states).

Under this light, Hellegren contends that Cypherpunks represent a community rather than an ideology. The unifying element, which makes the Cypherpunks as a community, is their belief that technology and the development of strong encryption technologies on cyberspace is the primary way for (internet) freedom. Nevertheless, “Crypto-advocates have over time emptied crypto of its particular meaning and filled it with multiple possible meanings that unite different political objectives through the

construction of a social antagonism” (Hellegren, 2017, 290). They are unified through their discursive practices governing the meaning-making processes with these communities. Moreover, so much as the state is concerned, “[t]he US Government had the historical upper hand when it came to defining the meaning of crypto, and did so in terms of war materiel.” According to Treuger (2019, in Beltramini, 2021), the internet has been domesticated by the state due to the state’s possession of resources and capabilities to shape technology, in its broader sense, in its quest towards social control. The states, thus, played an important role in destroying the emancipatory project envisioned around the internet since its early days. This role of the state can still be seen in relation to more recent digital developments, from data infrastructures and the development of advanced algorithms, to the control of social media platforms, throughout the globe.

For Coleman and Golub (2008) the internet is “a privileged site for projecting the aspirations of liberal society.” (270), in the context of which crypto-freedom is only one particular mode. It is a particular moral genre of hacking—along with Free/Open Source Software and the hacker underground. They engage and are all part and different manifestations of the liberal *‘expressive self’*. Liberalism here is “not as it is traditionally framed – as a coherent body of philosophical, economic and legal thought or a set of normative precepts and doctrines – but as a cultural sensibility closely wedded to what Charles Taylor has called the *‘expressive self’*” (256). Computer hacking is a location wherein liberalism is not only manifested but also a location wherein its commitments and critiques are articulated and transformed, though in technical idioms, in a dialogical and heterogeneous manner, with/as a set of historical, moral and cultural sensibilities. Moreover, there is no one hacker ethics, but rather multiple various ethics, with a number of different, though coherent articulations; “a constellation of shifting genres”. Here, ‘hacking [...] is in fact one crucial location whereby the fractured and cultural character of liberalism is given new life and visibility in the digital age.’ (258).

‘Crypto-freedom’ articulates particularly the liberal values of individual autonomy and freedom from government interference, using the language of cryptography, where (especially later with the Cypherpunks) self-reliance and self-control are

applied to the digital world. The Cypherpunks are a case that represents the general American liberal sensibility similar to those of De Tocqueville's gentleman farmers in a new idiom of cryptography—particularly in relation to their distrust of institutionalised authorities. Nevertheless, the suspicion they hold can equally be seen as within libertarian right as well as within the anti-military left pacifism (this brings up discussions of the 'Californian ideology' as the result of such a mix, discussed below).

However, it is on neither wing of the political spectrum. They do not adopt any clear political affiliation, and many think of their projects as continuation and affirmation of cultural and constitutional principles inherited from earlier times. Nevertheless, unlike the Free/Open Software mode, for example, they embraced a notion of negative freedom as absolute freedom that lacks the liberal elements of sharing and pedagogy, despite the latter's drawing on the same underlying liberal culture. This notwithstanding, there is an oscillation between negative and positive notions of freedom, in addition to a tension between individualism and collectivism—which are both tensions that can be traced back in the tradition of liberalism itself and its cultural context, particularly in relation to freedom.

In the case of crypto-freedom the realisation of the 'expressive self' is realised by 'writing code' (in the word of Hughes) that protects itself from surveillance. While Coleman and Golub assert the overlapping and interrelatedness of these three modes of hacking, and conceive them as variations and manifestations of the same long standing western 'expressive self', the similarities and interconnectedness might be even more than what they suggest, and the borders between these moral genres seem to be more blurred and porous. For example, the Cypherpunks have central elements of the underground—as was discussed in relation to the underground economies. In fact, they encourage the emergence of underground, illegal alternatives. Additionally, at the core of their movement is a free/open approach to software development—the Cypherpunks emphasise sharing software openly for others to develop it, in accordance with their principle of dispersion.

As such, the Cypherpunks propagate a sense of freedom that is within the psychopolitical information regime. They reinforce this logic of the entrepreneur

self/project. The individual is an autonomous being. A citizen and a consumer. She is resourceful and through technological tools and DIY projects, he can go beyond the confinements of the authoritarian institutions. In this sense, the individual is akin to the snake of the society of control, who can open up spaces beyond the enclosures of disciplines. They adopt and propagate a negative concept of freedom (Hellegren, 2017) which removes the responsibility from states and lays it on the shoulders of individuals if they wish to protect themselves from surveillance and technocratic authoritarianism and to practice their freedom of speech online. This negative concept of freedom operates in line with the imperatives of positivity, in the information regime. Positivity eradicates the negativity in reflection, it does not work through prohibition and repression, rather through seduction and encouragement. Here the individual is the sole responsible for achievement—he is an achievement-subject. She bears the responsibility to achieve and succeed. As such, again, he is an entrepreneur project, constantly re-molding and in continuous movement, as a ‘free’ subject. He, thus, adopts this ‘expressive self’ (Coleman & Golub, 2008), constantly self-exposing and self-illuminating. However, this happens more in accordance with the imperatives of the neoliberal information regime, rather than liberalism.

The Cypherpunks, thus, are, in this regard, located within the surveillance regime. They operate along the imperatives of the psychopolitical regime. They reinforce the logic of the master—while seeking to counter it using the master’s tools against it. They exacerbate the ‘crisis of freedom’ (as articulated by Han). They propagate the illusion of freedom while seeking to counter the logic of the regime that has created it. This is partly due to the shared premises and ideological assumptions that the Cypherpunks (being a technologist counter-surveillance) have in common with other technologist forces of the information regime. In the following discussion I will look into the Californian Ideology, from the context and ideology of which the Cypherpunks emerged.

This connectedness leads to the discussion of Californian Ideology. Cypherpunk and crypto-anarchy might be better understood if placed in the context of a particular subculture and ideology in the United States (or at least connected through it) rather than directly to the American context at large or being cast as anarchist or

libertarian—as they lack such ideological character. As was mentioned earlier, the first link between crypto-anarchism and libertarianism was first publicly established in the second issue of the renowned WIRED technology-focused magazine. The cover of this issue (Issue 1.02 of May/June 1993) featured the founders of the Cypherpunks, Timothy C. May, Eric Hughes, and John Gilmore; masked and holding the flag of the US, with a text reading “Rebels with a Cause (Your Privacy)”. Twenty years later the cover of the 22.09 issue of Wired depicted Edward Snowden, the renowned whistleblower and contractor of the US National Security Agency (NSA). The Magazine was, using the words of Richard Barbrook and Andy Cameron, “the monthly bible of the ‘virtual class’” (2001, 368).

The Californian Ideology has dominated the technology scene in the United States and beyond. Advocated by the digerati (digital literati) and the virtual class. The Californian ideology is seen as a form of Nietzschean-libertarianism of tribalistic technopaganism, as a form of individualism that “would make Ayn Rand blush” (according to Purdy, 1998), a retrofuturism, a new Jeffersonian democracy (Barbrook & Cameron, 20001), and as a utopian fervour (Ludlow, 2001). The proponents of the Californian ideology included people like Kevin Kelly, Douglas Rushkoff, Lou Rossetto, and John Perry Barlow—also known as the digerati.

For the adherents of this ideology the advances in technology and biotechnology would allow life to move beyond the confines of evolution. Technology will make humanity superior. The avant-guards of such development are none but the digerati themselves, the collection of the boundless get-it-alone individuals, the ultra-individualists, who would ‘advance civilisation’ (Purdy, 1998). Furthermore, this vision can be traced back to the ideas of Ecosystems and cybernetics (Curtis, 2011). For the digerati, the truth hitherto hidden is that Life is nothing but a self-ordering and self-reproducing system, with feedback loops. In the language of Kevin Kelly, Life consists of vivisystems that are driven by an invisible hand with a spontaneous order; which should not be interfered with. Furthermore, now with the advances in genetic sciences, AI, and self-replicating computers and advanced algorithms, the line between the made and the natural is irreversibly blurred. Moreover, computers, like humans, are vivi-systems. The task of the digerati, and humanity at large, is to

facilitate and extend the passing of life to the new vivi-system, since out of all vivi-systems, only humans can create computers (Purdy, 1998).

According to Purdy's reading (1998), it is for this reason that the digerati are uninterested in politics and social life (except when it concerns their cyber interests), since after all these issues do not bear much significance, considering the larger picture of how things and life works and evolves; a position they confirmed in different occasions. Moreover, "[i]n place of counterproductive regulations, visionary engineers are inventing the tools needed to create a "free market" within cyberspace, such as encryption, digital money, and verification procedures" (Barbrook&Cameron, 2001, 369). According to Barbrook & Cameron (2001), at a critical juncture of historical, economic and technological developments in the context of the emerging information society and information economies, in the US, in addition to a lacking of any rivals capable of countering the narrative of its proponents, the Californian ideology has flourished. "At this crucial juncture, a loose alliance of writers, hackers, capitalists, and artists from the West Coast of the United States have succeeded in defining a heterogeneous orthodoxy for the coming information age—the Californian Ideology" (365).

Purdy (2001) contends that the digerati are post-human vitalists, the roots of which can be traced back to Nietzsche and romantic vitalism. The individualist, as portrayed by Wired, is the *supermensch* of Nietzsche. He is a boundless individual for whom laws, morals and community are meaningless and are worthy of contempt, and who would do or change things at will. "Wired is about the most powerful people on the planet today—the Digital Generation." (Wired's first issue, 1993, cited in Purdy, 1998). They despise government, preferring a spontaneous order (which is more akin to the invisible hand of free market). An order which is the self-organising and self-producing force similar to the Nietzschean will to power, that is the roaming force of life which brings order out of chaos. Moreover, they draw from romantic vitalism which overlooks the intricacies of life, with its political, economic, and social dilemmas and troubles, favouring the celebration of Life, as envisaged by them.

Moreover, the digerati are a tribe seeking comradeship among equals, and are wilfully ignorant and negligent of others. These others are, however, the groups who

are the most affected and harmed by the new technologies and discourses developed and advocated for by the digerati. In addition, theirs is just an adolescent temperament of overgrown boys with too much money, who are also wilfully ignoring the limitations of life, with their doctrines effusing through channels like the Wired magazine. It is a complacency that is deeply rooted in, and not just a by-product of the line of thought and the temperament of the digerati, leading the digerati to see new technologies as a new world, or vivi-system. It necessarily leads them to over-emphasise their assumptions and to assert them as universal, at the expense of other groups. Among such groups are data-entry workers, shop clerks and other labourers, for whom their labour and economic conditions will be of the same, with the same problems as before despite the advances of digital technologies. Moreover, the digerati are oblivious to the fact that their environment is largely run by white men and the doctrinal documents they produce are largely written by these white men, dominated by big technological corporations; leading them to such meaningless and undesirable grim utopias. For Purdy, theirs is a vitalistic picture of democracy, bordering on mysticism and enmeshed with intellectual pretence and delusions.

Barbrook & Cameron (2001) have a different vision of the Californian ideology and its ideologues, whom they call the ‘virtual class’. The Californian Ideology is a form of retrofuturism that seeks a Jeffersonian democracy, bringing back some of the most atavistic elements of the American culture, with a wilful negligence of the Other, all the while maintaining a pretence of being progressive. At that point in time, it had an irresistible lustre and appeal, influencing various groups of people. Moreover, the Californian ideology exerted influence beyond the United States reaching other geographies in Europe and Asia, appealing to the digerati of the virtual class there, who were in fact closer to their Californian peers than to the working classes in their societies. This is so despite the fact that the ideology was a result of a particular group of people with particular socioeconomic environment and within a particular technological context.

