ZUZANNA SONENBERG

The electronic and economic mass surveillance of GAFAM

MASTER'S THESIS

Written under the guidance of Professor François-Xavier de Vaujany

To be presented for public discussion at Université Paris-Dauphine on 6th of September 2019

UNIVERSITE PARIS-DAUPHINE

Year 2018-2019

ABSTRACT

The “datafication” of the world has accelerated with its digitization, leading to the emergence of private actors able to capture its value. New market entrants such as GAFAM (Google, Apple, Facebook, Amazon, Microsoft) developed business models powered by personal data. However, these “free” digital services turned out to be at the same time powerful weapons of surveillance. The continuous aggregation of personal data allows them to track their users anywhere at any time. This thesis proposes an analysis of the surveillance and control system set up by digital platforms by mobilizing the concepts of Michel Foucault, Gilles Deleuze, Antoinette Rouveroy and Shoshana Zuboff, in order to understand its functioning. In order to confront the conceptual framework with reality, a quantitative study was conducted to understand the online habits and perceptions that individuals have of GAFAM. Although the study illustrates the lucidity of users on the need to protect themselves against the risks associated with data extraction, it also highlights the lack of knowledge of alternative solutions and the lack of reflection on individual responsibility in modern surveillance capitalism.

KEYWORDS

Mass surveillance, GAFAM, panopticon, society of control, electronic collar, surveillance capitalism, algorithmic governmentality, information and communication technologies (ICT), personal data, tracking, privacy in the digital age

ACKNOWLEDGEMENTS

Before I start the presentation and explanation of the topic covered in this thesis, I would like to thank all those who have, directly or indirectly, contributed to it.

First of all, I would like to thank my supervisor Mr. François-Xavier de Vaujany, Professor of Management at Université Paris-Dauphine, who has directed my work over the past ten months. He made himself available and was responsive in answering to my questions. Throughout the year, he has been a great help to me and had provided valuable ideas that allowed me to acquire better comprehension of my subject. Thanks to him, I was able to reach and interview some specialists, who guided me in my research.

I would like to express all my gratitude to Hugo Roumillac, who has helped me throughout the year. The time he has spent to assist me in my reflection, in the construction of the research question and the structure, as well as in the analysis of the results, was decisive for the realization and the final outcome of this work. His dynamism and positivism made me want to continue my efforts. This thesis would have never been written without him.

In addition, I would like to extend my thanks to all the interviewees, all the people who answered to my survey and all other persons who guided and helped me in this process. Thank you for your time, attention and help, for valuable comments and advice, and especially constructive criticism that allowed me to reach this final result.

I would also like to thank my friends and family for their unconditional support throughout the year. They encouraged me in difficult times. A special thank for Hugo's parents who massively shared my questionnaire.

Finally, I would like to thank Université Paris-Dauphine, as I was able to write this thesis in the context of the master's degree diploma.

Thank you all.

TABLE OF CONTENT

TABLE OF CONTENT **4**

LIST OF TABLES **7**

LIST OF FIGURES **8**

LIST OF ABBREVIATIONS **9**

1. INTRODUCTION **10**

1.1. Opening remarks **10**

1.2. Motivation of the research **11**

1.2.1. Thesis genesis 11

1.2.2. Links with social science fiction 11

1.3. Definitions and research objectives **12**

1.4. Thesis structure **15**

2. LITERATURE REVIEW **16**

2.1. GAFAM electronic surveillance: between the theories of Michel Foucault and Gilles Deleuze **16**

2.1.1. The Foucauldian *panopticon* 16

2.1.2. Deleuze's interpretation and the *society of control* 19

2.1.3. Traceability and the *electronic collar* 22

2.2. Merchandising of personal data: an economic surveillance for the benefit of GAFAM **25**

2.2.1. A Business Model entirely based on personal data 25

2.2.2. An algorithmic *biopower* for financial purposes 30

2.2.3. *Surveillance capitalism* 33

2.3. GAFAM's monopole and hyperpower **37**

2.3.1. From attention economy to addiction economy 37

2.3.2. Concentration of power and the lack of alternatives 39

2.3.3. GAFAM dictatorship: a regime allowed by people's consent 41

2.4. Research modeling **45**

2.6. Resulting assumptions 46

3. RESEARCH METHODOLOGY 48

3.1. Research objectives 48

3.2. Research design: the survey methodology 48

3.2.1. Presentation of the survey methodology 49

3.2.2. The added value of the method 50

3.3. Data collection 51

3.3.1. The exploratory interviews 52

3.3.2. The online questionnaire 55

3.4. Data treatment and analysis 57

3.4.1. The exploratory interviews 57

3.4.2. The online questionnaire 58

4. RESULTS 59

4.1. Assumptions to be tested 59

4.2. Modern electronic collars ownership 59

4.3. Personal data value 61

4.4. GAFAM addiction 64

4.5. The lack of alternatives 67

4.6. The consent to surveillance and control 69

5. DISCUSSION 72

5.1. Theoretical inputs 72

5.2. Methodological inputs 73

5.3. Empirical inputs 73

5.4. Management recommendations 75

5.5. Limitations 77

5.5.1. Data collection 77

5.5.2. Data analysis 80

5.6. Future research avenues 82

6. CONCLUSION 85

6.1. A brief synthesis 85

6.2. Closing personal remarks 85

7. REFERENCES 86

7.1. Publications 86

7.2. Scientific articles 87

7.3. Reports 90

7.4. Sitography 91

7.5. Radio broadcasts 92

8. APPENDICES 93

Appendix 1 – Interview guide and interview summary 93

Appendix 2 – Interview summary 96

Appendix 3 – Interview Transcript #1 97

Appendix 4 – Interview Transcript #2 103

Appendix 5 – Interview Transcript #3 114

Appendix 6 – Interview Transcript #4 129

Appendix 7 – Interview Transcript #5 136

Appendix 8 – Online questionnaire 141

Appendix 9 – Results of the online questionnaire 147

LIST OF TABLES

Table 1: Interviewees – Academics **53**
Table 2: Interviewees – Knowledgeable **54**
Table 3: Comparison of the collected data with the official INSEE data (2016) **79**

LIST OF FIGURES

Figure 1: GAFAM Business Model 27
Figure 2: Holders of connected watch by sex and age 60
Figure 3: Proportion of users who do not accept the use of data for personalized services among those who accept the general conditions of use 62
Figure 4: Proportion of users who are against giving data to receive free services among those who accept the general conditions of use 62
Figure 5: Monetary value of personal data depending on the perception of data as a market good 63
Figure 6: Proportion of users who would be willing to pay for using GAFAM services among those who consider these services as irreplaceable 65
Figure 7: Proportion of users who think that GAFAM are irreplaceable among those who think they do not have competitors 67
Figure 8: Proportion of users who think that GAFAM have competitors among those who are familiar with free software 68
Figure 9: Percentage of users who accept the general terms and conditions of use among those who believe they do not have control over their data 69
Figure 10: Proportion of users who accept the general conditions of use among those who believe that the level of GAFAM intrusion into private life is too high 70

LIST OF ABBREVIATIONS

AWS: Amazon Web Services

CNIL: Commission Nationale de l'Informatique et des Libertés

GAFAM: Google, Apple, Facebook, Amazon, Microsoft

GDPR: General Data Protection Regulation

ICT: Information and Communication Technology

IoT: Internet of Things

INSEE: Institut National de la Statistique et des Études Économiques

IT: Information Technology

1. INTRODUCTION

1.1. Opening remarks

The publication of several press articles during the summer of 2019 about the wiretapping of some conversations or requests made by users of voice assistants such as Siri, Alexa, Google Assistant or Facebook Messenger made a lot of noise. Individuals have discovered that this practice is widespread among large digital companies: sound clips, sometimes notably private, are transmitted to subcontractors so that they can transcribe the content of audio recordings. Transcriptions are then used, through the identification of keywords, to refine advertising targeting and better calibrate users' news feeds according to their interests (Dekonink, 2019).

However, isn't wiretapping a process usually used by the police or by an official intelligence authority? Doesn't it require prior judicial authorization to be legal? How can this usually highly regulated practice be exercised by private companies? Apparently, GAFAM do not seem to be concerned about the secrecy of correspondence which yet is a fundamental legal principle. To the contrary, they use espionage and state surveillance procedures in order to improve their services.

A situation that would seem to belong to the *1984* universe, with a modern telescreen capturing all the sounds emitted by individuals (Orwell, 1949). Like Winston, as long as the user remains in the field of view of the GAFAM (Google, Apple, Facebook, Amazon, Microsoft) digital devices, he can be seen as well as heard, and "*there is of course no way of knowing whether you are being watched at any given moment"* (Orwell, 1949). For indeed, as the Thought Police, digital giants monitor their users, the media revelations about the listening of voice conversations prove this state of affairs and the difficult if not non-existent relationship they have with privacy protection. Thus, just as in Orwelian dystopia "*you have to live - did live, from habit that became instinct - in the assumption that every sound you make is overheard, and, except in darkness, every movement scrutinized*" (Orwell, 1949).

1.2. Motivation of the research

1.2.1. Thesis genesis

The author's interest in modern surveillance operated by the digital companies was born following the publication of Bernard Harcourt's book: *Exposed. Desire and Disobedience in the Digital Age*. Harcourt stated that no one can self-describes his tastes better than likes, clicks, shares, and purchases on the Internet. He pointed out the fact that what best characterizes people is their data and drew attention to the new virtual transparence to which users are exposed. Indeed, these data are used by a power that is not constituted by the State but by a combination of private actors in order to increase their market shares and rentability. According to Harcourt, we are building an "expository society" with an unprecedented level of exhibition, watching, and influence, within which we become unfree, however we seem not to care about it at all. To the contrary, we crave exposure and knowingly surrender our privacy and anonymity in order to benefit from convenient digital services.