Set against the raid by the state on hippies occupying People’s Park in California, on May 15<sup>th</sup> 1969, Barbrook and Cameron look into the emergence of the ‘virtual class’

in the space between the New Left and the New Right in the United States. The virtual class are the skilled workers of the technological industry, they are “the techno-intelligentsia of cognitive scientists, engineers, computer scientists, video-game developers, and all the other communications specialists” (Kroker & Weinstein, 1994, cited in Barbrook & Cameron, 2001, 367). The radical hippies and the New Left combined political struggles and cultural rebellion, with some advocating the return to nature with many others believing in the potential lying within technological development for turning their ideals into social realities. Marshal McLuhan was an English professor who advocated for the idea that “the power of big business and big government would be imminently overthrown by the intrinsically empowering effects of new technology on individuals” (366). With the influence of McLuhan, they engaged in developing information technologies, which were imagined to be leading to ‘ecotopia’ where “cars had disappeared, industrial production was ecologically viable, sexual relationships were egalitarian, and daily life was lived in community groups.” (366). Moreover, an agora will emerge, through which direct democracy would become possible. All this was almost at hand.

On the other hand, in the 1990s, the New Right celebrated economic liberalism, with its liberated individuals within a market place, but the technological appeal was still retained. The new technological developments would lead to a free market rather than to an ecotopia. It would lead to individual freedom rather than the collective freedom of the hippies. In addition, McLuhan’s predictions were re-interpreted in various works of non-fiction and science fiction, like those of Asimov and Heinlein.

The information companies relied heavily on the virtual class, who were not suitable for the typical corporate hierarchy and organisation. As such, the high-tech artisans of the virtual class were employed with fixed-term contracts, and despite being well-paid and enjoying a level of autonomy they had no guarantee as to the future of their employment. The Californian Ideology reflects and explains their professional reality. The result was a bizarre and ambiguous mix of elements from the New Left and the New Right, that believes in and seeks to realize the utopias of both wings simultaneously and without any critical take. At one and the same time, advanced technologies would realise the electronic agora and replace big government and

corporate capitalism while empowering the individual to freely interact with the economy in the free market which will advance the progress of technology and lead to the Jeffersonian democracy. This self-contradicting position can only be made by a firm, positive technological determinism.

Furthermore, the appeal of this ideology and the fact that many people globally believe in it as a way for the future comes primarily from this ambiguity it harbours. In any case, the Californian ideology contradicts facts on the ground, as governmental policies subsidies and the culture of D.I.Y. (do it yourself) have, more than private enterprise, brought forward the development of computers and the Internet. The authors argue that they are indeed Jeffersonian by their creating technologies to mediate their interaction with the reality of labour, as did Jefferson with his slaves reducing his interaction with slaves through technology and various gadgets. They are Jeffersonian as well in the sense of advocating for progressive objectives while at the same time being engaged in the opposite of such claims; like owning plantations with hundreds of slaves while calling for the abolition of slavery. This utopian vision creates a new form of apartheid between the information-rich and the information-poor, and the virtual class opt for 'living' in the hyperreality of virtual communities, calling for further immersion in the cyberspatial world, reinforcing the impacts of their wilful blindness and dependence on the Other. While it is optimistic and emancipatory, it is also a pessimistic, repressive and atavistic vision of the future.

The Cypherpunks, thus reinforce the crisis of freedom, while attempting to counter the surveillance regime which caused it. The group does not operate in a manner leading to a collective action, capable of resulting in a political will to disturb the information regime as it claims to do. It operates more like a swarm. Despite persisting in terms of time, their reliance on digital communication, result in isolating the members of the group. They are digerati that are placed in a system that perpetuates their precarity, further isolating them. They are swarms operating and seeking a system of elitist equals. This tribalism is incapable of bringing up a collective will, a spirit that is necessary for a collective action. Moreover, they are within the information regime to the extent they adopt the imperatives of

behaviouralism, which dominates the Dataist worldview. In this worldview politics is relegated to a secondary position, not important considering the grand scheme of life. All can be optimised and made functional through the use of technology, which is the force to move life forward. Reflection, reasoning, and ‘freedom realised through the other’ become meaningless.

This being said, the oppositional characters of the Cypherpunks make them not outright Dataists. Their behaviouralist tendencies are mitigated by the libertarian influences they have. Moreover, the critique of the imperative of transparency they offer (through their conceptualisation of privacy and its locus in society), distinguishes it from the information regime, and mitigates their role in reinforcing the imperatives of the information regime. The Cypherpunks were capable of producing ameliorative outcomes, despite being ineffective in terms of bringing about a collective action against the surveillance regime.

### **4.3. Conclusion**

While the information regime has been a new form of control, it provided affordances for resistance against the same oppressive regime. One approach to counter surveillance relies on technologies of the information regime themselves as the strategy for resistance. Cypherpunks is such a movement of technologist counter surveillance. Through the lens of the imperatives and dynamics of psychopolitics, this chapter sought to demonstrate that the Cypherpunks as a technologist counter surveillance movement is a complex and amorphous phenomenon. It takes place ‘within’ the information regime it tries to counter. It fosters the illusion of freedom on the basis of technology and shares similar positions with digital rationality. Moreover, it reinforces the logic of gamification of life and operates as a swarm rather than a collective. Yet at the same time, the Cypherpunks seek to counter the imaginaries of the information regime about the free circulation of information by emphasising privacy, and establishing a distinction between the powerful vis a vis the weak in relation to privacy. Moreover, the critique and action of the Cypherpunk targets the structures of power in a holistic way—yet, not an effective way, due to these characteristics.

On one hand, a significant critique of the information regime by the Cypherpunks is that power in the era of technological authoritarianism has become subtle and manipulative. The Cypherpunk detected and criticized an authoritarian trend emerging along with the digital paradigm. Moreover, the Cypherpunks make an important distinction within one of the main imperatives to the psychopolitical regime of control—namely the transparency imperative. They emphasise privacy in opposition to transparency of neoliberal psychopolitics, through the development and advocacy of Strong Cryptography. This locates it in opposition to the information regime as a resistance force with an emancipatory potential.

On the other hand, the Cypherpunks propagate a sense of freedom that is within the psychopolitical information regime. They reinforce this logic of the entrepreneur self/project. The individual is an autonomous being. A citizen and a consumer. She is resourceful and through technological tools and DIY projects, he can go beyond the confinements of the authoritarian institutions. In this sense, the individual is akin to the snake of the society of control, who can open up spaces beyond the enclosures of disciplines. He bears the responsibility to prevent the harms of surveillance and the detriments of the information regime. As such they reinforce the logic of Positivity and the Achievement Society. The group does not operate in a manner that can potentially lead to a collective action, capable of resulting in a political will to disturb the information regime as it claims to do. It operates more like a swarm. Despite persisting in terms of time, their reliance on digital communication, result in isolating the members of the group. Their tribalism revolving around elitist equals, is incapable of bringing up a collective will, a spirit that is necessary for a collective action. In this worldview, like Dataism, politics is relegated to a secondary position, not important considering the grand scheme of life.

As such, the Cypherpunks are, in this regard, located within the surveillance regime. They operate along the imperatives of the psychopolitical regime. They reinforce the logic of the master—while seeking to counter it using the master's tools against it. They exacerbate the 'crisis of freedom' (as articulated by Han). They propagate the illusion of freedom while seeking to counter the logic of the regime that has created it. This is partly due to the shared premises and ideological assumptions that the

Cypherpunks (being a technologist counter-surveillance) have in common with other technologist forces of the information regime.

This being said, the oppositional characters of the Cypherpunks make them not outright Dataists or proponents of the information regime. Their behaviouralist tendencies are mitigated by the libertarian or anarchist influences they have. Moreover, the critique of the imperative of Transparency they offer (through their conceptualisation of privacy and its locus in society), distinguishes it from the information regime as an oppositional force, and mitigates their role in reinforcing the imperatives of the information regime, the outcomes produced by the Cypherpunks had an ameliorative impact on the current situation, yet they do not constitute a truly democratic moment—a truly questioning of and disturbance in the existing relations of power.

## CHAPTER 5

### CONCLUSION: THE TECHNOLOGIST COUNTER-SURVEILLANCE IN THE INFORMATION REGIME

Surveillance has intensified and became prevalent with the emergence of the digital era—especially, after the data revolution. Nowadays, advanced algorithms (including AI and its derivatives) and digital data infrastructures (including, Big Data and Small Data) govern all aspects of life. These technologies are essentially technologies of surveillance. It is the age of the information (surveillance) regime. It is a new form of domination in which the decisive influence on the social, political and economic fields is exerted by information—that is, through the collection, storing, and processing of data and information (Han, 2022). With it, novel forms of counter-surveillance come to being.

One form of counter-surveillance is technologist counter-surveillance. It emphasises the importance and the primacy of digital technology itself as the principal means and strategy of resistance against the information regime. Examples of technologist counter-surveillance are numerous and varying, and its applications are used by a cohort of individuals and collectives. Salient examples include the Cypherbunks, who advocated technology, primarily strong encryption, as the only means for resistance and developed various technologies to that end. +KAOS is another example focusing on developing alternative data infrastructures to counter the power and dominance of the data infrastructures of the information regime. In contrast to ‘technical counter-surveillance,’ there are a number of other strategies, including ‘artistic counter-surveillance’ where works of art are adopted as the principal means of countering surveillance in order to disrupt the ‘police order’ of surveillance. In addition, ‘pedagogical counter-surveillance’ emphasises the educational element and increasing awareness. Moreover, ‘legal counter-surveillance’ which believes in the

power of law to limit the harmful impact of these technologies of surveillance and to instate justice and equality.

There is a dilemma at the heart of the technologist approach to countering surveillance. They are an intimate part of the technologist information regime which they seek to oppose, yet at the same time they have been a disturbing force that significantly caused ameliorative outcomes, and has had a pivotal emancipatory role. At times, they have reinforced power relations of domination and at other times they have been forces of emancipation. This dilemma in relation to technologist counter-surveillance is the concern of this Thesis.

The thesis built on the analysis of the philosopher Byung-Chul Han. In particular, his work on psychopolitics and the Information regime. Han's analysis will be developed in detail in Chapter 3 of this thesis. Through the lens of the imperatives of psychopolitics and the Information regime, this thesis investigated the Cypherpunks as an exemplary case of technologist counter-surveillance, to understand the relationship between surveillance and counter-surveillance as they take place within the contemporary information regime. It argues that technologist Counter-surveillance takes place necessarily as a force for the information regime which it tries to counter. It is of a dual character, as both progressive and reactionary; disruptive of and reinforcing. Furthermore, as such, its efficacy in countering surveillance is limited to ameliorative impact, to the extent it is intimate with the regime it seeks to counter. The study will build on the following theoretical framework.

A significant critique of the information regime by the Cypherpunks is the transformation in the nature of power. Power in the era of technological authoritarianism (or the information regime) has become subtle and manipulative—in contrast to earlier forms of authoritarianism. This is an element in which the Cypherpunks as a technologist movement distinct itself from the mainstream of technological euphoria which accompanied the digital turn—the new Enlightenment. Unlike Dataism or cybernetics, the Cypherpunks detected and criticized an authoritarian trend emerging along with the digital paradigm. This criticism locates it

in opposition to the information regime as a resistance force with an emancipatory potential. Moreover, the Cypherpunks disturb a central psychopolitical imperative—that is, the compulsion for transparency. Transparency is the compulsion to self-expose, enacted upon the individual by the various mechanisms of neoliberal psychopolitics. Privacy here becomes obsolete and undesirable for capital as it hinders productivity and efficiency. Through the development of strong cryptographic technologies, and the advocacy for a widespread adoption of cryptographic knowledge and utilization, stand in direct opposition to the Transparency regime and the information regime.

The Cypherpunks propagate a sense of freedom that is within the psychopolitical information regime. They reinforce this logic of the entrepreneur self/project. The individual is an autonomous being. A citizen and a consumer. She is resourceful and through technological tools and DIY projects, he can go beyond the confinements of the authoritarian institutions. In this sense, the individual is akin to the snake of the society of control, who can open up spaces beyond the enclosures of disciplines. They adopt and propagate a negative concept of freedom (Hellegren, 2017) which removes the responsibility from states and lays it on the shoulders of individuals if they wish to protect themselves from surveillance and technocratic authoritarianism and to practice their freedom of speech online. This negative concept of freedom operates in line with psychopolitical imperatives of positivity, dominant in the information regime. Positivity eradicates the negativity in reflection, operating through seduction and encouragement, rather than prohibition and repression. Here the individual becomes the sole responsible for achievement and success—he is a project, an achievement-subject. She bears the responsibility to achieve and succeed. As such, again, he is an entrepreneur project, constantly re-molding and in continuous movement, as a ‘free’ subject. He, thus, adopts this ‘expressive self’ (Coleman & Golub, 2008), constantly self-exposing and self-illuminating. However, this happens more in accordance with the imperatives of the neoliberal information regime, rather than liberalism. The Cypherpunks thus are, in this regard, located within the surveillance regime. They operate along the imperatives of the psychopolitical regime. They reinforce the logic of the master—while seeking to counter it using the master’s tools against it. They exacerbate the ‘crisis of freedom’

(as articulated by Han). They propagate the illusion of freedom while seeking to counter the logic of the regime that has created it. This is partly due to the shared premises and ideological assumptions that the Cypherpunks (being a technologist counter-surveillance) have in common with other technologist forces of the information regime. In the following discussion I will look into the Californian Ideology, from the context and ideology of which the Cypherpunks emerged.

The Cypherpunks, thus reinforce the crisis of freedom, while attempting to counter the surveillance regime which caused it. The group does not operate in a manner leading to a collective action, capable of resulting in a political will to disturb the information regime as it claims to do. It operates more like a swarm. Despite persisting in terms of time, their reliance on digital communication, result in isolating the members of the group. They are digerati that are placed in a system that perpetuates their precarity, further isolating them. They are swarms operating and seeking a system of elitist equals. This tribalism is incapable of bringing up a collective will, a spirit that is necessary for a collective action. Moreover, they are part of the information regime to the extent they adopt the imperatives of behaviouralism, which dominates the Dataist worldview. In this worldview politics has a secondary position, irrelevant in the grand scheme of life. Everything should be constantly optimised through the use of technology, which is the force to bring the progress of life. Reflection, reasoning, and ‘freedom realised through the other’ become meaningless. This being said, the oppositional characters of the Cypherpunks make them not outright Dataists. Their behaviouralist tendencies are mitigated by the libertarian influences they have. Moreover, the critique of the imperative of Transparency they offer (through their conceptualisation of privacy and its locus in society), distinguishes it from the information regime, and mitigates their role in reinforcing the imperatives of the information regime.

The Cypherpunks are located within the surveillance regime. They operate along the imperatives of the psychopolitical regime. They reinforce the logic of the master—while seeking to counter it using the master’s tools against it. They exacerbate the ‘crisis of freedom’ (as articulated by Han). They propagate the illusion of freedom while seeking to counter the logic of the regime that has created it. This is partly due

to the shared premises and ideological assumptions that the Cypherpunks (being a technologist counter-surveillance) have in common with other technologist forces of the information regime. This being said, the oppositional characters of the Cypherpunks make them not outright Dataists or proponents of the information regime. Their behaviouralist tendencies are mitigated by the libertarian or anarchist influences they have. Moreover, the critique of the imperative of transparency they offer (through their conceptualisation of privacy and its locus in society), distinguishes it from the information regime as an oppositional force, and mitigates their role in reinforcing the imperatives of the information regime. As such, while incapable of effecting a collective action against the surveillance regime, the Cyberpunks throughout their history were capable of producing positive outcomes. Their outcomes had an ameliorative impact on the current situation, yet they do not constitute an instant of what Jacques Ranciere calls dissensus, a truly democratic moment—a truly questioning of and disturbance in the existing relations of power.

## REFERENCES

- Abu-Laban, Y. (2014a). Gendering Surveillance Studies: The Empirical and Normative Promise of Feminist Methodology. *Surveillance & Society*, 13(1), 44–56. <https://doi.org/10.24908/ss.v13i1.5163>
- Abu-Laban, Y. (2014b). Gendering Surveillance Studies: The Empirical and Normative Promise of Feminist Methodology. *Surveillance & Society*, 13(1), 44–56. <https://doi.org/10.24908/ss.v13i1.5163>
- Ali, N. M., Abdullah, S. Z., Salim, J., Sulaiman, R., Zaman, H. B., & Lee, H. (2012). Exploring user experience in game using heart rate device. *Asia-Pacific Journal of Information Technology and Multimedia*, 1(2), 28-36.
- Ali, T. & Kunstler, M. (2019). Chronology of Major Events. In Ali, Tariq & Kunstler, Margaret (eds.) (2019) *In Defense of Julian Assange* (pp. xxviii-xxxiv) OR Books. New York and London.
- Amster, R. (2018). Anti-Hierarchy. In Franks, B., Jun, N., & Williams, L. (Eds.). (2018). *Anarchism: a conceptual approach* (pp.14-27). Routledge.
- Andary, R. W., & Auza, A. (2025). Language, Emotion, And Algorithms: The Dynamics Of Communication In The Social Media Era. *Akrab Juara: Jurnal Ilmu-ilmu Sosial*, 10(3), 887-897.
- Anderson, C. (2008, June, 23). *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*. WIRED. <https://www.wired.com/2008/06/pb-theory/>

Aradau, C., & Blanke, T. (2017). Politics of prediction: Security and the time/space of governmentality in the age of big data. *European Journal of Social Theory*, 20(3), 373–391. <https://doi.org/10.1177/1368431016667623>

Assange J. et al. (2012) *Cypherpunk: Freedom and the Future of the Internet*. OR Books, New York and London.

Assange Julian (2006a). *Conspiracy as Governance*. [Online]. <https://estaticos.elmundo.es/documentos/2010/12/01/conspiracies.pdf>

Assange Julian (2006b December 31.) *The non linear effects of leaks on unjust systems of governance*. <https://web.archive.org/web/20071020051936/http://iq.org/#Thenonlineeffectsofleaksonunjustsystemsofgovernance>

Baaz, M., Lilja, M., Schulz, M., & Vinthagen, S. (2023). The ABC of resistance: towards a new analytical framework. *Journal of Political Power*, 16(1), 59-80.

Barakat, R. (2013). Criminals or Martyrs? British Colonial Legacy in Palestine and the Criminalization of Resistance. *Omran*, 2(6), 55-72.

Baranova, T. D. (2020). Print Wars in Europe during the Sixteenth Century. *Encyclopédie d'histoire numérique de l'Europe* [online]. <https://ehne.fr/en/node/12350>

Barbrook, R. & Cameron, A. (2001). Californian Ideology. In Ludlow, Peter (ed.) (2001) *Crypto Anarchy, Cyberstates, and Pirate Utopias* (363-387). The MIT Press. England.

Barry, L. (2019). The rationality of the digital governmentality. *Journal for Cultural Research*, 23(4), 365–380. <https://doi.org/10.1080/14797585.2020.1714878>

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. John Wiley & Sons.

BBC (2011) *Pirate Parties: From digital rights to political power*. BBC. <https://www.bbc.com/news/technology-15288907>

Bellanova, R. (2017). Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory*, 20(3), 329–347. <https://doi.org/10.1177/1368431016679167>

Beltramini, E. (2021). Against technocratic authoritarianism: A short intellectual history of the cypherpunk movement. *Internet Histories*, 5(2), 101-118.

Benjamin, R. (2019). *Race after technology*. Polity.

Biggar, N. (2023). *Colonialism: a moral reckoning*. William Collins.

Bigo D (2006) Security, exception, ban and surveillance. In Lyon D. (ed.) *Theorizing Surveillance* (pp.46-68). London: Routledge.

Block, L. (2024). The long history of OSINT. *Journal of Intelligence History*, 23(2), 95–109. <https://doi.org/10.1080/16161262.2023.2224091>

Brooks, D. (2013, Feb 4). *The philosophy of data*. New York Times, 4(02). <https://www.nytimes.com/2013/02/05/opinion/brooks-the-philosophy-of-data.html>

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

- Cheney-Lippold, J. (2011). A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society*, 28(6), 164–181. <https://doi.org/10.1177/0263276411424420>
- Chia, A., Keogh, B., Leorke, D., & Nicoll, B. (2020). Platformisation in game development. *Internet Policy Review*, 9(4), 1-28.
- Choi, K. H., Denice, P., Haan, M., & Zajacova, A. (2021). Studying the social determinants of COVID-19 in a data vacuum. *Canadian Review of Sociology/Revue canadienne de sociologie*, 58(2), 146-164.
- Coleman, E. G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, 8(3), 255-277.
- Coleman, G. (2015). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso books.
- Couldry, N., & Mejias, U. A. (2019). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*, 20(4), 336–349. <https://doi.org/10.1177/1527476418796632>
- Curtis, A. (Director) (2011). *All watched over by machines of loving grace* [Film]. BBC. London.
- Cybulski, A. D. (2014). Enclosures at play: Surveillance in the code and culture of videogames. *Surveillance & Society*, 12(3), 427-432.
- Dean, M. 2009. *Governmentality: Power and rule in modern society*, 2nd ed. London, UK: Sage.

- Deleuze, G. (1992). Postscript on the Societies of Control. *October*, Vol. 59. (Winter, 1992), pp. 3-7.
- Denning, D. E. (1996). The Future of Cryptography. In Ludlow, Peter (ed.) (2001) *Crypto Anarchy, Cyberstates, and Pirate Utopias* (pp. 85-102). The MIT Press. England.
- Denning, D. E. (2001). Afterword to “The Future of Cryptography”. In Ludlow, Peter (ed.) (2001) *Crypto Anarchy, Cyberstates, and Pirate Utopias* (pp.103-104). The MIT Press. England.
- Egliston, B. (2020, Feb 1). *The unnerving rise of video games that spy on you*. WIRED. <https://www.wired.com/story/video-games-data-privacy-artificial-intelligence/>
- Egliston, B. (2021). *Gamed: Predatory Platforms and Indie Game Development*. The Reboot
- Ettliger, N. (2018). Algorithmic affordances for productive resistance. *Big Data & Society*, 5(1), 205395171877139. <https://doi.org/10.1177/2053951718771399>
- Fekete, L., & Hagelbäck, M. (2012). *Gameplay experience with eye tracking* [Thesis]. BTH-Blekinge Institute of Technology.
- Flusser, V. (1997). *Medienkultur*. Fischer. Frankfurt am Main.
- Flyverbom, M., Madsen, A. K., & Rasche, A. (2017). Big data as governmentality in international development: Digital traces, algorithms, and altered visibilities. *The Information Society*, 33(1), 35–42. <https://doi.org/10.1080/01972243.2016.1248611>

Forensic Architecture. (2017, July 20). *Torture And Detention In Cameroon*. Forensic Architecture. <https://forensic-architecture.org//investigation/torture-and-detention-in-cameroon>

Forensic Architecture. (2020a, October 28). *Police Brutality At The Black Lives Matter Protests*. Forensic Architecture. <https://forensic-architecture.org//investigation/police-brutality-at-the-black-lives-matter-protests>

Forensic Architecture. (2020b, December 30). *NSO Group's Breach Of Private Data With 'fleming', A Covid-19 Contact-tracing Software*. Forensic Architecture. <https://forensic-architecture.org//investigation/nso-groups-breach-of-private-data-with-fleming-a-covid-19-contact-tracing-software>

Forensic Architecture. (2021, March 7). *Digital Violence: How The Nso Group Enables State Terror*. Forensic Architecture. <https://forensic-architecture.org//investigation/digital-violence-how-the-nso-group-enables-state-terror>

Forensic Architecture. (2022, June 9). *Gold Mining And Violence In The Amazon Rainforest*. Forensic Architecture. <https://forensic-architecture.org//investigation/gold-mining-and-violence-in-the-amazon-rainforest>

Forensic Architecture. (2023a, December 20). *Destruction Of Medical Infrastructure In Gaza*. Forensic Architecture. <https://forensic-architecture.org/investigation/destruction-of-medical-infrastructure-in-gaza>

Forensic Architecture. (2023b, April 17). *"tear Gas Tuesday" In Downtown Portland*. Forensic Architecture. <https://forensic-architecture.org//investigation/tear-gas-tuesday-in-downtown-portland>

Forensis. (2023, July 7). *The Pylos Shipwreck*. Forensis. <https://counter-investigations.org//investigation/the-pylos-shipwreck>