Sounds scary. This book has enabled the author to become aware, for the first time, of the dangers of the Internet and the potential harmful consequences that digital technologies may have on the contemporary society. Indeed, one can notice that, although the growing number of whistleblowers and media scandals about the violation of privacy by digital platforms, nobody seems to be really concerned about them. Permanent digital distraction and the convenience offered by these services prevent individuals from thinking and questioning the real functioning of Internet companies.

1.2.2. Links with social science fiction[1]

Further analysis of the subject reveals that, as mentioned before (see 1.1 Opening remarks), the current situation has many similarities with dystopian fictions, especially with two major books:

[1] "*Narratives that extrapolate from current social science concepts in order to predict or speculate about the future shape of society*". Social Science Fiction, Encyclopedia.com, [Online] Retrieved from: https://www.encyclopedia.com/social-sciences/applied-and-social-sciences-magazines/social-science-fiction

George Orwell's *1984* and Aldous Huxley's *Brave New World.* The first describes a totalitarian regime with an ubiquitous eye embodied by Big Brother, where all thoughts are carefully monitored and freedom of speech do not longer exist ; the second presents a world where happiness and pleasure are law, a hierarchical society conditioned from the embryonic stage to feel and think in a way "in conformity" with its caste so that any rebellion is psychically impossible.

The use of new technologies and GAFAM services underlines that we are currently living on the border of the two worlds: a society made up of digital entertainment that makes life easier for users by fulfilling all their desires, but at the same time framed by an ubiquitous eye that monitors every move and action and listens to our most intimate secrets. As everyone emphasizes the many virtues of digital services, no one is questioning nor trying to overthrow the system in place. To the contrary, people continue to comply with the totalitarian power of the GAFAM, ignoring the hidden side of these actors.

This observation leads the author to carry out this research work in order to better understand the organization and functioning of surveillance conducted by private digital companies nowadays.

1.3. Definitions and research objectives

The advent of the World Wide Web and digital technologies has distress people's lives. With this technological change, everything has become faster, more accessible et efficient. Many digital services have appeared, radically changing the daily lives of its users.

By surfing the web - the new online space - individuals create a second identity for themselves. The "*Homo Digitalis"* (Harcourt, 2015), the virtual and immortal double of each Internet user, that may remind the immortal body of the monarch as exposed in the two bodies of the King theory (Kantorowicz, 1957), continuously generates digital traces. These traces, also known as personal data, are according to the CNIL: "*any information related to an identified or identifiable individual. As it concerns people, that information must remain under their control"*[2].

[2] Personal data, CNIL Website, [Online] Retrieved from: https://www.cnil.fr/fr/definition/donnee-personnelle

It is also defined as: "*traces of interactions with a digital device that are at the origin of the value of the digital service*" (Isaac, 2018). As it generates value, personal data have become the black gold of the 21st century (Cercy and Nitot, 2016; Paquette 2018), a new form of capital (Rouveroy, 2017) coveted by a growing number of actors. Private companies, like GAFAM (Google, Apple, Facebook, Amazon, Microsoft), have built vast empires and developed business models powered by individuals' personal data. Those companies share common characteristics: they are all American, however deeply globalized in their activities and strongly financialized. Indeed, they represent the world's largest market capitalizations (NASDAQ Companies, 2019). They form a global oligopoly and continue to extend their grip on the Internet, in order to maintain their hegemony and generate exceptional and ever-increasing profitability. As an example, Facebook has 2,234 billion active users per month in 2019, while the companies it owns account for 1500 billion users for WhatsApp, 1300 billion for Messenger and 1 billion for Instagram (Hervé, 2019); more than 1.3 billion Apple products (iPhone, iPod, iPad, Apple TV and Apple Watch) are in use around the world in 2018 (Marchand, 2018); Google covers 90% of the search engines market share (Coëffé, 2018) while Microsoft covers 90% of the operating system world market share (Auffray, 2019). It is now obvious that those services have become essential and indispensable to the daily life of the majority of world citizens, who could not imagine not having them anymore.

However, under the guise of convenience, these digital services are proving to be at the same time powerful weapons of surveillance. The notion of surveillance is here understood as "*any focused attention to personal details for the purposes of influence, management, or control*" (Lyon, 2007). Indeed, the collection and aggregation of personal data allows GAFAM to track their users anywhere at any time. Thanks to the huge amount of digital information, they are able to draw up a faithful profile of each of their user in order to influence his choices and offer personalized content. Those companies are thus in the position to manipulate opinions and actions, to shape human behaviors and "*can be seen as tools and practices for social control*" (Ball *et al.*, 2006). Moreover, GAFAM collect and appropriate what does not belong to them. As said above, personal data relates to people and have to remain under their control, but in fact, they are dispossessed of their property. Private companies make profit and increase their power on the back of individuals, who are most of the time, unaware of the situation. The merchandizing of people's digital traces and the resale of personal data to third parties allow those companies to finance themselves.

The extent of data collection and the resulting monitoring are difficult to perceive for individuals, since it is painless and largely done without their knowledge, or at least without their consent being truly informed (Charmet, 2016). Individuals do not perceive the hidden side of GAFAM, as the free nature of their services divert their attention from the implicit presence of surveillance and control.

The crux of the problem is users' consent, their free willingness and strong desire to expose themselves online (Harcourt, 2015). Unconsciously, individuals are accomplices in this surveillance. Big Brother is not just watching you, it feeds on the information that Internet users voluntarily offer to him. Individuals "*feed the beast*" (Mao in Delorme, 2016) by submitting to the conditions of use of GAFAM services without paying attention to consequences. They do not perceive their digital vulnerability, their lack of digital sovereignty and autonomy. Unaware of the danger, they continue "*to put themselves on the screen"* (Harcourt in Bourmeau, 2016). This voluntary servitude (La Boétie, 1546) deprives them of their fundamental rights, as they wilfully renounce to their privacy.

Thus, the development of the digital era and the new distribution of power that supports it have been achieved in parallel with the erosion of humanist values: the preservation and defense of privacy, which are fundamental Human Rights. Indeed, the power held by GAFAM is unprecedented and very extensive. Antoinette Rouveroy (2017) talks about the hyperpower of these actors and their digital imperialism. Nothing seems to stop them. They are deeply rooted in the contemporary society. Faced with an omnipotent opponent, Internet users feel powerless, accepting the non-choice of the GAFAM dictatorship.

In this context, this research thesis sets out to understand the functioning of the surveillance system conducted by private digital companies with the following research question:

"***How did GAFAM impose an invisible system of surveillance and control, which structures the society of the 21st century?***"

1.4. Thesis structure

The first step will be to provide an overview of existing and relevant literature pertaining to surveillance, control and merchandizing of individuals' personal data, and the identification of theoretical concepts that may be applied to GAFAM practices (**Part 2**).

Thereafter, the selected research methodology is presented in order to describe the procedure applied to the fieldwork and used to answer the research question. The reasons why this specific research strategy has been chosen, data collection, data treatment and analysis method are outlined in this section (**Part 3**).

In order to present the contribution of this work to the object of study and provide concrete evidences, an analysis of the results achieved from the empirical research is exposed. The data collected thanks to the online questionnaire is processed and interpreted in order to provide the most accurate analysis of people's digital uses. All the insights are then used to draw conclusions and identify the measures that should be followed (**Part 4**).

Finally, theoretical, methodological and empirical contributions of this work are presented in order to highlight the inputs of the thesis. Then, management recommendations are described, reflecting the author's point of view on the approach that should be followed. Reflections on future research topics which have emerged during the research process are also exposed, as well as all the limitations of the research that must be considered by the reader (**Part 5**).

2. LITERATURE REVIEW

2.1. GAFAM electronic surveillance: between the theories of Michel Foucault and Gilles Deleuze

The use of digital tools and the way people expose themselves on the web make them easily observable. Digital traces make possible an electronic surveillance of Internet users (Haggerty and Ericson, 2000; Lyon, 2007, 2010; Richards, 2013). A practice that was once reserved to people on the margins of the society like suspects or deviants, has become extended to cover the majority of the population, which can nowadays be categorized, analyzed and targeted (Ball *et al.*, 2006).

2.1.1. The Foucauldian *panopticon*

In the 18th century, Jeremy Bentham imagined a prison architecture called the Panopticon. This structure consists of a building with a circular ground plan and a central tower that allows the person who sits inside to have a panoramic view of the whole. Its objective is to allow a guard, housed in the central tower, to observe all the prisoners, locked in individual cells around the tower, who are unable to know if they are being observed. This system is based on the principles of continuous visibility, which leads detainees to believe that they can be constantly monitored, without never really knowing it.

The philosopher Michel Foucault takes up the concept of the Panopticon in his book *Discipline and Punish* (1975). According to Foucault, the Panopticon reflects a metaphor, that of the disciplinary society, based on the principles of permanent visibility, normalization and individualization of behaviors (Leclercq-Vandelannoitte, 2017). Knowing that he is being watched, the subject integrates himself the constraints of the power, and thus becomes the principle of his own subjection (Milburn, 2007). The major effect of the Panopticon is "*to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to*

arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action [...] in short, that the inmates should be caught up in a power situation of which they are themselves the bearers" (Foucault, 1975).

The Panopticon appears as the archetype of surveillance (Haggerty and Ericson, 2000; Willcocks, 2006; Leclercq-Vandelannoitte and Isaac, 2013). It can be used to describe recent forms of surveillance that have developed with the widespread use of information and communication technologies (ICTs) and digital companies, as the Foucauldian concept is "*a generalizable model, applicable to any social function, in the sense that it illustrates the daily power relations diffused in the society, which go well beyond the architectural design of the Panopticon*" (Leclercq-Vandelannoitte and Isaac, 2013). It symbolizes the new surveillance mechanisms put in place in the contemporary society.