- Forensis. (2024, February 4). *German Arms Exports To Israel*. Forensis. <https://counter-investigations.org/investigation/german-arms-exports-to-israel-2003-2-023>
- Foster, J. B., & McChesney, R. W. (2014). Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age. *Monthly Review*, 66(3), 1. [https://doi.org/10.14452/MR-066-03-2014-07\\_1](https://doi.org/10.14452/MR-066-03-2014-07_1)
- Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*, trans. A. Sheridan. Vintage.
- Foucault, M. (1978). *The History of Sexuality, Volume 1: An Introduction*, trans. R. Hurley. Vintage.
- Foucault, M. (1990). *The History of Sexuality, Volume 2: The Use of Pleasure*, trans. R. Hurley. Vintage.
- Franks, B., Jun, N., & Williams, L. (2018). Introduction. In Franks, B., Jun, N., & Williams, L. (Eds.). (2018). *Anarchism: A Conceptual Approach* (pp. 1-12). Routledge.
- Fredericks, B., Bradfield, A., Nguyen, J., & Ansell, S. (2022). Disrupting the colonial algorithm: Indigenous Australia and social media. *Media International Australia*, 183(1), 158–178. <https://doi.org/10.1177/1329878X211038286>
- Fuchs, C. (2010). How Can Surveillance Be Defined? Remarks on Theoretical Foundations. *The Internet & Surveillance*. Research paper series, 1-22.
- Fuchs, C. (2013). Political Economy and Surveillance Theory. *Critical Sociology*, 39(5), 671–687. <https://doi.org/10.1177/0896920511435710>

- Fuchs, C. (2021). *Social media: A critical introduction*. Sage Publications.
- Gerovitch, S. (2002). *From newspeak to cyberspeak. A History of Soviet Cybernetics*. The MIT Press, Cambridge.
- Gilley, B. (2017). The case for colonialism. *Third World Quarterly*, 1–17.
- Gilley, B. (2023). *The case for colonialism* (First edition). New English Review Press.
- Gilliom, J. (2001). *Overseers of the poor: Surveillance, resistance, and the limits of privacy*. University of Chicago Press.
- Gonzales, C. (2024, April 30). *A Phantom's Tale: The Coyote Influencer on TikTok*. Bellingcat. <https://www.bellingcat.com/news/2024/04/30/a-phantoms-tale-the-coyote-influencer-on-tiktok/>
- Greenberg, A. (2024). *Signal Is More Than Encrypted Messaging. Under Meredith Whittaker, It's Out to Prove Surveillance Capitalism Wrong*. WIRED Magazine (last Accessed June 28th 2025) <https://www.wired.com/story/meredith-whittaker-signal/>
- Guo, C., Cao, J., Zhang, X., Shu, K., & Yu, M. (2019). Exploiting emotions for fake news detection on social media. arXiv preprint. *arXiv:1903.01728*.
- Haggerty, K. D. (2006). Tear down the walls: on demolishing the panopticon. In Lyon D. (ed.) *Theorizing Surveillance* (pp. 23-45). London: Routledge.
- Han, B. C. (2015b). *The burnout society*. Stanford University Press.

Han, B. C. (2017a). *Psychopolitics: Neoliberalism and new technologies of power*. Verso Books.

Han, B. C. (2017b). *In the swarm: Digital prospects*. MIT press.

Han, B. C. (2022). *Infocracy: Digitization and the crisis of democracy*. John Wiley & Sons.

Han, B.-C. (2015a). *The transparency society*. Stanford Briefs.

Hellegren, Z. I. (2017). A history of crypto-discourse: Encryption as a site of struggles to define internet freedom. *Internet Histories*, 1(4), 285-311.

Hughes, E. (1993, March 9). *A Cypherpunk's Manifesto*. Satoshi Nakamoto Institute. <https://nakamotoinstitute.org/library/cypherpunk-manifesto/>

Introna, L. D. (2016). Algorithms, Governance, and Governmentality: On Governing Academic Writing. *Science, Technology, & Human Values*, 41(1), 17-49. <https://doi.org/10.1177/0162243915587360>

Jarvis, C. (2021a). Cypherpunk ideology: objectives, profiles, and influences (1992-1998). *Internet Histories*, 6(3), 315-342.

Jarvis, C. (2021b). *Crypto wars: the fight for privacy in the digital age: A political history of digital encryption*. CRC Press.

Kapsch, P. H. (2022). Exploring user agency and small acts of algorithm engagement in everyday media use. *Media International Australia*, 183(1), 16-29.

- Katz, Y. (2020). *Artificial whiteness: Politics and ideology in artificial intelligence*. Columbia University Press.
- Katzenbach, C., & Ulbricht, L. (2019). Algorithmic governance. *Internet Policy Review*, 8(4). <https://doi.org/10.14763/2019.4.1424>
- Kaur-Gill, S. (2023). The cultural customization of TikTok: Subaltern migrant workers and their digital cultures. *Media International Australia*, 186(1), 29–47. <https://doi.org/10.1177/1329878X221110279>
- Kerr, A., De Paoli, S., & Keatinge, M. (2014). Surveillant assemblages of governance in massively multiplayer online games: A comparative analysis. *Surveillance & Society*, 12(3), 320-336.
- Khabbakh, H. (2013). The Arab Spring and Surveillance Collapse in the face of Social Media Networks. *Omran*, 2(6), 99-121.
- Kırlı, C. (2013). Surveillance and the Formation of the Public Sphere in the Ottoman Empire. *Omran*, 2(6), 33-54.
- Kitchin, R. (2014a). *The data revolution: Big data, open data, data infrastructures and their consequences*. Sage.
- Kitchin, R. (2014b). Big Data, new epistemologies and paradigm shifts. *Big data & society*, 1(1), 2053951714528481.
- Kroker, A., & Weinstein, M. A. (1994). *Data trash: The theory of the virtual class*. *New World Perspectives*.
- Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & class*, 60(4), 3-26.

- Latzer, M., & Festic, N. (2019). *A guideline for understanding and measuring algorithmic governance in everyday life*. *Internet Policy Review*, 8(2). <https://doi.org/10.14763/2019.2.1415>
- Laurent, S. Y. (2021). The archipelago of global surveillance—without States—in the Western world. In Marklund, A., & Skouvig, L. (2021). *Histories of Surveillance from Antiquity to the Digital Era* (pp. 180-192). Routledge.
- Lecomte, R. (2011). Révolution tunisienne et Internet: le rôle des médias sociaux. *L'année du Maghreb*, (VII), 389-418.
- Lester, A. (2023). The British Empire in the Culture War: Nigel Biggar's Colonialism: A Moral Reckoning. *The Journal of Imperial and Commonwealth History*, 51(4), 763–795. <https://doi.org/10.1080/03086534.2023.2209947>
- Li, M. (2009). The Pirate Party and the Pirate Bay: How the Pirate Bay Influences Sweden and International Copyright Relations. *Pace International Law Review*, 21(1), 281. <https://doi.org/10.58948/2331-3536.1040>
- Lilja, M. (2022). The definition of resistance. *Journal of Political Power*, 15(2), 202-220.
- Lilja, M., Baaz, M., Schulz, M., & Vinthagen, S. (2017). How resistance encourages resistance: theorizing the nexus between power, 'Organised Resistance' and 'Everyday Resistance'. *Journal of Political Power*, 10(1), 40-54.
- Loewenstein, A. (2023). *The Palestine Laboratory*. Verso.
- Ludlow, P. (2001) New Foundations: On the Emergence of Sovereign Cyberstates and Their Governance Structures. In Ludlow, Peter (ed.) (2001) *Crypto Anarchy, Cyberstates, and Pirate Utopias* (pp. 1-24). The MIT Press. England.

- Lyon, D. (2016). Big data surveillance: Snowden, everyday practices and digital futures. In Basaran, T., Bigo, D., Guittet, E. P., & Walker, R. B. (Eds.). (2016). *International political sociology: Transversal lines* (pp. 268-285). Routledge.
- Lyon, D. (2017). Surveillance culture: engagement, exposure, and ethics in digital modernity. *International Journal of Communication*. 11(2017), 824-842
- Lyon, D. (2019). Surveillance capitalism, surveillance culture and data politics. In Ruppert, E., Isin, E., & Bigo, D. *Data politics: Worlds, subjects, rights* (pp. 64-77). Routledge.
- Lyon, D. (2022). Surveillance. *Internet Policy Review*, 11(4). <https://doi.org/10.14763/2022.4.1673>
- Lyon, D., Haggerty, K. D., & Ball, K. (2012). Introducing surveillance studies. In Ball, K., Haggerty, K., & Lyon, D.. *Routledge handbook of surveillance studies* (pp. 1-11). Routledge.
- Magalhães, J. C. (2022). Algorithmic resistance as political disengagement. *Media International Australia*, 183(1), 77–89. <https://doi.org/10.1177/1329878X221086045>
- Marx, G. T. (2012). Your papers please”: Personal and professional encounters with surveillance. In Ball, K., Haggerty, K., & Lyon, D.. *Routledge handbook of surveillance studies* (pp. xx–xxxi). Routledge.
- Marx, G. T. (2015). Surveillance Studies. In *International Encyclopedia of the Social & Behavioral Sciences* (pp. 733–741). Elsevier. <https://doi.org/10.1016/B978-0-08-097086-8.64025-4>
- Marx, G. T. (2016). *Windows into the Soul: Surveillance and Society in an Age of High Technology*. University of Chicago Press. <https://doi.org/10.7208/chicago/9780226286075.001.0001>

- Matykiewicz-Włodarska, A. (2022). The Luther effect: The consequences of the Reformation in the area of printed media and communication (M. Jaros & J. Giebułtowski, Trans.). *Napis Pismo Poświęcone Literaturze Okolicznościowej i Użytkowej*, 1, 255–270. <https://doi.org/10.18318/napis.2022.en.1.14>
- Maxigas (2017). Preface. In Beritelli, L. (2017). + *KAOS: ten years of hacking and media activism* (pp. 11-18). Institute of Network Cultures. Amsterdam
- May, T. (2008). *Political Thought of Jacques Rancière: Creating Equality*. Edinburgh University Press.
- May, T. C. (1988). *Crypto-Anarchist Manifesto*. Satoshi Nakamoto Institute. <https://nakamotoinstitute.org/library/crypto-anarchist-manifesto/>
- May, T. C. (1994a, September 10). *The Cyphernomicon*. Satoshi Nakamoto Institute. <https://nakamotoinstitute.org/library/cyphernomicon/>
- May, T. C. (1994b, December). *Crypto Anarchy and Virtual Communities*. Satoshi Nakamoto Institute. <https://nakamotoinstitute.org/library/virtual-communities/>
- McQuade, B. (2018). Windows into the Soul or the Clouded Glass of Surveillance Studies. *Critical Sociology*, 44(4–5), 815–824. <https://doi.org/10.1177/0896920517751588>
- McQuillan, D. (2022). *Resisting AI: An anti-fascist approach to artificial intelligence*. Policy Press.
- Moran, R. E., Grasso, I., & Koltai, K. (2022). Folk Theories of Avoiding Content Moderation: How Vaccine-Opposed Influencers Amplify Vaccine Opposition on Instagram. *Social Media + Society*, 8(4). <https://doi.org/10.1177/20563051221144252>

Morison, J. (2016). Algorithmic Governmentality: Techo-optimism and the move towards the dark side. *Computers and Law*, 27(3).

Musiani, F. (2013). Governance by algorithms. *Internet Policy Review*, 2(3). <https://doi.org/10.14763/2013.3.188>

Nashif, N. (2017). *Surveillance Of Palestinians And The Fight For Digital Rights*. Al-Shabaka.

Ocheni, S., & Nwankwo, B. C. (2012). Analysis of colonialism and its impact in Africa. *Cross-cultural communication*, 8(3), 46-54.

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin. UK.

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

Pereira, G., Moreschi, B., Mintz, A., & Beiguelman, G. (2022). We've always been antagonistic: Algorithmic resistances and dissidences beyond the Global North. *Media International Australia*, 183(1), 124–138. <https://doi.org/10.1177/1329878X221074792>

Piratpartiet (2021) *Principprogram*. Piratpartiet. <https://piratpartiet.se/principprogram/#1-Digitaliseringen-forandrar-allt> [Accessed: July 26 2025]

Piratpartiet (N.D.) *Homepage*. <https://piratpartiet.se/>. [Accessed: July 26 2025]

- Purdy, J. S. (1998) The God of the Digerati. In Ludlow, Peter (ed.) (2001) *Crypto Anarchy, Cyberstates, and Pirate Utopias* (pp. 353-362). The MIT Press. England.
- Quartz (2018, October 31). *The Future of Gaming: Your data, your wallet*. [Video]. Quartz. <https://www.youtube.com/watch?v=VFofnju3V8I>
- Rashed, A., Shirmohammadi, S., Amer, I., & Hefeeda, M. (2025). A review of player engagement estimation in video games: Challenges and opportunities. *ACM Transactions on Multimedia Computing, Communications and Applications*. 192:1-192:33
- Roberts, S. L. (2019). Big Data, Algorithmic Governmentality and the Regulation of Pandemic Risk. *European Journal of Risk Regulation*, 10(1), 94–115. <https://doi.org/10.1017/err.2019.6>
- Roberts, S. L., & Elbe, S. (2017). Catching the flu: Syndromic surveillance, algorithmic governmentality and global health security. *Security Dialogue*, 48(1), 46–62. <https://doi.org/10.1177/0967010616666443>
- Robinson, R. (2021). Big data in early China: Population surveillance in the early Chinese empires. In Marklund, A., & Skouvig, L. (2021). *Histories of Surveillance from Antiquity to the Digital Era* (pp. 20-36). Routledge.
- Rouvroy, A. (2020). *Algorithmic governmentality and the death of politics*. Green European Journal.
- Rouvroy, A., & Stiegler, B. (2016). The digital regime of truth: From the algorithmic governmentality to a new rule of law. *La Deleuziana*, (3), 6-29.
- Rouvroy, A., Berns, T., & Carey-Libbrecht, L. (2013). Algorithmic governmentality and prospects of emancipation. *Réseaux*, 177(1), 163-196.

- Ruensuk, M., Cheon, E., Hong, H., & Oakley, I. (2020). How do you feel online: Exploiting smartphone sensors to detect transitory emotions during social media use. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies*, 4(4), 1-32.
- Sağiroğlu, S., & Sinanç, D. (2013). Big data: A review. *2013 International Conference on Collaboration Technologies and Systems (CTS)*, 42–47. <https://doi.org/10.1109/CTS.2013.6567202>
- Salter, L. A., & Dutta, M. J. (2025). The algorithmic big Other: Using Lacanian theory to rethink control and resistance in platform work. *Distinktion: Journal of Social Theory*, 26(1), 1–16. <https://doi.org/10.1080/1600910X.2023.2224521>
- Sewell, S. A. (2021). Surveillance on the assembly line: Communist resistance to modern production at the Stollwerck Chocolate Factory, 1924–1930. In Marklund, A., & Skouvig, L. (2021). *Histories of Surveillance from Antiquity to the Digital Era* (pp. 87-104). Routledge.
- Shaw, A. (2012). Do you identify as a gamer? Gender, race, sexuality, and gamer identity. *New Media & Society*, 14(1), 28-44.
- Sifa, R., Drachen, A., & Bauckhage, C. (2018). Profiling in games: Understanding behavior from telemetry. *Social interactions in virtual worlds: An interdisciplinary perspective*, 337-375.
- Silverman, Dan P. (1988). National socialist economics: the wirtschaftswunder reconsidered. In Eichengreen, B. J., & Hatton, T. J. (Eds.). *Interwar unemployment in international perspective* (pp.185-220). Dordrecht: Springer Netherlands, 1988.
- Singh, S. (2018, July 5). *Weaponizing data for politics - Shivam Shankar Singh*. [Video]. Hasgeek TV. <https://www.youtube.com/watch?v=QJin9a0KtXI>

Singh, S. (2020). Collecting race-based data during coronavirus pandemic may fuel dangerous prejudices. *The Conversation*.

Skare, E. (2016). *Digital Jihad: Palestinian resistance in the digital era*. Bloomsbury Publishing.

Skinner, B. F. (1973). *Beyond freedom and dignity*. New York: Bantam, Vintage Book.

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

Stevens, A. (2024). *Resisting State Surveillance in the Digital Age: Precarious Coalitions, Contested Knowledge, and Diverse Opposition to Mass-Surveillance in the UK*. Routledge. <https://doi.org/10.4324/9781003297321>

Stoneman, E. (2024 ). Digital Psychopolitics: Towards the Total Control Society. In Knepper, S., Stoneman, E and Wyllie, R. *Byung-Chul Han: A Critical Introduction* (pp. 64-93). Polity. Cambridge.

Suárez Val, H., D'Ignazio, C., Acosta Romero, J., Teng, M. Q., & Fumega, S. (2023). Data activism and femicide. *Big Data & Society*, 10(2), 1-6.

Treguer, F. (2019). *L'utopie dechue: Une contre-histoire d'Internet, XVe-XXIe siècle*. Paris: Fayard.

Tunisian Labour Communist Party (2005) *A Document Project for a Popular Democratic Alternative*. Al-Hiwar Al-Mutamaddin. <http://www.ahewar.org/debat/show.art.asp?aid=30199> Accessed: July 26 2025

- Van Der Velden, L. (2015). Forensic devices for activism: Metadata tracking and public proof. *Big Data & Society*, 2(2), 1-14. <https://doi.org/10.1177/2053951715612823>
- Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & society*, 12(2), 197-208.
- Walker, A. (2014). Watching us play: Postures and platforms of live streaming. *Surveillance & Society*, 12(3), 437-442.
- Wang, Y., & Pal, A. (2015, July). Detecting emotions in social media: A constrained optimization approach. In *IJCAI* (pp. 996-1002).
- Weller, T. (2012). The information state: An historical perspective on surveillance. In Ball, K., Haggerty, K., & Lyon, D.. *Routledge handbook of surveillance studies* (pp. 57-63). Routledge.
- Weller, T. (2022). The historical ubiquity of surveillance. In Marklund, A., & Skouvig, L. (2021). *Histories of Surveillance from Antiquity to the Digital Era* (pp. 163-179).
- Whitson, J. R., & Simon, B. (2014). Game studies meets surveillance studies at the edge of digital culture: An introduction to a special issue on surveillance, games and play. *Surveillance & Society*, 12(3), 309-319.
- Wyllie, R. (2024 ). Burnout: Against Achievement Culture. In Knepper, S., Stoneman, E and Wyllie, R. *Byung-Chul Han: A Critical Introduction* (pp. 8-34). Polity. Cambridge.
- Yee, N., Ducheneaut, N., & Nelson, L. (2012, May). Online gaming motivations scale: development and validation. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 2803-2806).

Yu, Z., Treré, E., & Bonini, T. (2022). The emergence of algorithmic solidarity: Unveiling mutual aid practices and resistance among Chinese delivery workers. *Media International Australia*, 183(1), 107–123. <https://doi.org/10.1177/1329878X221074793>

Zayed, A. (2013). From Spying to Conflict and Violence: Surveillance Mechanisms in the Modern Egyptian State. *Omran*, 2(6), 13-32.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs, New York.

Zureik, E. (2013). Constructing Palestine through Surveillance Practices. *Omran*, 2(6), 73-98.

Zureik, E., Lyon, D., & Abu-Laban, Y. (Eds.). (2013). *Surveillance and control in Israel/Palestine: Population, territory and power*. Routledge. <https://doi.org/10.4324/9780203845967>

## APPENDICES

### A. TURKISH SUMMARY / TÜRKÇE ÖZET

Bu tez, Büyük Veri ve gelişmiş algoritmalar çağında gözetim ve karşı-gözetimi yeniden düşünmektedir. Teknoloji Karşı-gözetimine odaklanmaktadır. Bu ikilemi, genel olarak 'bilgi rejimi'ne direnişin kalbinde anlamaya çalışmakta, teknoloji karşı-gözetiminin örnek bir vakası olarak Cypherpunk'ları incelemektedir. Aşağıdaki amaçları belirlemektedir:

1. Bilgi rejiminde bir direniş stratejisi olarak, Cypherpunklar vakasında tezahür eden teknoloji karşı-gözetiminin ne olduğunu keşfetmek;
2. Çağdaş bilgi rejimi içinde gerçekleşen gözetim ve karşı-gözetim arasındaki ilişkiyi anlamak;
3. Bilgi rejiminin kontrolüne karşı teknoloji karşı-gözetiminin potansiyel etkinliği üzerine düşünmek.

Dijital çağın ortaya çıkmasıyla, özellikle veri devriminden sonra gözetim yoğunlaştı ve yaygınlaştı. Günümüzde gelişmiş algoritmalar (Yapay Zeka ve türevleri dahil) ve dijital veri altyapıları (Büyük Veri ve Küçük Veri dahil) hayatın her alanını yönetmektedir. Bu teknolojiler esasen gözetim teknolojileridir. Bu, bilgi (gözetim) rejimi çağıdır. Sosyal, politik ve ekonomik alanlarda belirleyici etkinin bilgi tarafından, yani veri ve bilgilerin toplanması, depolanması ve işlenmesi yoluyla sağlandığı yeni bir hakimiyet biçimidir (Han, 2022). Bununla birlikte, yeni karşı-gözetim biçimleri de ortaya çıkmaktadır.

Karşı-gözetim biçimlerinden biri teknoloji karşı-gözetimidir. Bilgi rejimine karşı direnişin ana araç ve stratejisi olarak bizzat dijital teknolojinin önemini ve önceliğini vurgular. Teknoloji karşı-gözetiminin örnekleri çok sayıda ve çeşitlidir ve uygulamaları bir grup birey ve topluluk tarafından kullanılmaktadır. Öne çıkan

örnekler arasında, direnişin tek aracı olarak teknolojiyi, özellikle güçlü şifrelemeyi savunan ve bu amaçla çeşitli teknolojiler geliştiren Cypherpunklar yer almaktadır. +KAOS, bilgi rejiminin veri altyapılarının gücüne ve hakimiyetine karşı koymak için alternatif veri altyapıları geliştirmeye odaklanan başka bir örnektir. 'Teknik karşı-gözetim'in aksine, gözetimi bozmak amacıyla sanat eserlerinin gözetimi engellenmenin ana aracı olarak benimsendiği 'sanatsal karşı-gözetim' gibi başka stratejiler de bulunmaktadır. Ayrıca, 'pedagojik karşı-gözetim' eğitim unsurunu ve farkındalığın artırılmasını vurgular. Dahası, bu gözetim teknolojilerinin zararlı etkilerini sınırlamak ve adalet ile eşitliği sağlamak için hukukun gücüne inanan 'hukuki karşı-gözetim' de bulunmaktadır.

Teknoloji yaklaşımının gözetimi engelleme konusundaki temelinde bir ikilem yatmaktadır. Karşı çıkmaya çalıştıkları teknoloji bilgi rejiminin ayrılmaz bir parçasıdır, ancak aynı zamanda önemli ölçüde iyileştirici sonuçlara yol açan ve dönüştürücü bir özgürleştirici role sahip olan rahatsız edici bir güç olmuşlardır. Zaman zaman hakimiyetin güç ilişkilerini pekiştirmişler, zaman zaman da özgürleştirici güçler olmuşlardır. Teknoloji karşı-gözetimi ile ilgili bu ikilem, bu Tezin konusudur.

Bu tez, teknoloji karşı-gözetiminin örnek bir vakası olduğu için Cypherpunkları vaka çalışması olarak seçmektedir.

Teknoloji odaklı, siber güvenlik ve gözetim konusunda uzmanlaşmış bir dergi olan WIRED Magazine'in kıdemli yazarlarından Andy Greenberg (2024), uygulamanın 10. yıldönümünde en güvenli iletişim, kar amacı gütmeyen yazılım uygulaması olan Signal'in başkanı Meredith Whittaker ile yaptığı röportajı bildirmeden önce şunları yazıyor: "O Temmuz 2014'ten bu yana Signal, bir anarşist kodlayıcı tarafından yaratılan, San Francisco'da tek bir odada çalışan derme çatma bir ekip tarafından yönetilen, paranoya puanları için yarışan hackerlar tarafından kulaktan kulağa yayılan bir Cypherpunk merakından, tam teşekküllü, ana akım, şifreli iletişim fenomenine dönüştü."