The constant exposure to observation

The massive adoption of ICT and connected devices as well as the constant use of digital services have given rise to the panoptic power of GAFAM. The Panopticon metaphor can be used to highlight the electronic surveillance operated by digital companies: users are prisoners locked in cells, ICTs and connected devices represent the central tower that provides a panoramic view of everything that is happening, and GAFAM embody the guard watching prisoners in silence without being seen. The observation process remains the same, only the interface required for monitoring changes. Indeed, "*surveillance now involves an interface of technology and corporeality*" (Haggerty and Ericson, 2000) which is a "*surface of contact between organic and non-organic orders, between life forms and webs of information, or between organs/body parts and entry/projection systems*" (Bogard, 1996 in Haggerty and Ericson, 2000). ICTs and connected devices are electronic panopticons (Gordon, 1987 in Haggerty and Ericson, 2000) of the XXI° century with a new particularity: they are "*panopticons without walls*" (Webster and Robins, 1993 in Willcocks, 2006). Indeed, nowadays, "*humans and their eyes do not have to physically operate in the surveillance tower*" (Willcocks, 2006), GAFAM can watch remotely, as these tools transform the individual's private space into a permanently observable field. By making all actions visible, and by allowing to keep a trace of each action performed, ICTs and connected devices strengthen the monitoring of GAFAM, since users become post-visible (Boulay, 2007) through the archiving and storage of personal data.

Thanks to this constant informational transparency (Amintas, 2002) permitted by a continuous monitoring of their users, GAFAM thus have a real electronic panoptic power.

Integration of the norm and self-discipline

According to Foucault, the objective of the Panopticon is to impose self-discipline on prisoners. The potential constant monitoring leads to self-regulation by the persons who are being watched. Subjects internalize and comply with surveillance standards, as "*panoptic surveillance targets the soul, disciplining the masses into a form of self-monitoring*" (Haggerty and Ericson, 2000). Indeed, the Panopticon is more than a simple device for observation, it works "*in conjunction with explicitly articulated behavioral norms*" (*Ibid.*, 2000). By using ICTs and connected devices, individuals accept all the conditions required and thus submit in the same way to the monitoring that results from them. According to Poster (1990, in Willcocks, 2006), "*the populace has been disciplined to surveillance and participating in the process [...] it participates in its own self-constitution as subjects of the normalizing gaze of the superpanopticon*". Poster's superpanopticon relies to the modern form of surveillance based on computerized databases and information technologies (IT). This modern monitoring that targets behaviors, helps to build individuals as manageable and malleable people (Amintas, 2002). Thanks to the panoptic metaphor, "*Foucault reminds us, how much human use of ICT is a will toward control, certainty, and knowledge*" (Willcocks, 2006).

Nevertheless, the comparison between GAFAM and the Panopticon has some limitations. Indeed, the panoptic structure is fixed and operates in a closed environment: a place where isolated prisoners are confined in individual cells. On the contrary, users of digital platforms live in an open environment and interact with each other. Moreover, the central tower of the Panopticon is an apparent physical architecture consciously seen by the prisoners. The particularity of modern surveillance technologies lies in their capacity to blend into the background becoming unnoticed and perfectly integrated in the daily lives of the individuals. These differences show that, although the Foucauldian concept is metaphorically adapted to characterize GAFAM surveillance, it must be overcome.

2.1.2. Deleuze's interpretation and the *society of control*

The contemporary surveillance carried out by GAFAM is opening up to more flexible logics and practices. These are allowed by new technologies that add a more advanced level to surveillance: they allow the control of individuals.

Gilles Deleuze is the first to highlight the shift from the disciplinary society of Foucault to a control society of modern times. "*We are entering societies of 'control' which are no longer exactly disciplinary, [...] which no longer function by confinement but by continuous control and instant communication*" (Deleuze, 1990). The modern era has seen the emergence of a new form of power born of the development of information technology (IT). The control society no longer physically encloses individuals but exercises continuous control through ICTs and connected devices. It is characterized by "*ultra-fast forms of open-air control*", which "*replace the old disciplines operating in the duration of a closed system*" (*Ibid.*, 1990). The new form of surveillance put in place is ubiquitous, omnipresent, multi-channel, following the individual wherever he or she may be (Leclercq-Vandelannoitte and Isaac, 2013).

The control society is also characterized by a digital language made up of numbers, which mark access to information. Individuals are no longer masses, but " '*dividuals', samples, [...] data*" (Deleuze, 1990). This data is tracked by GAFAM since it allows to follow the slightest movement of each user. The control society marks the advent of the information society (Willcocks, 2006) and of a new type of individual one comprised of pure information (Haggerty and Ericson, 2000). Digital traces are characteristic of this information society and are collected, processed, categorized and aggregated by digital companies. They come from different sources as new technologies are reticular.

Rhizomatic surveillance

New technologies lead to a rise of network power which replaces the panoptic power of surveillance. This transformation reflects a profound change in supervision and control methods (Bauman and Lyon, 2013).

In the era of the society of control, surveillance is characterized by its "rhizomatic" aspect. Rhizomes are plants with an interconnected vertical root system, as opposed to plants with a single deep root structure. The rhizome metaphor was developed by Deleuze and Guattari in order to clarify and better understand the new forms of electronic surveillance. Indeed, the new monitoring system is based on many varied authorities, all linked to an underlying and invisible infrastructure of interconnected technologies (Leclercq-Vandelannoitte and Isaac, 2013). Two attributes of the rhizome accentuate and underline the functioning of modern surveillant: "*its phenomenal growth through expanding uses, and its leveling effect on hierarchies*" (Haggerty and Ericson, 2000). Far from being limited to a top-down logic as in the Panopticon, surveillance transforms the hierarchies of observation by broadening the view of one another and making the process more vertical. The efficiency of the reticular control system lies in the abolition of hierarchies (Milburn, 2007). Modern power no longer operates through permanent visibility by the superior, but through open-air, rhizomatic, and lateral control, affecting the boundaries between personal life and the outside world (Leclercq-Vandelannoitte and Isaac, 2013).

Moreover, the rhizome "*may be broken, shattered at a given spot, but it will start up again on one of its old lines, or on new lines*" (Deleuze and Guattari, 1987 in Haggerty and Ericson, 2000). According to Haggerty and Ericson, network surveillance has comparable expansive and regenerative qualities. All the attributes of the new monitoring system let the two authors to theorize modern surveillance as a "*surveillant assemblage*". The assemblage reflects "*the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole*" (Haggerty and Ericson, 2000) in order to provide an increased degree of surveillance capacity. The combination of information, objects' and actors' networks gives strength and effectiveness to the new surveillance in terms of normalizing behaviors (Milburn, 2007).

The rhizome metaphor may be transposed to GAFAM surveillance as those companies use an invisible infrastructure of interconnected technologies and services to track their users. As an example, Facebook does not only refer to the users' Facebook accounts to keep an eye on their attitude. The company mobilizes all the services included in its network, both all the owned entities as Messenger, Instagram, and WhatsApp, as well as partner services. This also applies to Google which is declined in various services as Google Search, Gmail, Google Maps, Google Drive, Google Agenda etc., or Apple which offers different devices that can only be synchronized with

each other, encouraging users to invest throughout the fleet: iPhone, iMac, iPod, iPad, iWatch, etc., to benefit from an optimal operation. And these internal networks and interconnected: "Google gives to Apple $9.5 billion each year to put Google Search as the default browser in the iPhone and iPad" [free translation] (Nitot, appendix 7). The network of all digital services provided enable both the companies to monitor and collect massive amounts of data and individuals to watch their peers through social networks.

An apparent freedom under permanent control

The "*surveillant assemblage*" gives rise to a less visible, more subtle form of control, which no longer depends on confinement to be practiced. Movement and freedom replace imprisonment and become the very conditions of control. Indeed, according to Deleuze, freedom in society of control is in fact a "*control mechanism that competes with the hardest confinement*" (Deleuze, 1990). The open environment, the open air, is only an illusion of the gain of freedom (Sabot, 2012). "*The open environment can be understood as an improvement of the prison system rather than as 'human' progress"* (Razac, 2008). Modern control technologies are no more tolerable or preferable than detention practices related to disciplinary technologies (Sabot, 2012). Deleuze's society of control sets up regulatory mechanisms that invest all the areas of human life and whose effectiveness depends on their capacity to blend into the background, to become unnoticed and perfectly integrated in the daily lives of the individuals who form their effective and often benevolent relays (*Ibid.*, 2012). ICTs and connected devices, acquired voluntarily by users, are thus the relays for the remote control and surveillance of GAFAM.

Finally, the society of control, which makes use of means aimed for self-regulation of each individual in his relations with others and the surrounding world, does not constitute any progress compared to the disciplinary society described by Foucault. On the contrary, it prolongs and strengthens the exercise of disciplinary power by "*extending it even outside the walls*" (Sabot, 2012). Indeed, according to Sabot (2012), "*the control society is in reality an open prison, a space where control (which involves subtle forms of surveillance) takes over from punishment to reach (in order to treat them, as information is treated) behaviors, individualities (dangerous or vulnerable) that have so far escaped any control*".

This new form of distant domination penetrates intimacy to a higher degree and implies an agreed subjection of the individual. Subjectivity is an element of manipulation. Through their connected services, GAFAM are able to control and influence the behavior of users who have previously consented to this co-constructed monitoring. Within this "*open prison*", nothing is left to chance, the slightest movement is now tracked.

2.1.3. Traceability and the *electronic collar*

ICTs and connected devices share an important aspect: they are both mobile. They can be transported anywhere at any time and thus follow individuals in their constant movements. Modern surveillance operated through those tools is carried out on subjects in action in the open air. Each move is analyzed and processed remotely, which generates a "*flow control*" (Munro, 2000 in Leclercq-Vandelannoitte and Isaac, 2013).

The Deleuzian reading of modern surveillance technologies reflects with great acuity the traceability of actions in real time, aloof. Such traceability is made possible by the massive use of sophisticated digital tools, based on geolocation. To characterize those tools that allow a permanent tracking, Deleuze uses the concept of "*electronic collar"*. The latter is "*a control mechanism that gives at each moment the position of an element in an open environment, an animal in a reserve, a man in a company [...] the computer identifies the position of each person, legal or illegal, and operates a universal modulation*" (Deleuze, 1990).