WIRED dergisi, ikinci sayısında, bir yandan Cypherpunkları (kripto-anarşizm) diğer yandan da Liberteryenizmi ilk kez birbirine bağladı. Bu sayının (Mayıs/Haziran

1993, Sayı 1.02) kapağında, Cypherpunkların kurucuları Timothy C. May, Eric Hughes ve John Gilmore, ABD bayrağını tutarken maskeli olarak yer aldı ve "Bir Davası Olan Asi (Gizliliğiniz)" yazısı bulunuyordu. Yirmi yıl sonra, Wired dergisinin 22.09 sayılı sayısının kapağında, ünlü ihbarcı ve ABD Ulusal Güvenlik Ajansı (NSA) yüklenicisi Edward Snowden yer aldı. İhbarcılık, büyük ilgi çeken önemli bir çağdaş konudur. Cypherpunk vizyonunun merkezi bir yönünü temsil eder.

Cypherpunklar, 1992 yılında Silikon Vadisi'nde Timothy C. May tarafından Eric Hughes ve John Gilmore ile birlikte kuruldu. 16 kişilik bir grup, her Cumartesi teknoloji başlangıç şirketleri için ayrılmış bir bölgede toplanmaya başladı. Kısa bir süre sonra moderasyonsuz, özgür ve anonim bir posta listesi oluşturdular. Jarvis'e (2021a) göre Cypherpunklar dört stratejik hedef öngördü. İlk hedef, vatandaşların kriptografik teknolojilere serbest erişimiyle ilgilidir. Bu, diğer hedeflerinin temelini oluşturur; ikincisi ise anonim iletişimi kapsar. Üçüncü amaç, hükümet müdahalesi olmadan anonim ekonomik etkileşimlerde bulunma özgürlüğünü vurgular. Son olarak, devletin gücünü azaltmak için ihbarcılık ve sızdırma platformları geliştirilmelidir.

Tarihteki emsallerine rağmen, dijital dünyadaki ihbarcılık yeni bir boyut kazandı ve benzeri görülmemiş bir erişim, hacim ve etki yarattı. Wikileaks'in Aralık 2006'daki ilk yayınından bu yana etkisi, tarihte muhtemelen eşsizdi. Cypherpunk posta listesinin orijinal bir katkıcısı olarak Assange'ın fikirleri, hareketin genel ideolojisi, işleyiş biçimi ve hayal gücü ile uyumludur. Timothy C. May, 1988 gibi erken bir tarihte kriptolojik teknolojinin ihbarcılık için kullanılmasını önermiş ve bunu kripto araçları için temel bir uygulama olarak dile getirmiştir. Ayrıca farklı ihbarcılık platformlarının kurulmasını teşvik etmiştir. Çağdaş zamanlarda önemli bir diğer konu ise Kripto para birimidir. Konu, grubun ilk günlerine, özellikle David Chaum'un dijital nakit üzerine çalışmalarına kadar uzanmaktadır. Anonim ekonomik işlemlerin özgürlüğü (Jarvis, 2021a), Cypherpunkların temel bir hedefi ve stratejilerinin merkezi bir yönüdür. Dahası, siber savaşlar devam etmektedir (Jarvis, 2021a) ve hem ihbarcılık hem de kripto para birimleri etrafındaki fikirler hala Cypherpunkların mirası ve ideolojilerinden beslenmektedir.

Cyberpunkların, kripto savaşları bağlamındaki devam eden etkisi, grubun bir vaka çalışması olarak seçilmesinin nedenlerinden biridir. Beltramini'ye (2021) göre Cyberpunklar, "muhtemelen tarihteki siber uzayda özgürlüğü korumaya adanmış en etkili taban örgütüdür" (101). Bu, Cyberpunkların motive edici ruhu ve ideolojisinin özüdür, ancak aynı zamanda o dönemde Amerika Birleşik Devletleri'nde ve ötesinde, özellikle Batı Avrupa ve Asya'daki müttefik ülkelerde ortaya çıkan grupların ve kuruluşların çoğunun da temelini oluşturur. Bu ideoloji veya vizyon, farklı varyasyonlarda da olsa, Yapay Zeka (YZ), Büyük Veri ve genel olarak bilgisayar teknolojisi hakkındaki çağdaş girişimler, söylemler ve hayal gücü üzerinde önemli bir etki yaratmaya devam etmektedir; bu etkiyi farklı "Sınırları" veya "Devrimleri" savunanlar yapmaktadır. Dahası, Kaliforniya ideolojisi, Amerika Birleşik Devletleri'nin ötesine, Batı Avrupa ve Asya'daki diğer coğrafyalara etki ederek, oradaki sanal sınıfın digerati'sine hitap etmiş ve bu kişiler aslında kendi toplumlarındaki işçi sınıflarından çok Kaliforniyalı akranlarına daha yakındı. Bu durum, ideolojinin belirli bir sosyoekonomik çevreye ve belirli bir teknolojik bağlama sahip belirli bir insan grubunun sonucu olmasına rağmen böyledir.

Önemli bir diğer neden ise grubun Amerikan yaklaşımına sahip olmasıdır. Birincisi, bu durum, 11 Eylül sonrası Amerika Birleşik Devletleri'nden çıkan fikirlerin öncülük ettiği küresel güvensizlik kavramlarının yaydığı "endişe hali" bağlamında Bigo (2006; Stevens, 2025'te) tarafından adlandırılan durum için önemli hale getiriyor. Dahası, hegemony açısından bakıldığında, Amerika Birleşik Devletleri ve Amerikan Büyük Teknoloji şirketleri, teknoloji aracılığıyla gözetim konusunda sistematik ve yapısal bir şekilde dünyaya hakimdir (Kwet, 2019). Bu durum, bu hegemonik bağlam içinde teknolojik karşı gözetimi araştırmayı önemli kılmaktadır. Barbrook & Cameron'a (2001) göre, Kaliforniya ideolojisi, ABD'deki gelişmekte olan bilgi toplumu ve bilgi ekonomileri bağlamında, tarihsel, ekonomik ve teknolojik gelişmelerin kritik bir dönüm noktasında, savunucularının anlatısına karşı koyabilecek herhangi bir rakip olmadan gelişmiştir. "Bu kritik dönüm noktasında, Amerika Birleşik Devletleri'nin Batı Yakası'ndan bir yazar, hacker, kapitalist ve sanatçı grubunun gevşek bir ittifakı, yaklaşan bilgi çağı için heterojen bir ortodoksi tanımlamayı başarmıştır – Kaliforniya İdeolojisi." (365).

Dahası, bu tezin konusuna daha uygun olanı ise, gözetim rejimine karşı hareketin teknolojik yaklaşımıdır; veya bazen "teknokrazi" veya teknokratik totalitarizm olarak da adlandırılan şeydir. Gözetim ve gizlilik, Cypherpunk ideolojisi/kavramsal çerçevesinin temel unsurlarıdır ve Cypherpunk'lar belgelerinde ve konuşmalarında, etkili çözümün yasa değil (örneğin, karşı gözetimin yasal yaklaşımlarının aksine) teknolojinin (özellikle güçlü kriptografi) kullanımı ve geliştirilmesi olduğunu vurgularlar. Dahası, Cypherpunk'lara göre tüm bireyler, gerçekten özgür olmak istiyorlarsa, en azından kriptografinin temellerini öğrenmelidir. Cypherpunk'lar "kod yazar" ve bu kod, teknolojik otoriterliğin bilgi rejimine karşı stratejilerini, taktiklerini ve söylemlerini şekillendirir. Bu neden, diğer nedenlerle birlikte, Cypherpunk'ları yukarıda tartışılan önerilen çerçeve ve araştırma hedefleri ışığında incelenmeye değer örnek bir vaka haline getirmektedir.

Başka bir gerekçe ise, bir yandan teknolojik karşı gözetim olarak Cypherpunk'lar ile diğer yandan yıkmaya çalıştıkları sistem arasındaki ilişkidir. Cypherpunk'ların dili ve hayal gücü, dijital paradigma içindeki rakipleriyle yakın bir ilişki ortaya koyar, ancak "teknolojiyi efendilerinin hizmetine sokmayı" tercih ederler (Assange 2006, 2). Dahası, Cypherpunk'lar, sahip oldukları düşünce yapısı ve mizacın bir yan ürünü olmaktan çok, derinden kök salmış bir kayıtsızlıkla suçlanırlar (Barbrook & Cameron, 2001). Hatta bazıları onları, uluslararası bir yaklaşım gerektiren, sadece yanlısamalara dayanan küresel suçlular ve teröristler için bir sığınak olarak uluslararası bir tehdit olarak görebilir (Denning, 1996, 2001). Bu, hareketin olumlu etkilerini göz ardı etse de, gözetim rejiminin çağında teknolojik karşı gözetimi anlamlı bir şekilde anlamak için, bu ilişkiyi basitçe karşıtığa indirgemeden, karşı gözetim ve gözetim arasındaki bu ilişkiyi anlamak önemlidir.

Bu vaka çalışmasının seçimi için bu açıdan daha önemli olan, bu hareket içindeki gerilimlerdir. Bu vaka çalışması, bireysel ve kolektif eylem arasındaki direnişteki gerilimi – bireysel direniş ve sosyal hareket direnişi arasındaki gerilimi göstermektedir. Çeşitli ideolojik konumlar arasındaki çizgileri bulanıklaştırır, çeşitli fikirlerin bir karışımı olarak, genellikle çakışan özelemlerle ortaya çıkar. Hem hem de hiçbirini. Bazı gözlemcilerin kendiyi çelişen olarak adlandırabileceği bu konum, yalnızca sağlam bir teknolojik determinizme sahip böyle bir ideolojinin sonucu olabilir.

Yukarıda belirtilen gerekçeler ışığında, bu tez, Cypherpunk'ları ve kriptografiye olan inançlarını (Kripto Savaşları bağlamında) inceleyecektir. Bu vaka, bu tezin araştırma hedefine ulaşmak için, veri altyapısı ve gelişmiş algoritmalarıyla bilgi rejiminde teknoloji karşı gözetim hakkındaki tartışmayı örneklendirmek ve göstermek amacıyla ele alınmıştır.

Çalışma, nitel, yorumlayıcı sosyal araştırma alanına girmektedir. Cypherpunk'ların tarihi ve ideolojisi üzerine mevcut literatürden yararlanacaktır. Dahası, Cypherpunk'lar ve gruptaki veya onlarla ilişkili önde gelen figürler tarafından yayınlanan belgeleri kullanacaktır. Teknolojist karşı-gözetimin, karşı çıkmaya çalıştığı bilgi rejimi için zorunlu bir güç olarak gerçekleştiği argümanını desteklemek için bu yaklaşımı benimseyecektir. Hem ilerici hem de gerici; yıkıcı ve pekiştirici olmak üzere ikili bir karaktere sahiptir. Dahası, bu nedenle, gözetimi engellemedeki etkinliği, karşı çıkmaya çalıştığı rejimle yakınlığı ölçüsünde, iyileştirici bir etkiyle sınırlıdır.

Bu tez, filozof Byung-Chul Han'ın analizine dayanmaktadır. Özellikle, psikopolitika ve bilgi rejimi üzerine çalışmaları. Han'ın analizi bu tezin 3. Bölümünde ayrıntılı olarak geliştirilecektir. Bilgi rejimi, bilgi aracılığıyla - yani veri ve bilgilerin toplanması, depolanması ve işlenmesi yoluyla - sosyal, politik ve ekonomik alanlarda uygulanan yeni bir hakimiyet biçimini ifade eder (Han, 2022). Bilgi rejimi, bireylerin ve kitlelerin davranışlarını ön-refleksif bir düzeyde etkilemeyi amaçlayan psikopolitika zorunlulukları doğrultusunda çalışır. Aynı zamanda, bilgi rejimi psikopolitikanın güçlendirir ve yayar.

Psikopolitikanın işleyişine bir örnek mikro hedeflemedir. Mikro hedefleme, bir bireyin davranışı hakkında toplanan verilere dayanarak mesajları kişiselleştirerek çalışır. Siyasi mesaj veya ticari reklam artık çeşitli kişiliklere, ideolojik konumlara ve arzulara sahip bir nüfusu hedeflememektedir. Bunlar artık onu alana kişiyi etkilemek üzere özel olarak ayarlanmıştır. Aslında, tekrarlanan içerik türü, davranış kontrolü amacıyla değiştirilir.