Internet, smartphones, Internet of Things (IoTs), induce a new form of portable surveillance and control. Electronic collars are embodied by mobile phones, GPS, connected watches, social networks that power GAFAM's data factories. Connected machines are the snitches of digital companies and the services and applications that supply them are "*Trojan horses"* that individuals voluntarily place in their pockets (Nitot, appendix 7). The electronic collar is only a camouflaged version of electronic bracelets of the penitentiary system, which reflect "*the transition from a logic of confinement and exclusion (linked to closed environments) to a logic of traceability (linked to the fine control of individuals' movements)*" (Sabot, 2012). It is both a tool for liberation and autonomy, but also a vector for distant surveillance. The electronic collar virtualizes control and allows an extension of the prison space more than it replaces it (Razac, 2008). This system has no time or space constraints, since the connected tools record, translate, and make visible human

behaviors continuously, thus providing universal transparency. Paradoxically, as disciplinary power becomes less visible, individuals and their behaviors become more and more visible (Leclercq-Vandelannoitte, 2017).

According to Alain Damasio (in Nitot and Cercy, 2016), a shift from the society of control to continuous and ubiquitous hyper-control took place at the beginning of the century. This hyper-control is accompanied by cross-control, intra-control, self-data, self-censorship and self-monitoring. The Smartphone is "*the most fantastic self-administered control tool ever designed*" (Damasio, in Nitot and Cercy, 2016), as it embodies the electronic collar, that is to say the ultimate stage of the open prison. However, individuals do not seem to understand this aspect of the tool, which is seen as a daily support for interaction and communication and as a source of information. They wear it voluntarily and agree to be geolocated all the time, while this "*totalitarian nomadic object*" (*Ibid.*, 2016) is the support for a continuous production of data and traces. "*Nothing that is human is no more foreign to the GAFAM. [...] This society of traces has made us incontinent dogs who pee everywhere without knowing it, and us as much as the bloodhounds who sniff these traces in our professions, in our private spheres, to monitor and control what our loved ones do*" (*Ibid.*, 2016).

The electronic collar seen as the *surveillant assemblage* theorized by Haggerty and Ericson (2000) "*brings into the visual register a host of heretofore opaque flows of auditory, scent, chemical, visual, ultraviolet and informational stimuli*" (Haggerty and Ericson, 2000). The visualizing devices make and record discrete constant observations. Thus, the authors take up Rousseau's famous proclamation of *The Social Contract*: "*Man was born free, and he is everywhere in chains*" and update it as: "*Humans are born free, and are immediately electronically monitored*" (Haggerty and Ericson, 2000) by all the electronic collars spread everywhere, producing information, tracking data, making all behaviors visible, recording and categorizing, framing and disseminating internalized norms (Leclercq-Vandelannoitte and Isaac, 2013).

Thus, more than one theoretical perspective is needed to understand GAFAM surveillance. The contemporary society of control refers to unconfinement, movement and freedom in space, the relation to the body is modified since it is no longer a question of training docile bodies but of connecting mobile bodies through network technologies that move and closely follow each individual. There is no pure substitution of society of control for disciplinary society as some disciplinary practices are still in place. The modern era is rather reflected in a strengthening of control within disciplinary society, which implies that Foucauldian disciplinary theories are intertwined with Deleuzian control theories, leading to a hybridization of surveillance and control systems (Leclercq-Vandelannoitte and Isaac, 2013).

Nevertheless, while in the disciplinary society the central power "*conducts the conduct*", shapes bodies with the aim of maintaining order, the objective of GAFAM electronic surveillance is different. The digital world, to the contrary, "*let conduct be conducted*" [free translation] (Cercy, appendix 5) in order to generate as many traces as possible that may be resold and thus generate profit, as modern surveillance is driven by financial imperatives.

2.2. Merchandising of personal data: an economic surveillance for the benefit of GAFAM

Electronic surveillance coordinated by web companies is in fact an economic surveillance more than a disciplinary monitoring. According to Bauman (1992, in Haggerty and Ericson, 2000), panopticism plays the role of social integration nowadays, as subjects instead of being repressed are "*increasingly constituted as consumers and seduced into the market economy. Surveillance is used to construct and monitor consumption patterns*". The purpose of modern monitoring is the reconstruction of a person's actions, habits, behavior and lifestyle in order to establish consumer profiles. All this is possible thanks to personal data.

2.2.1. A Business Model entirely based on personal data

According to the Cambridge Dictionary, a business model is a "*description of the different parts of a business or organization showing how they will work together successfully to make money*"[3]. GAFAM have set up a specific business model based on personal data of their users. It is thanks to data that these companies are able to generate profit. However, the way these five actors are making money is not identical and has some differences. We can establish a dichotomy with Google and Facebook on one side, and Apple, Amazon and Microsoft on the other (Cercy, appendix 5).

Google and Facebook have similar and comparable business models. They are natively digital actors. The collection of personal data is absolutely elementary and necessary for their survival (Nitot, appendix 7). Facebook generates its revenues from its extensive user base and the one coming from its subsidiaries. It collects personal data, then sells it to third parties by putting a price on this virtual material. Facebook's main product is therefore the data of its users. Google and

[3] Business Model, Cambridge Dictionary Website, [Online] Retrieved from: https://dictionary.cambridge.org /dictionary/english/business-model

its entities operate on the same principle: the entry of money is allowed by the resale of personal data collected during the use of the company's services.

Apple, Amazon and Microsoft's revenues are more diversified. Initially, these actors are suppliers of physical market goods. Their business models have gradually been digitized in order to create value through the personal data of their customers. Microsoft sells both hardware and software, but also develops its digital services by offering cloud computing, Bing web browser, LinkedIn social network, and Skype software, which allows it to collect personal data that is then sold to third parties. Amazon is best known for its e-commerce and fast delivery activities, but the company's main source of profit is its subsidiary AWS (Amazon Web Services) specialized in cloud computing services. Other digital services that extract personal data are also available, such as Amazon Alexa: the group's intelligent personal assistant. Apple has a slightly different model as the sales of technological equipment represent the majority of the company's resources. Nevertheless, data capture is very present since all Apple products are interconnected and collect massively information about their users.

Whether primary or secondary, the collection of personal data is an inexorable part of the GAFAM business model. All of them understood the value and use that could be made in order to perpetuate their profitability.

GAFAM user *versus* GAFAM client

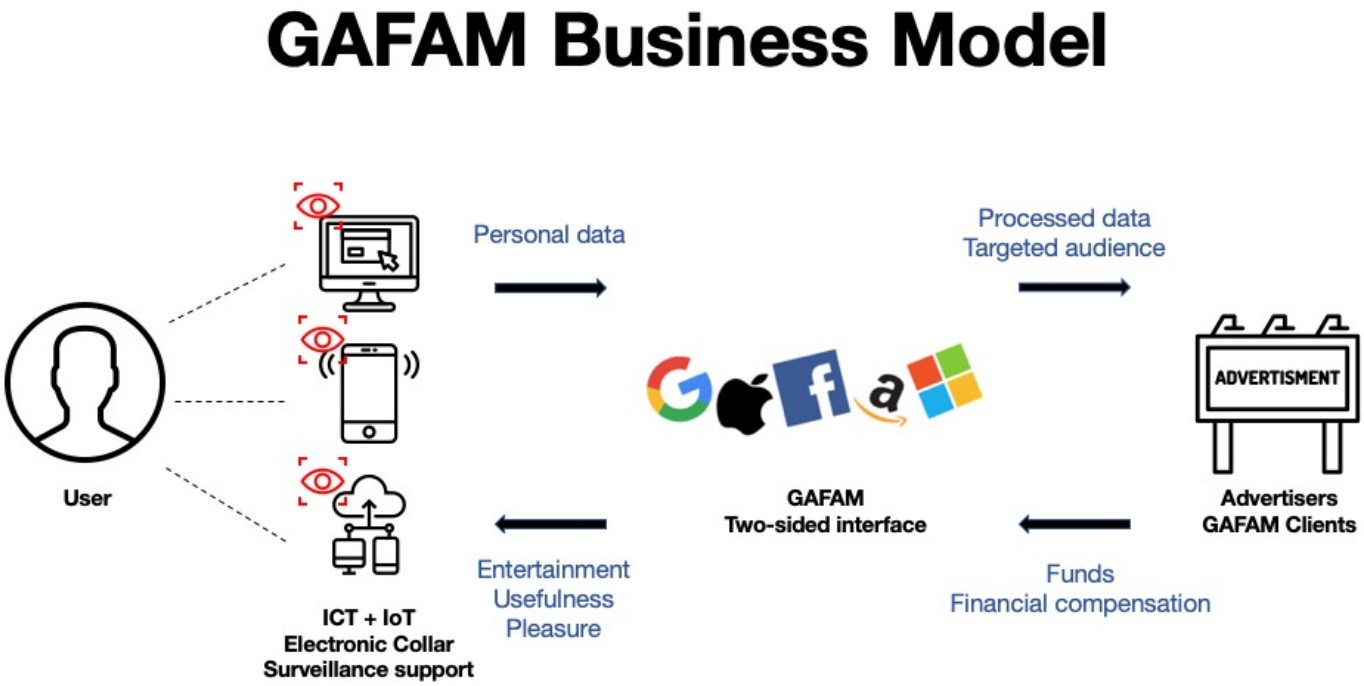
GAFAM's business model consists at first of bringing together a maximum of followers around their services, attracting the highest number of users and transforming the attention paid by the latter into commitment. The use of the services allows a continuous extraction of personal data. This explains the hunt for the number of users.

The second step is for GAFAM to transform user engagement into revenue. Indeed, digital companies create value and find their source of financing in selling the knowledge they have about their users to third party actors who are their real clients. The objective of GAFAM is therefore to extract information, to deduce correlations in order to sell everything to advertisers: the real clients. "*In order to advertise effectively, you have to target. In order to target, you have to monitor people, you have to capture as much data as possible*" [free translation] (Cercy, appendix 5) because this

then helps to maintain people's attention, which is sold to third parties. GAFAM surveillance is carried out with the aim of generating profit above all. "*The consumer surveillance potential on the Internet [...] has made the collection of personal information of millions of consumers a potentially very profitable business*" (Singh and Lyon, 2013).

According to Nina Cercy (appendix 5), individuals have become accustomed to the use of digital services for which they believe they are customers, while the customer relationship between the user and the platform does not exist. Indeed, "*we are the useful idiots of Google and Facebook*" for Tristan Nitot (appendix 7). He caricatures the behavior of GAFAM's users by giving the example of two cows in an enclosed meadow thinking they are fed and housed for free. By considering themselves as customers of digital platforms, individuals understand everything wrong in the same way as these cows. "*We are not their customer; we are their cattle. [...] There are on one side the users and on the other side the advertisers. In the case of platforms, the one who gives real money is the advertiser. The farmer's real customer is the dairy cooperative, not the cows. The raw material is milk to be sold"* [free translation] (Nitot, appendix 7).

Figure 1: GAFAM Business Model



The figure above illustrates the functioning of the GAFAM business model. ICTs and connected devices are the physical interfaces of surveillance, which allow digital companies to monitor their users. These mobile electronic collars give access to digital services which enable the collection and storage of personal data for digital companies, and at the same time allow the users to enjoy useful services. Personal data is processed, analyzed and interpreted and then sold to advertisers. In exchange for the data, GAFAM receive financial compensation. This virtuous circle is based on the black gold of the 21st century (Cercy and Nitot, 2016; Paquette, 2018), which is the personal data.

Personal data value

Users of digital platforms generate data for free. All traces left online and appropriate by companies are free of charge. However, thanks to this raw material, GAFAM are able to make lucrative profits.

Indeed, according to Tristan Nitot, the available digital services are inexpensive. An actor like Facebook "*provides a service for less than 3 euros per user per year*" [free translation] (Nitot, appendix 7). In the case of Google, "*a Western user provides between 60 and 90 euros per year*" [free translation] (*Ibid.*, appendix 7). The margins achieved by digital companies using personal data are therefore considerable given the number of registered users. Indeed, Facebook has 2,234 billion active users per month in 2019, while the companies it owns account for 1500 billion users for WhatsApp, 1300 billion for Messenger and 1 billion for Instagram (Hervé, 2019); Google covers 90% of the search engines market share in 2018, Google Chrome has 750 million active users per month the same year, Gmail 900 million and Android is implemented on 1 billion terminals (Coëffé, 2018).

Every time a person uses a digital service, he or she deliberately provides content by sharing photos, comments, likes. However, in addition to the content, personal data is captured by digital companies without the user's knowledge. "*People did not conceptualize what the data really is. It is invisible and dematerialized, transmitted by WIFI or 4G. [...] The data is captured without the user noticing, such as GPS data for example. When the geographic coordinates are communicated to Google, the user does not receive any notification that informs him*" [free translation] (Nitot,

appendix 7). Thus, a strong imbalance appears in the relationship between the user and the platform, as individuals are not aware of the volume and the value of the information they provide. They give away their personal data for free, which allows GAFAM to record significant gains in exchange of cheap digital services. For Tristan Nitot "*it is like during the slave trade: glassware was given in return for people or land. We took advantage of the fact that the guy in front of you had no idea of how much he was giving and what he was getting in return. Here, it's the same: we give things without understanding their value*" [free translation] (Nitot, appendix 7).

Users are therefore unaware of the value of the personal data collected freely by digital platforms. This poses several problems. First of all, as Tristan Nitot and Jérémy Aroles assert, this underlines the unequal nature of the exchange as the two parties do not have the same degree of knowledge and understanding of the goods exchanged. Moreover, this exchanged good should not be in fact exchanged since it is not a commercial good like any other. Personal data "*are not objects, they are the emanation of a subject, they are the digital traces of a person; the fact of concentrating them as if they were objects goes against of what personal data really is. Data is not just something that we produce, it is something that says a lot about us, it is something that we have but that we are as well, and that for me we cannot sell*" [free translation] (Cercy, appendix 5). Data "*is an outgrowth of the individual*" (Bayard, in Andrade and Mira, 2019). GAFAM therefore appropriate people's attributes through their data and sell them to advertisers.

Nevertheless, some, such as Jaron Lanier (2018), see in these practices something much more worrying than a simple source of funding for the GAFAM. Indeed, targeted advertising made thanks to personal data allows mass manipulation. Indeed, "*the advertising cannot be called advertising anymore as it turned to behavior modification*" (Lanier, 2018). Social networks have become modification empires: "*one cannot live in a society where two people wishing to communicate can only succeed if this communication is financed by a third party, who wishes to manipulate them*" (*Ibid.*, 2018). This manipulation made by GAFAM, which is similar to body dressage and distant control, can be perceived as modern *biopower*.

2.2.2. An algorithmic *biopower* for financial purposes

Biopower was theorized by Michel Foucault in 1976. From the 18th and 19th centuries onwards, the State, as the main producer of data, became capable of acting on reality to rationalize social organizations and discipline populations. The aim was to normalize behaviors that deviate from the established norm by instilling "good practices" in the population through the implementation of specific public policies (Rouveroy, 2018). This life-management-centered way of exercising power is called biopower. Foucault also speaks about governmentality, as the emergence of regulatory mechanisms that regulate the life of bodies and address living subjects is observed. This new power no longer intervenes to kill (repress), but to keep people alive (develop life through mass control) (Ibid., 2018).

According to Antoinette Rouveroy (2018), digital technology takes us far beyond Foucault. By monitoring and capturing individuals' personal data, GAFAM have a detailed knowledge of users' single wish and desire. This allows them to " '*manage the smallest parcels of human life*' as Foucault says" [free translation] (Leclercq-Vandelannoitte, appendix 3) and to manipulate user's choices in order to maximize their profits.

Profiling: categorization and conduct without norms

According to the 4th Article of the General Data Protection Regulation (GDPR), profiling means "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements*"[4]. Profiling is therefore the predictive analysis of a person's behavior. It allows to predict personal habits, purchases and wishes. Thanks to profiling, a company can offer content that is adapted and

[4] Profiling, Article 4 EU GDPR "Definitions", [Online] Retrieved from: http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm

interesting to the profiled person. This method is therefore one of the biggest challenges of Big Data.

GAFAM users are constructed as "*objects of knowledge by marketers through the use of Internet technologies of surveillance and individuation*" (Humphreys, 2006). All the collected data is used to predict, shape and determine future desires of the individuals. Indeed, " *'digital aggregators' involved in the experience of surveillance, connect pieces of various puzzles that consumers leave in different databases, such as names, social security numbers, past residential addresses, credit histories, lifestyle information and various details of friends or associates*" (Singh and Lyon, 2013). All these information gives the opportunity to digital companies to formulate "data doubles" (Haggerty and Ericson, 2000; Singh and Lyon, 2013) and classify individuals. According to Humphreys (2006), who examines the marketing practices employed by Amazon, "*just as in an asylum all individuals exhibiting the same tendencies are classified into groups, the Amazon.com Wish List classifies individuals according to shopping habits and consumer tendencies*". GAFAM therefore create standard profiles and categorize their users by cloistering them in specific "boxes". Indeed, digital actors "*know so much about us, they can almost see through us*": the users become "*glass consumers*" (Lace, 2005 in Singh and Lyon, 2013). Thus, through profiling, GAFAM have the possibility to modify individuals' actions. They do not act directly on subjects, but on their future actions. The opportunity of guiding action and putting in order its possible results is Michel Foucault's definition of power according to Amintas (2002). GAFAM are thus conditioning individuals in a certain way.

However, while Foucauldian biopower wants to normalize behaviors by instilling "good practices", GAFAM's biopower "*have little normative claim*" (Humphreys, 2006). In the case of Amazon, its agenda is to "*fulfill your desires, not repress them or correct them to a norm. There are no objectively correct or even normal preferences in the mind of Amazon.com. […] [The purpose] is to encourage and profit from tendencies of the consumer*" (*Ibid.*, 2006). According to Cercy (appendix 5), GAFAM do not want the user to censor himself. On the contrary, they wish to offer the largest freedom of choice to individuals, as it allows to define people's interests more precisely and then sell their profile more expensively. *"Google doesn't care about selling you red or blue shoes, the only thing it wants is to make sure that your purchasing behavior is consistent with the profile it has established of you"* [free translation] (Cercy, appendix 5). GAFAM therefore do not impose normalized conduct or regulated discipline, they "*let conduct be conducted in order to derive an economic value*" [free translation] (*Ibid.*, appendix 5). According to Cercy (appendix

5), "*profiling is a conduct without norms, a conduct that is normalized by nothing else than the conduct of others, [which is] extremely dangerous because it gives rise to a very strong conformism*".

Algorithmic governmentality

GAFAM's electronic surveillance which allow profiling is comprised of algorithms that storage, retrieval and process data. Algorithms are "*a set of operating rules whose application makes it possible to solve a problem*"[5]. An algorithm can be translated, using a programming language, into a program that can be executed by a computer. This is exactly what GAFAM do in order to analyze all the data collected on their users. Thanks to algorithmic calculations, they are able to profile and assort individuals into categories. Algorithms are at the heart of data processing today.