Devam etmeden önce, Han'ın çalışmalarında 'bilgi' ve 'gözetim' arasındaki ilişkiye dikkat çekmek önemlidir. Han, Fuchs (2010) tarafından öne sürülenlere benzer bir

şekilde, bilgi rejiminin zorunlu olarak bir gözetim rejimi olmadığını savunarak, bilgi rejimi ile gözetim rejimi arasında örtük bir ayrım yapmaktadır. Bununla birlikte Han, mevcut bilgi rejimini bir gözetim rejimi olarak görmektedir ve bunu bilgi rejimi terimleriyle formüle etmektedir. Bilgi rejimi ve gözetim rejimi, neoliberal dönemde örtüşmektedir. Dolayısıyla, her iki kavram da birbirinin yerine kullanılmaktadır (bkz. Han, 2022).

Han, özgürlük krizi adını verdiği gözlemiyle başlar. Neoliberal psikopolitika altında, hakimiyetin antitezi olması gereken özgürlük, kontrol biçimi olarak sömürülmekte ve kullanılmaktadır (Han, 2017a). Özgürlük baskı üretir. Bu, tarihte büyük bir dönüşümün parçasıdır - sanayi kapitalizminden bilgi kapitalizmine. Burada, 19. yüzyıl kapitalizminden temelde farklı kılan yeni bir üretim biçimi, kapitalizmde bir mutasyon gözlemliyoruz. Ağlı, ağsız, endüstri sonrası, yeni bir üretim biçiminde yaşıyoruz, bu da önceki üretim biçimlerinde bulunan verimlilik ve etkinlik artışı sınırlamalarını aşmaktadır. Mevcut kapitalizm, genellikle Üçüncü Dünya'ya yaptırılan üretimden ziyade, yüksek dereceli bir üretimdir. Bu, üretim değil, ürünler kapitalizmidir, yani bitmiş ürünleri satın almak ve hizmet satmak ve hisse senedi almak ister. Ortaya çıkan şey bir kontrol toplumdur (Aynı eser; Han, 2017b).

Bu kontrol toplumu, Michel Foucault'nun önerdiği disiplinler toplumundan bir mutasyondur. Biyogüç yerine psikolojik güç doğrultusunda çalışır. Michel Foucault (1978), on yedinci yüzyıldan itibaren güç mekanizmalarında egemen güçten disiplinler güce doğru bir dönüşüm gözlemlemiştir. Disipliner güç, egemen gücün kaba saba doğasına kıyasla özünde daha incelikli ve hassastı; yaşamı eksiltmek yerine yaşamı yönetmeyi amaçlıyordu. Bu yaşam üzerindeki güç iki biçimde gelişti: insan bedeninin anatomo-politikası (veya beden disiplinleri) ve nüfusun biyopolitikası (veya nüfus düzenlemeleri). Biyogüç, ikili doğasıyla üretim ve verimlilik amacıyla bedenleri ve enerjileri kontrol etmeyi amaçlıyordu. Hedefi, bireyi itaatkar bir makine haline getirmek, montaj hattına yerleştirmek için şekillendirmek olan 'itaatkar bedendi'. Bunun için disiplinler uygulandı. Disiplinler kısıtladı, yasakladı ve sınırlamalar getirdi ve eğitim kurumları, hapisane, fabrika ve klinik gibi çeşitli ortam ve çevrelerde uygulandı.

Buna karşılık psikopolitika, farklı buyruklar doğrultusunda çalışır. Engellemek yerine baştan çıkarır ve teşvik eder, kısıtlamak yerine bireyi özgür bırakır. Bu nedenle, "Tarihin, özgürlüğün kendisinin baskı ve zorlama anlamına geldiği tekil bir evresinde yaşıyoruz. Aslında özgürlük, zorlamanın antitezi anlamına gelir. Ve yine de bu antitezi şimdi zorlama ve kısıtlama doğuruyor. Daha fazla özgürlük daha fazla baskı anlamına gelir. Bu nedenle, özgürlüğün sonunu işaret eder." (Han, 2017b, 48-9). Birey kendini sömürür. Bu, pişeyi psikopolitik güç teknolojileri tarafından ele geçirmesinin bir sonucudur. Biyopolitika bedenlerle ilgilenir. Bireyin 'bedeni' ile birlikte bir 'ırk' olarak beden, nüfus disiplinlerin hedefidir. Buna karşılık psikopolitika psikolojiyle ilgilenir; özneyi, yani girişimciyi, ön-refleksif, bilinçdışı düzeyde kontrol etmek için pişeye nüfuz eder. Birey, aslında optimize edilenin sistem olduğu, bireyin değil, sürekli optimizasyon arayan bir girişimci olarak kendini gören özgürlük yanılısaması altında yaşıyor. Başka bir deyişle, bedenin özgürleşmesi sömürüyü ortadan kaldırmaz, aksine "hayat projelerimiz, sömürüye açık her türlü duygusal, bedensel ve içgüdüsel boyutları içerir." (Wyllie, 2024, 16).

Uber örneğinde platform çalışanları bu durumu aydınlatıyor. Bu durumda, Salter ve Dutta'nın (2023) gösterdiği gibi, bilgi ve uygulama arasında bir paradoks mevcuttur. Mevcut ve hissedilen sömürüye rağmen, platform iş modeli ve algoritmaları, kural yıkan girişimciye dair ideolojik bir fanteziyi mümkün kılıyor. Bu şekilde çalışanlar bu iş modelinin ağına yakalanıyor. Sömürü, güvencesizlik ve adaletsizliklerin farkında olmalarına rağmen, çalışanlar kural yıkan girişimciye dair bu ideolojik fantezi tarafından yönlendirilerek platform için çalışmaya devam ediyorlar, farklı bir alternatif aramak yerine. İşin bu psikopolitik oyunlaştırılması, çalışanların kendi çıkarlarına aykırı çelişkili, mantıksız pozisyonlar benimsemesine neden olan durumun sebebidir.

Ayrıca, psikopolitika dijital teknolojilerle iç içedir. Psikopolitika, dijital paradigmayı mümkün kılar ve ona bağımlıdır. Gözetim rejiminden yararlanır ve onu sağlamlaştırır. Bilgisayar cihazı ve bilgisayar ağları olmadan bireyin pişesine nüfuz etme yeteneği imkansızdır. Dahası, dijital çağın ilk günlerinin ütopyacılığı basit bir yanılısamadır (Han, 2017b). Kurtuluş için bir güç yerine, yeni bir tahakküm biçimine sahibiz - 'bilgi rejimi' (Han, 2022).

Büyük Veri ve gelişmiş algoritmalar aracılığıyla bilgi rejimi, hem bireyin hem de nüfusun 'psikografik' çizelgelerini sağlayabilmektedir. Psikopolitika bu şekilde, bir refleks öncesi düzeyde psişeye nüfuz edebilir ve insanların davranışlarını - ister ticari satın alma tercihleri ister siyasi karar alma ve oy verme olsun - etkileyebilir. Bu, tarihte eşi benzeri görülmemiş bir akıllı güç biçimidir. Bu manipülatif akıllı gücün sosyal, siyasi ve ekonomik etkileri çok geniştir. Örneğin, sosyal medya platformlarının, algoritmaların ve analitiklerin çağdaş sahnesinde siyaset ve kamusal alan dramatik bir şekilde değişmiştir. Trump (ilk Twitter başkanı) tarafından benimsenen sahte haberlerin gerçeküstü siyaseti, Büyük Veri ve gelişmiş algoritmaları ile bilgi rejimi altında mümkündür. Komplo teorileri de bu koşullar altında, hakikat ve temsil kriziyle birlikte temel ve yaygın güvensizlikle (Han, 2022) gelişmektedir.

Bu durum, Büyük Birader gözetiminin 'dostça' hale geldiği bir durumla ilgilidir. Artık gözetim gönüllü olarak gerçekleşiyor. İnsanlar kendilerini maruz bırakıyor ve kendi kendilerini aydınlatıyorlar. Lyon (2017), gözetimle ilgili eşi benzeri görülmemiş bir kültürün ortaya çıktığını gözlemliyor. Bunu yakalamak için 'gözetim kültürü' kavramını öneriyor. Bunun iki ana yönü vardır. Birincisi, çağdaş toplumda yaygın olarak bulunan gözetime uyumu ilgilendirir. Gözetim kültürünün ikinci ana yönü, genel olarak nüfusun artık devlet veya kurumsal gözetimin yalnızca hedefi veya nesnesi olmamasıdır. İnsanlar, gözetimle etkileşim kurmakla kalmayıp aynı zamanda onu başlattıkları için aktif katılımcılar haline gelmişlerdir.

Han'a göre bu, neoliberal psikopolitik tahakküm biçiminde gücün temel teknolojileri olan duygusallık ve oyunlaştırma aracılığıyla açıklanabilir. Duygular, özgürleşmiş öznelliğin ifadesi olarak ortaya çıkarılır ve çağrılır - bu 'ifade edilmiş', 'iletişim kurulmuş' öznelliğin sömürülmesi için. Han'a göre bu ani patlama, her şeyden önce ekonomik bir süreçten - 'yeni, maddi olmayan bir üretim biçiminin' ortaya çıkışından kaynaklanmaktadır. Bizim zamanlarımızda "Duygular bir üretim aracı haline geldi" (Han, 2017a, 45). Biyopolitiğin itaatkar 'itaatkar bedeni' duygulardan mahrum bırakılmıştı - bırakılmamalıydı. Duygular, biyopolitik disiplin toplumunda yıkıcı bir güç olarak görülüyordu. Kontrol toplumunda, duygular sömürü için ortaya çıkarılır. Biyopolitiğe kıyasla bir güç olarak, "duygu, bütünsel kişiyi, kişinin tamamını

psikopolitik olarak yönlendirmek için oldukça etkili bir araç sağlar." (Han, 2017a, 48)

Ayrıca, bilgi rejiminde yaşamın ve iletişimin bütünlüğü 'oyunlaştırılıyor'. Düşünmenin iki biçimi vardır. Birincisi işte düşünmek, diğeri ise oyunda düşündürmektir. Oyunların üretken olmayan - emeğin karşıtı - olmaları beklenir. Kapitalizmin bu yeni mutasyonu, sömürü için üretkenlik amacıyla oyun oynamayı emek alanına yatırır ve varsayar. Oyun ve emek örtüşür - yaşamın bütünlüğü sömürülebilir hale gelir (Han, 2017a).

Duygusallaşma ve oyunlaştırma, siyasi yansıma ve kolektif eylem için uygun olmayan özel zamansallıklara sahiptir. Dahası, nüfusun refleks öncesi bilinçaltı düzeyde kontrolü, yansıtıcı ve kolektif eylemi daha da olası kılmayan psikolojik hastalıklara yol açar. Böyle bir salgın hastalıklardan biri, belirtileri dikkat eksikliği ve insanların analitik yeteneklerinin giderek bozulmasını içeren Bilgi Yorgunluğu Sendromu'dur (IFS). Ek olarak, sorumluluk kabul etme yeteneklerini giderek kaybettiler (Han, 2017b). Güç ilişkilerini sorgulayan ve bozan etkili bir kolektif eylem için gerekli zamansal ve zihinsel koşullar olası değildir. Siyasi kimliğe sahip bir kitle yerine, bilgi rejiminin ortaya çıkardığı şey 'sürülerdir' - değişken, geçici ve kısa süreli toplantılar. Sürülerin etkili siyasi eylem için gerekli birleştirici ruh ve süreden yoksun olduğu belirtilmektedir (aynı yer).

Han'ın çalışmasının önemi öncelikle psikopolitik kontrolün dinamikleri ve içerdiği unsurların analizinden kaynaklanmaktadır. Analizi, Büyük Veri ve gelişmiş algoritmalar çağındaki gözetim rejimini, özelliklerini ve dinamiklerini anlamak açısından önemlidir. Dahası, teknoloji karşı-gözetimin gerçekleştiği bağlamı ve direniş nesnelere anlamak, etkinliğini incelemek ve bu tezin problem ifadesinde sunulan ikilemi anlamak için önemlidir. Han'ın anlatısı, bu tezin konusuyla ilgili analitik araçlardan oluşan sentetik bir repertuar sunarak dinamiklerine daha derinlemesine inmektedir.