However, according to Antoinette Rouveroy, algorithms are not only about processing information, they govern people (2017). Indeed, according to Paquette (2018), with the new configurations brought by Big Data, a transition from the society of control to an algorithmic society has occurred. The logic instituted by the algorithmic society has set up an algorithmic governmentality which is a "*mode of governance of conduct based on quantifiable digital data. The objective is not to manage the present but to protect against uncertainty and the future. We no longer govern rational subjects but control speculative space by analyzing an individual's potential to adopt a particular behavior*" (Rouveroy, 2017). In this algorithmic society, individuals are understood as transmitters of digital data, of computable signals. The signals produced are similar to traces left by animals, traces that they can neither prevent themselves from emitting nor erase. They are "*a kind of digital pheromones that fuel algorithms, which identify statistically significant correlations within the gigantic masses of data that are used to produce behavioral models*" (*Ibid.*, 2017). Algorithmic governmentality anticipates future behavior and thus predicts the future in general. "*The process of formalization and expression of desire is short-circuited*" (Rouveroy,

[5] Algorithm, the Larousse Dictionary, [Online] Retrieved from: https://www.larousse.fr/dictionnaires/francais/algorithme/2238

2018). Thanks to their algorithms, GAFAM guide the consumption choices of their users, because they "*connect directly to their pre-conscious impulses and thus produce the passage to the act of purchase by minimizing prior reflection*" (*Ibid.*, 2018). The individual is thus deprived of his or her free will and ability to make choices in an individual and reasoned way.

This technique is a form of control of the future. GAFAM want to "*offer the consumer the illusion of autonomous choice. Realistically, this illusion is the source of constituting control over consumers. The strategy is that this control, and its implementation, do not necessarily leave the consumer with the feeling of subordination; […] this is a kind of control which represents consumers' active participation in self-manipulation*" (Singh and Lyon, 2013). Algorithmic governmentality is a control device that deprives the individual of a part of autonomy, without him noticing it. It is an unconscious mechanism. The algorithmic society is based on programmed recommendations, as "*Big Data processes codify the past*" and thus configure the future; the past becomes the guarantor of the future (O'Neil, 2016). Thanks to these technological tools, GAFAM manipulate their users by influencing their desires and by pushing them towards consumption. Algorithmic governmentality allows digital companies to exercise a new type of power over individuals that aims to neutralize uncertainty (Rouveroy, 2017) and perpetuate their sales.

This process is a trend observed by other researchers, who see it as the advent of a new economic model characteristic of our century.

2.2.3. *Surveillance capitalism*

Deleuze has already stated in 1990 that the society of control was not only a technological evolution, it was above all a mutation of capitalism. This idea is supported by Shoshana Zuboff (2015, 2019) who introduce the concept of surveillance capitalism, which is "*a new form of information capitalism that aims to predict and modify human behavior as a means to produce revenue and market control*" (2015). It is "*the foundational framework of a surveillance economy*" (2019), as in the present world, nearly every aspect of human life becomes visible, knowable, and shareable. The information gathered by digital companies provide them a deeper level of transparency on their users. GAFAM algorithms monitor, evaluate, rank individuals, and adjust their rating in real time, to resell character traits to advertisers (see Figure 1: GAFAM Business

Model). The privacy of users, the prediction and modification of their behaviors are the driving force behind the growth of surveillance capitalism.

A real-time actual behavior modification

GAFAM's data extraction and aggregation have consequences for individuals, without them being aware of the constant monitoring to which they are exposed. This system is the consequence of what Zuboff calls *Big Other*: "*an ubiquitous networked institutional regime that records, modifies, and commodifies everyday experience from toasters to bodies, communication to thought, all with a view to establishing new pathways to monetization and profit*" (2015). In order to fuel surveillance capitalism, everything around individuals is being rethought to become a source of behavioral surplus, as the overage of data creates value and profit (Haggerty and Ericson, 2000). This overage of data has not only to be abundant but also varied. To achieve it, GAFAM have extended their data extraction operations from the virtual to the real world. Indeed, according to Zuboff, GAFAM are not only influencing and guiding users' choices online, as seen with the algorithmic governmentality (see 2.2.2 An algorithmic biopower for financial purposes), they have found the way to control individual behaviors in the real life. In order to prove it, Zuboff unveils the underside of the Pokemon Go. With the game developed by Niantic, which is a subsidiary of Google, the player believes he or she is hunting Pokemons in the real life, while in fact he or she is oriented towards a chosen destination for a specific reason. Indeed, Niantic's business model is based on sponsored sites. Private companies pay Niantic to be included in the virtual playground, given that the presence encourages attendance and thus increases their sales. Through the game of augmented reality, individuals gather in real-world places, move around in the real world and consume in real-world shops, and all these actions have been orchestrated by behavioral predictions in order to generate even more personal data. Pokemon Go is therefore "*a living laboratory for behavioral change*" (Zuboff, 2019), in the sense that it bypasses the state of consciousness and responsibility of users who submit to the will of the game and thus to the will of the companies, that have paid Niantic to bring the players to their shops. Thanks to surveillance capitalism and massive data accumulation, GAFAM are now able to control and manipulate individuals in the real world.

Towards a new economic model for the 21st century

GAFAM's economic model marks a paradigm shift in capitalist mechanisms: the capital is no longer a good or a stock, but a behavior and the way of informing and understanding it, the information that GAFAM can appropriate. Surveillance capitalism strongly contrast with Fordism, where the worker was both the producer of the value and the buyer of the produced good. In the modern system, individuals are no longer targets of sales but objects from which the material is extracted and then injected into databases that produce the real product sold to the real customers who are the advertisers (see Figure 1: GAFAM Business Model). Moreover, as computer mediation renders economy transparent and knowable, as algorithms can predict the future, the classic neoliberal perception of the market as intrinsically unknowable is no longer valid. Surveillance capitalism operates according to a knowable market where nothing is left to chance, as it is "*a movement that aims to impose a new collective order based on total certainty*" (Zuboff, 2019).

Moreover, this new economic model of surveillance highlights two kinds of asymmetries. First of all, the asymmetry of knowledge. There is a real lack of knowledge for the users. GAFAM know everything about them, "*Google knows far more about its populations than they know about themselves*" (Zuboff, 2015), however, the users know nothing about those opaque and obscure companies that seem to be untouchable. As Zuboff says: "*Surveillance capitalism thrives on the public's ignorance. Big Other is institutionalized in the automatic undetectable functions of a global infrastructure that is also regarded by most people as essential for basic social participation*" (2015). GAFAM take advantage of their privileged place in the lives of individuals and the high rate of use of their services to maintain their control and extend their surveillance. This highlights the second asymmetry, which is a power asymmetry. Indeed, only 5 actors share the new information economy, which presents threats.

Thus, GAFAM have set up a surveillance system for economic purposes that allows them to increase their profits and maximize their gains. The only objective of these companies is the massive accumulation of data, which is the source of their income. Their business model is based on personal data they extract from their users in order to fuel algorithms that make predictions and anticipate individual behaviors. This new economic model, known as surveillance capitalism, characterizes the society of the 21st century.

Nevertheless, by becoming deeply rooted in the contemporary digital landscape, by accumulating unlimited knowledge about their users and by centralizing a constantly growing wealth, GAFAM have increased their power over individuals to the point of competing with sovereign states and escaping control, a situation that comes with many risks.

2.3. GAFAM's monopole and hyperpower

GAFAM took possession of the digital economy in a record time. They form henceforth a global oligopoly and continue to extend their grip on the Internet, in order to maintain their hegemony and generate exceptional and ever-increasing profitability. As they represent the world's largest market capitalizations (NASDAQ Companies, 2019), their financial weight now competes with some States.

According to Jaron Lanier (2018), GAFAM's business model is dangerous for the society in the long term. The Web is becoming increasingly concentrated and privatized, whereas it was imagined as a decentralized space by its creators. The addiction of individuals to GAFAM services and the lack of alternatives reinforce and sustain the power of these five actors.

2.3.1. From attention economy to addiction economy

The attention economy, which is a branch of economics and management science, focuses on the "attention" of digital platform users, that is to say on the time they spend on offered services; and on the value that it represents as attention is considered as a scarce commodity.

It is Herbert Simon in the 1970s, following his work focused on the interference between information and cognitive capacities, who laid the foundations for this new field of research and highlighted the reversal of the economic paradigm engendered. Indeed, when the cost of the access to information becomes marginal and it is easily available, scarcity is no longer the access to information, but the attention needed to process it (Kessous, 2011). "*What information consumes is rather obvious: it consumes the attention of its consumers. Hence a wealth of information creates a poverty of attention and a need to allocate that attention efficiently among the overabundance of information sources that might consume it*" (Simon, 1971 in Festré and Garrouste, 2015). GAFAM's business model is based on the attention economy. Digital players have set up a kind of implicit exchange between a free and personalized service and "attention deposits" from the users. To deepen their knowledge of individuals and collect more and more data, GAFAM are continually improving their techniques for capturing attention, as it is this attention that becomes the tradable and marketable good.

The process of capturing attention is of transactional nature (Kessous, 2011), however, this aspect is not known by everyone: "*most of the people do not realize the transactional dimension of all this. When you use Google to search for something, you don't necessarily realize that you are making some kind of contract with Google. I can use the platform, but in return I give personal data. This transaction is really not explicit*" [free translation] (Aroles, appendix 6). Indeed, according to Cercy (appendix 5), individuals have always been used to valuing a good or service in relation to the price they paid. In the case of GAFAM, the price seems to be zero cost as there is a "*lack of materiality*" (Aroles, appendix 6), whereas in fact, individuals pay with their attention, from which GAFAM extract personal data. Data hunting is therefore the result of this attention economy.

In the GAFAM's ecosystem, the struggle for attention becomes an object of competition. A rivalry is developing between the five actors in order to capture users' interest, as it reveals their intentions, tastes and preferences. Yet, as seen above, it is this information that is sold to advertisers. The financial stakes are therefore high.

Towards an addiction economy

Nevertheless, the attention dedicated to digital platforms is gradually turning into an addiction. GAFAM have succeeded in becoming obligatory crossing points, reflexes for individuals. They are omnipresent: in the public, professional and especially private sphere. "*We cling to our [electronic] collars. There is an invasive structuring of new technologies. […] The time spent on social networks is far too long*" [free translation] (Nitot, appendix 7). Platforms have become standards, habits, automatisms: "*it seems so obvious. We no longer even ask ourselves the question of doing otherwise. […] We are so embedded in this system that it is difficult to change*" [free translation] (Leclercq-Vandelannoitte, appendix 3). Individuals are in a situation of dependence upon five actors who concentrate the majority of digital services. They impose their conditions and especially the type of relationship they wish to maintain with their users (Cercy, Appendix 5). They are the ones who "lead the way" taking advantage of the carelessness of their audience. It is in this context that Tristan Nitot introduces the concept of "Big Mother". According to him, the GAFAM are not Orwelian Big Brothers, but a Big Mother, who through profiling and behavioral predictions, provides individuals with what they need, when they need. Big Mother is

"*surveillance with an aspect of addiction […] we are freely trapped in something we consider to be irreplaceable in our daily lives. One believes that it is impossible to get rid of it*" [free translation] (Nitot, appendix 7). Individuals therefore voluntarily but unconsciously confine themselves into a kind of "golden cage" where all their desires and needs are satisfied before they even have had time to express or formulate a single wish. The speed, efficiency and utility of GAFAM's digital services provide unprecedented daily comfort to individuals, who, thanks to the illusion of free access, enhance their use. This state of dependence reinforces GAFAM's power, who can thus maintain control and surveillance over individuals without raising any objections.

Constantly capturing the attention of individuals and offering ever more personalized and tailor-made services, GAFAM are becoming essential and irreplaceable in the contemporary digital landscape. They implement various strategies to keep their audience and not allow individuals to go elsewhere. Thanks to their notoriety and financial domination, GAFAM systematically eliminate competition and players who could overshadow them.

2.3.2. Concentration of power and the lack of alternatives

As Zuboff (2015, 2019) points out, by accumulating infinitely large quantities of personal data, GAFAM concentrate a very extensive knowledge on their users. At the same time, it gives them power, since they can influence individual behaviors. This relationship between knowledge and power is theorized by Michel Foucault in *Discipline and Punish* (1975). According to the philosopher: "*power and knowledge are directly involved in each other; there is no power relation without the correlative constitution of a field of knowledge, nor any knowledge that does not presuppose and constitute at the same time, power relations*". The centralization of personal data, and therefore of knowledge, increases GAFAM's power, which thus become hyper-powerful (Rouveroy, 2018). According to Rouveroy, digital companies acquire more power than any state as they control what wealth is today, namely data and predictive algorithms; and "*who masters the space of potentiality masters the world*" in her opinion. GAFAM would thus be the new masters of the digital world but also of the real world. By monitoring and controlling individuals in the present, they anticipate the potentialities of the future and prevent anyone who wishes to do so from overthrowing their power.

The lack of counter-power

As Cercy points out (appendix 5), the centralization of knowledge and therefore power by the GAFAM creates a huge entrance barrier for new actors. Due to their size and technological advance, it is very difficult to compete with them. Small emerging structures "*will not be able to capture as much data as Google, which has been living at a loss for years before finding a viable economic model*" [free translation] (Cercy, appendix 5). Facing these giants while generating profits is therefore very complicated.

In addition, GAFAM systematically neutralize competition and any actor that may threaten their dominant position. The strategy adopted is redemption: digital platforms integrate successful companies and new growth businesses. This is the case, for example, of Instagram and WhatsApp, which were acquired by Facebook, or of YouTube and Waze, which were repurchased by Google. As Cercy states: "*once GAFAM own almost all the companies that are successful, they are thus able to impose their model and buy back an innovation that may have chosen another model*" [free translation] (Cercy, appendix 5), and thus destroy it. GAFAM's hyper-power allows them to stop any counter-power that could challenge them. The concentration of power, knowledge and wealth between only five actors creates a strong monopolistic situation that cancels out any possibility of an alternative. However, as Aroles (appendix 6) points out: "*for Deleuze, if we want to progress in the world, we need a window of possibilities; from the moment you lose it, you switch to totalitarianism*" [free translation]. It is in this sense that Zuboff (2019) affirms that GAFAM are antithetical to democracy and denounces generated inequalities and asymmetries. Like absolute monarchs, digital companies free themselves from counterweights by preserving all powers in their hands.

Given the lack of alternatives, individuals therefore resolve themselves to the "non-choice" (Charmet, in Nitot, 2015) of GAFAM, since the power of these omnipresent companies creates in them the feeling that it is useless to rebel. According to Aroles (Appendix 6), there is indeed a feeling of helplessness among individuals. This lack of collective action and willingness to overthrow the established digital order favors the dominant position of digital companies, which perpetuate their surveillance and control.

Thus, GAFAM have established themselves as uncontrolled technological superpowers. They operate as an alliance of monopolies which, by their size and technological advance, concentrate a set of powers and impose their model. They dominate the digital economy and inhibit the competition.

The central position enjoyed by GAFAM is indeed a consequence of their hyperpower, but it also results from the willingness of individuals to submit to these actors.

2.3.3. GAFAM dictatorship: a regime allowed by people's consent

A dictatorship is a "*political regime in which an entity exercises all powers in an absolute way, without any law or institution limiting it*"[6]. Power is not shared or controlled, and individual freedoms are not guaranteed. GAFAM's power can be likened to a dictatorial power, as the extensive knowledge of individuals the companies hold, infringes on their privacy and contravenes Human Rights principles, as well as there is no control to limit those actions.

Breach of privacy

According to Solove (2007), privacy is not only associated to intimacy, as not all information are intimate. It is a plurality of different things related to a person and his or her life and actions. "*The right to privacy recognizes the sovereignty of the individual*" (Solove, 2007). Being the only one responsible for his actions, the sovereign individual has the right to decide what can be seen and known by others and what must remain in the strictly private domain. The massive accumulation of personal data and behavioral manipulation implemented by GAFAM prevents individuals from being sovereign subjects. The constant tracking of Internet activities is done in

[6] Dictatorship, the Larousse Dictionary, [Online] Retrieved from: https://www.larousse.fr/dictionnaires/francais/dictature/25352

disregard of privacy, since algorithms are fueled with the most personal things individuals have. Each action undertaken in this increasingly complex and even confusing digital world, generates a transversal sharing of data that is invisible and unstoppable. The individual "exposes" himself (Harcourt, 2015) as nothing can be hidden from GAFAM's eye. According to Charmet (in Nitot, 2015), constant surveillance does not only jeopardize the right to privacy and intimacy, but also threatens freedoms of opinion, belief and information, whose respect largely determines the belonging to a Democracy. With GAFAM, the most fundamental rights are violated and used for commercial purposes, while individuals should be able "*to set their own guidelines*" for the use of their data (Nitot and Cercy, 2016).

The concentration of knowledge creates the submission of users to digital dictators, which is constantly increasing, leading to a deepening of their dependence. Deprived of their digital sovereignty, users are equally deprived of their autonomy, since uncertainty and coicidence are banished in this new regime and each future event is scheduled. Users voluntarily enslave themselves (La Boétie, 1546) to GAFAM, "*while [they] should escape from the predetermined future in which one seeks to imprison [them]*" (Damasio, in Nitot and Cercy, 2016).

GAFAM's surveillance and control society is therefore a form of invisible or unconscious conditioning (Aroles, appendix 6). According to Nitot (2015), "*GAFAM are unknowingly taking the place of the State, of the States, in the daily management of our rights and freedoms. This almost invisible evolution has been achieved with the tacit consent (because the issue is misunderstood) of citizens-internet users-customers, and with the blind complicity of governments which, for the lack of political vision, have given up more and more ground each day believing that it is in their interest*". Privacy thus becomes the field of an information war (Nitot and Cercy, 2016) where individuals are not armed to protect themselves. This situation highlights a breach in the Social Contract where the State fails to protect its citizens. In Rousseau's conception, individuals accept to get out of the state of nature and to abandon certain freedoms in favor of the general interest and in exchange for their security provided by the State. According to Aroles (appendix 6), "*it worked very well in the context of the 18th century, but I think that here we have a breach of this Social Contract. We give access to all this data, all this information but precisely without being aware of it and without gaining anything in return"* [free translation].

However, the modern panoptic control society is only partially imposed. Indeed, it is increasingly difficult for individuals to maintain their anonymity and escape GAFAM monitoring, but electronic collars – the modern means of surveillance - are acquired voluntarily and the use of digital services requires explicit consent. This raises the question of personal responsibility.

The question of personal responsibility

The lack of materiality and the invisibility of surveillance, control and collection of personal data make it difficult to assign a responsibility (Aroles, appendix 6). It has become increasingly difficult to separate collective activity from technologies and digital resources, as nearly all actions require digital tools and services nowadays. This phenomenon raises questions about personal and collective responsibility, as new technologies "*deeply transform the nature of involved responsibilities, as well as the time and space of the experience of responsibility*" (De Vaujany *et al.*, 2019).

In 1994, Paul Ricœur has already pointed out the vagueness surrounding the concept of responsibility. In *Le concept de responsabilité. Essai d'analyse sémantique*, the philosopher shows the "semantic filiation" between responsibility and accountability: responsibility involves the ability to allocate, impute an action to a person, to attribute it as the person is its "true author". Individuals are the true users of digital platforms. This action is attributed to them. However, Ricœur goes on, stating that responsibility is only possible if one assumes "the freedom of the moral agent". Responsibility is attributed only to autonomous individuals, who make decisions in a free way without outside interference. By manipulating behaviors and profiling individuals, GAFAM do not allow their users to make decisions and act freely, their choices are oriented without them noticing it.

However, personal responsibility is in fact upstream of the use of digital services. According to Singh and Lyon (2013), "*a little attention is paid by consumers to the design of consumer surveillance; typically, consumers 'agree' to "privacy policies" without pausing to read them"*. While GAFAM explicitly present their operating mode through terms and conditions of use, individuals do not care and accept without understanding, eager to access the desired services. "*Individuals do not question themselves enough, act without thinking beyond, without thinking about the consequences of their actions*" [free translation] (Leclercq-Vandelannoitte, appendix 3).