Han'ın analizi ve teknoloji karşı-gözetim bağlamı, bu tezin 3. Bölümünde ayrıntılı olarak tartışılacaktır. Ayrıca bu tez, Han'ın felsefesinden yararlanan teorik çerçeveyi

zenginleştirmek amacıyla Gözetim Çalışmaları ve Direniş Çalışmaları'ndan elde edilen son teorik gelişmeleri ve ampirik sonuçları kullanacaktır. Gözetimin tarihi ve doğası üzerine yapılan tartışmalar, gözetim ve kontrol arasındaki ilişki üzerine yapılan tartışmalara ışık tutacaktır. Ek olarak, Direniş Çalışmaları, teknoloğ karşı-gözetimi karmaşıklık, çokluk ve dinamik yönlülük olgusu olarak bağlamlandırmada bilgilendirici olacaktır.

Tez, filozof Byung-Chul Han'ın analizine dayanmaktadır. Özellikle psikopolitika ve Bilgi rejimi üzerine yaptığı çalışmalarına. Han'ın analizi bu tezin 3. Bölümünde ayrıntılı olarak geliştirilecektir. Psikopolitika ve Bilgi rejimi zorunluluklarının merceğinden bakarak, bu tez Çağdaş bilgi rejimi içinde gerçekleşen gözetim ve karşı-gözetim ilişkisini anlamak için Cypherpunkları teknoloğ karşı-gözetimin örnek bir vakası olarak incelemiştir. Teknoloğ karşı-gözetimin, karşı koymaya çalıştığı bilgi rejimi için zorunlu bir güç olarak gerçekleştğini savunmaktadır. Hem ilerici hem de gerici; yıkıcı ve pekiştirici olarak ikili bir karaktere sahiptir. Dahası, bu nedenle, gözetimi karşı koymadaki etkinliğı, karşı koymaya çalıştığı rejimle yakınlığı ölçüsünde, iyileştirici etkiyle sınırlıdır. Çalışma aşağıdaki teorik çerçeveye dayanacaktır.

Cypherpunkların bilgi rejimine yönelik önemli bir eleştirisi, güç doğasındaki dönüşümdür. Teknolojik otoriterlik (veya bilgi rejimi) çağında güç, önceki otoriterlik biçimlerinin aksine, incelikli ve manipülatif hale gelmiştir. Bu, Cypherpunkları teknoloğ bir hareket olarak, dijital dönüşe eşlik eden teknolojik coşkunun ana akımından ayıran bir unsurdur; yeni Aydınlanma. Vericilik veya sibernetik gibi akımların aksine, Cypherpunklar dijital paradigma ile birlikte ortaya çıkan otoriter bir eğilimi tespit etmiş ve eleştirmiştir. Bu eleştiri, onu bilgi rejimine karşı özgürleştirici bir potansiyele sahip bir direniş gücü olarak konumlandırmaktadır. Dahası, Cypherpunklar, kontrolün psikopolitik rejiminin ana zorunluluklarından biri olan şeffaflık zorunluluğı içinde önemli bir ayırım yapmaktadır. Şeffaflık, birey üzerinde neoliberal psikopolitikanın çeşitli mekanizmaları tarafından uygulanan, kendini ifşa etme zorunluluğudur. Bu noktada gizlilik, üretkenliğı ve verimliliğı engellediğı için sermaye için eskimiş ve istenmeyen hale gelir. Güçlü kriptografik teknolojilerin geliştirilmesi ve kriptografik bilgi ve kullanımın yaygın olarak

benimsenmesi için savunuculuk yoluyla, şeffaflık rejimi ve bilgi rejimi ile doğrudan bir karşıtlık oluştururlar.

Cypherpunklar, psikopolitik bilgi rejimi içinde bir özgürlük duygusu yayarlar. Girişimci benlik/proje mantığını güçlendirirler. Birey özerk bir varlıktır. Bir vatandaş ve bir tüketicidir. Kaynakları olan ve teknolojik araçlar ve kendi yapımı projeler aracılığıyla otoriter kurumların sınırlamalarının ötesine geçebilen biridir. Bu anlamda birey, disiplinlerin kuşatmalarının ötesinde alanlar açabilen kontrol toplumunun yılanına benzer. Hellegren (2017) tarafından ifade edilen negatif bir özgürlük kavramını benimser ve yayarlar; bu kavram, devletlerin sorumluluğunu ortadan kaldırır ve bireylerin kendilerini gözetimden ve teknokratik otoriterlikten korumak ve çevrimiçi konuşma özgürlüklerini kullanmak istemeleri durumunda sorumluluğu onların omuzlarına yükler. Bu negatif özgürlük kavramı, bilgi rejimindeki olumluluk buyruklarıyla uyumlu olarak işler. Olumluluk, yansımadaki olumsuzluğu ortadan kaldırır; yasaklama ve baskı yoluyla değil, baştan çıkarma ve teşvik yoluyla işler. Burada birey, başarıdan tek başına sorumludur; o bir başarı-öznesidir. Başarmak ve başarılı olmak sorumluluğunu taşır. Dolayısıyla, yine, sürekli yeniden şekillenen ve sürekli hareket halinde olan, "özgür" bir özne olarak bir girişimci projesidir. Böylece, sürekli kendini ifşa eden ve kendini aydınlatan bu "ifadeli benliği" (Coleman & Golub, 2008) benimser. Ancak bu, liberalizmden ziyade neoliberal bilgi rejiminin buyruklarına daha uygun bir şekilde gerçekleşir. Cypherpunklar bu bağlamda gözetim rejimi içinde yer alırlar. Psikopolitik rejimin buyrukları doğrultusunda hareket ederler. Ustanın mantığını güçlendirirler - ustayı alt etmek için ustasının araçlarını kullanmaya çalışırken. Han'ın ifade ettiği "özgürlük krizi"ni şiddetlendirirler. Onu yaratan rejimin mantığına karşı çıkmaya çalışırken özgürlük yanılmasını yayarlar. Bu kısmen, Cypherpunkların (teknoloji karşıtı gözetimci olarak) bilgi rejiminin diğer teknoloji güçleriyle paylaştığı ortak öncüller ve ideolojik varsayımlardan kaynaklanmaktadır. Aşağıdaki tartışmada, Cypherpunkların ortaya çıktığı bağlam ve ideoloji olan Kaliforniya İdeolojisi'ni inceleyeceğim.

Cypherpunks, böylece özgürlük krizini güçlendirirken, buna neden olan gözetim rejimine karşı koymaya çalışıyor. Grup, iddia ettiği gibi bilgi rejimini rahatsız etmek için siyasi bir irade ile sonuçlanabilecek kolektif bir eyleme yol açacak şekilde

faaliyet göstermemektedir. Daha çok sürüsü gibi çalışır. Zaman açısından ısrarcı olmalarına rağmen, dijital iletişime güvenmeleri, grubun üyelerini izole etmekle sonuçlanır. Prekaritelerini devam ettiren, onları daha da izole eden bir sisteme yerleştirilen digeratilerdir. Onlar çalışan ve elitist eşitlerden oluşan bir sistem arayan sürüler. Bu kabilecilik, kolektif bir eylem için gerekli olan bir ruhu, kolektif bir iradeyi ortaya çıkarmaktan acizdir. Dahası, Dataist dünya görüşüne hakim olan davranışsalcılığın zorunluluklarını benimsedikleri ölçüde bilgi rejimi içindedir. Bu dünya görüşünde politika, yaşamın büyük şeması göz önüne alındığında önemli olmayan ikincil bir konuma indirgenmiştir. Hepsi, yaşamı ilerletme gücü olan teknolojinin kullanımıyla optimize edilebilir ve işlevsel hale getirilebilir. Diğer‘aracılığıyla gerçekleştirilen yansıma, akıl yürütme ve ’ özgürlüğü anlamsız hale gelir. Bu söyleniyor ki, Cypherpunkların muhalif karakterleri onları düpedüz Dataistler yapmaz. Davranışçı eğilimleri, sahip oldukları özgürlükçü etkilerle hafifletilir. Dahası, sundukları Şeffaflık zorunluluğunun eleştirisi (gizlilik kavramsallaştırması ve toplumdaki yeri aracılığıyla), onu bilgi rejiminden ayırır ve bilgi rejiminin zorunluluklarını pekiştirmedeki rollerini azaltır. Bu nedenle, gözetleme rejimine karşı kolektif bir eylemde bulunamazken, Siberpunklar tarihleri boyunca olumlu sonuçlar üretebildiler. Sonuçları mevcut durum üzerinde iyileştirici bir etkiye sahipti, ancak Jacques Ranciere'in muhalif olarak adlandırdığı şeyin bir anımı oluşturmuyorlar, gerçekten demokratik bir moment—a mevcut güç ilişkilerinde gerçekten sorgulanıyor ve rahatsız ediliyor.

Cypherpunks gözetim rejimi içinde yer almaktadır. Psikopolitik rejimin zorunlulukları boyunca faaliyet gösterirler. Master—'ın mantığını güçlendiriyorlar, buna karşı master's araçlarını kullanarak karşı koymaya çalışıyorlar. Freedom‘ın ’ krizini şiddetlendiriyorlar (Han tarafından dile getirildiği gibi). Kendisini yaratan rejimin mantığına karşı koymaya çalışırken özgürlük yanılısamasını yayarlar. Bu kısmen, Cypherpunkların (teknolog bir karşı gözetim olmak) bilgi rejiminin diğer teknoloji güçleriyle ortak olduğu ortak öncüllerden ve ideolojik varsayımlardan kaynaklanmaktadır. Bu söyleniyor ki, Cypherpunkların muhalif karakterleri onları doğrudan Dataist ya da bilgi rejiminin savunucuları yapmıyor. Davranışçı eğilimleri, sahip oldukları liberter veya anarşist etkilerle hafifletilir. Dahası, sundukları şeffaflık zorunluluğunun eleştirisi (gizlilik kavramsallaştırması ve toplumdaki yeri

aracılıđıyla), onu muhalif bir güç olarak bilgi rejiminden ayırır ve bilgi rejiminin zorunluluklarını pekiştirmedeki rollerini azaltır. Bu nedenle, gözetleme rejimine karşı kolektif bir eylemde bulunamazken, Cypherpunks tarihleri boyunca olumlu sonuçlar üretebildiler. Sonuçları mevcut durum üzerinde iyileştirici bir etkiye sahipti, ancak Jacques Ranciere'in muhalif olarak adlandırdığı şeyin bir anını oluşturmuyorlar, gerçekten demokratik bir moment—a mevcut güç ilişkilerinde gerçekten sorgulanıyor ve rahatsız ediliyor.

## B. THESIS PERMISSION FORM / TEZ İZİN FORMU

(Please fill out this form on computer. Double click on the boxes to fill them)

### ENSTİTÜ / INSTITUTE

- Fen Bilimleri Enstitüsü** / Graduate School of Natural and Applied Sciences
- Sosyal Bilimler Enstitüsü** / Graduate School of Social Sciences
- Uygulamalı Matematik Enstitüsü** / Graduate School of Applied Mathematics
- Enformatik Enstitüsü** / Graduate School of Informatics
- Deniz Bilimleri Enstitüsü** / Graduate School of Marine Sciences

### YAZARIN / AUTHOR

**Soyadı** / Surname : AL-MADHOUN  
**Adı** / Name : AHMED M. R.  
**Bölümü** / Department : Uluslararası İlişkiler / International Relations

**TEZİN ADI / TITLE OF THE THESIS (İngilizce / English):** RETHINKING SURVEILLANCE AND COUNTER-SURVEILLANCE IN THE ERA OF BIG DATA: THE CASE OF CYPHERPUNKS

**TEZİN TÜRÜ / DEGREE:** **Yüksek Lisans / Master**  **Doktora / PhD**

- Tezin tamamı dünya çapında erişime açılacaktır.** / Release the entire work immediately for access worldwide.
- Tez iki yıl süreyle erişime kapalı olacaktır.** / Secure the entire work for patent and/or proprietary purposes for a period of **two years**. \*
- Tez altı ay süreyle erişime kapalı olacaktır.** / Secure the entire work for period of **six months**. \*

\* Enstitü Yönetim Kurulu kararının basılı kopyası tezle birlikte kütüphaneye teslim edilecektir. / A copy of the decision of the Institute Administrative Committee will be delivered to the library together with the printed thesis.

**Yazarın imzası / Signature** ..... **Tarih / Date** .....

(Kütüphaneye teslim ettiğiniz tarih. Elle doldurulacaktır.)  
(Library submission date. Please fill out by hand.)

*Tezin son sayfasıdır. / This is the last page of the thesis/dissertation.*