They are unaware of the fact that by accepting all GAFAM clauses, they open up an access to their deepest privacy and automatically submit to the power and control of these five actors.

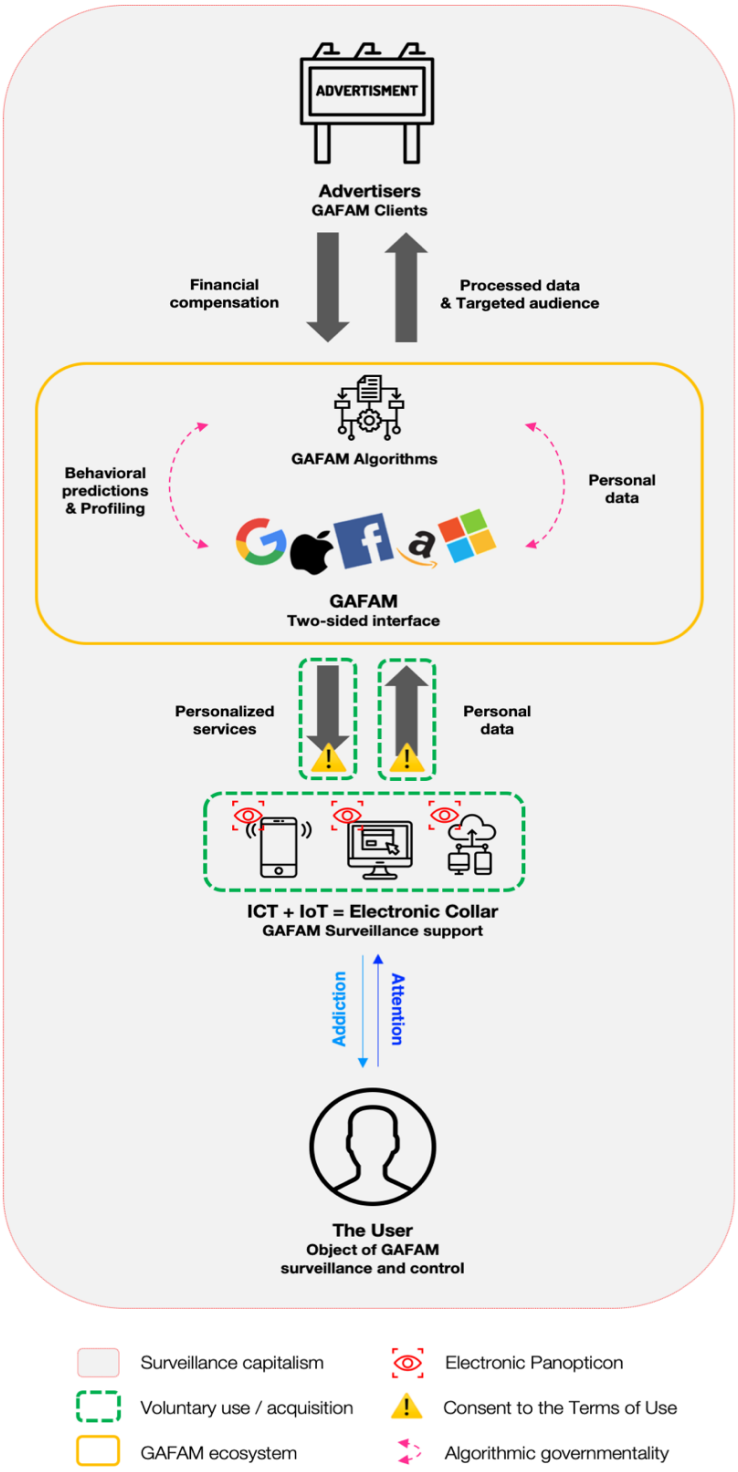
Ricœur's (1994) definition of responsibility highlights a third aspect: the link with the assessment, the evaluation of merits and failures (Jaeger, 2009). The link between responsibility and evaluation leads to control. The subject responsible for an action may eventually suffer a sanction or obligation to make reparation for his or her actions if it caused harm to others. In the context of GAFAM surveillance and control, the responsibility seems to be shared between the two parties: individuals, by their consent to the general terms and conditions of use, are co-responsible for their condition as objects of monitoring and control; and GAFAM are co-responsible for the looting of privacy of their users and the manipulation of their conduct. However, this co-responsibility does not result in any sanctions for the moment.

According to Cercy (appendix 5), however, Internet users should not be blamed, because the digital space is still an unregulated universe. By using GAFAM services, users respond to their "impulses" and their "comfort". This is why, it is not a question of individual irresponsibility, as "*it does not seem appropriate to place the burden of using companies that may or may not have good data governance on them*" [free translation]. On the contrary, she underlines the need for a more detailed legal framework for digital practices made by a legitimate entity able to set an appropriate sanction.

This is finally in line with the perception of De Vaujany *et al.* (2019), who state that: "*the complexity as well as the spatial and temporal extension of responsibility in modern, digital era should be a key issue for managers, politicians and activists and researchers in organization theory alike*", in order to better understand and identify the share of responsibility of each actor and achieve sustainable solutions for the years to come.

2.4. Research modeling

The various scientific theories raised above can be summarized in the following research modeling in order to help the understanding of all the interactions:



2.6. Resulting assumptions

Following the various scientific points of view and the research modeling, which help to clarify the vision of the research field for control and surveillance practices related to GAFAM and technological devices, it is possible to formulate assumptions that will be tested during the conducted research in order to confirm or disprove them.

Since all the people nowadays have ICTs and/or IoT, and use GAFAM services massively, it is easy for digital companies to track them and extract needed information. It can be assumed that:

H1: Individuals transmit their personal data to GAFAM through modern 'electronic collars', which follow them everywhere.

As Nitot and Zuboff state, the transaction between users and digital platforms is unequal since they do not realize the extent of the information that is captured by GAFAM. It can be assumed that:

H2: Individuals are unaware of the value of their data.

Given the omnipresence of GAFAM in the daily lives of individuals, in the public, professional and private spheres; given the unconscious shift (from the users' point of view) from an economy of attention to an economy of addiction, it can be assumed that:

H3: Individuals are dependent and addicted to GAFAM.

The lack of alternatives, which could offer superseded services to GAFAM, confines individuals in their current uses, by closing the Deleuzian 'window of possibilities' and accentuating the dominant but illegitimate power of GAFAM, which carry on their surveillance and control activities. Thus, it can be assumed that:

H4: The lack of alternatives reinforces GAFAM's power.

Although surveillance and control are not explicit, the terms and conditions of use are. By neglecting them, individuals agree to submit to GAFAM and their practices. It can be assumed that:

H5: Individuals unknowingly consent to GAFAM surveillance and control.

3. RESEARCH METHODOLOGY

3.1. Research objectives

The literature review enabled the mapping of the research subject, by highlighting different points of view, strong ideas and existing theories on surveillance and control related to GAFAM. However, during the pre-investigation period on the research subject, a lack of quantitative data related to the topic has been noticed. The formulated theoretical concepts do not provide quantifiable evidences. It is therefore difficult to demonstrate the extent of the phenomenon and the personal feelings and habits of digital platforms' users.

This research attempts to address it by providing quantitative insights about the digital practices of GAFAM users. The objective is to understand the functioning of GAFAM's surveillance and control system in France and to explain how it is implemented through the behaviors and perceptions of platform's users, who are the objects of the constant monitoring. This work tries to bring new elements to the research field.

3.2. Research design: the survey methodology

Research design is the architecture of the research, the framework that articulates all the elements that structure the research, namely research question, literature review, data, data analysis and the results. It is a crucial element for any empirical research project, regardless of the chosen subject and methodological point of view (Royer and Zarlowski in Thiétart, 2008). The research design selected for the present work is the survey methodology.

3.2.1. Presentation of the survey methodology

The survey methodology is an interrogative method in the sense that "*it interviews a certain number of individuals for the purpose of generalization*" (Ghiglione and Matalon, 1998 in Lugen, 2017). It enables the measurement of individuals' perception of social objects (Salès-Wuillemin, 2006). The researcher conducts surveys in order to test general theories against the empirical reality he observes and interprets (Paugam, 2012). The survey methodology is suitable for research that seeks to investigate opinions, attitudes, beliefs, perceptions, experiences or behaviors (Lugen, 2017). In general, it is a hypothetical-deductive method.

The survey methodology combines both quantitative and qualitative methods. To carry out this research, the online questionnaire method was used to collect and analyze empirical results, as well as qualitative exploratory interviews were conducted in order to better frame the research subject.

The exploratory interview

The exploratory interview allows the researcher to familiarize himself with the subject and to understand its issues in their entirety. The exploratory interview can reveal the image that targeted population has of the subject, help to make specific hypotheses or highlight individuals' reactions to the studied subject (Salès-Wuillemin, 2006). The researcher can then use the results of this pre-investigation for the conception of the questionnaire. The exploratory interview provides an initial approach and possible trends that have to be taken into account for further research.

The exploratory interview can also be an expert interview. The purpose is to collect information from recognized experts. It helps the researcher to better understand the issues, extend his knowledge on the treated subject and thus better orient the research. Experts can also give some advices on theoretical concepts and recommend essential authors. The author of this research has conducted exploratory interviews with experts. Indeed, five experts (both academics and private sector professionals) agreed to answer author's questions in order to guide her in the delimitation of the subject.

Exploratory interviews can be structured, semi-structured or unstructured. In this research, the semi-structured interview was chosen. The semi-structured interview is organized in a strict framework (the interviewer knows the specific points he wishes to address) that maintains a freedom of speech and flexibility (Lugen, 2017). The questions are formulated in advance and included in an interview guide that constitutes a standardized master plan limiting the risk of dispersion (Salès-Wuillemin, 2006). The interview guide is not rigid, the order of the topics does not matter as long as all the topics are covered.

The online questionnaire

The main interest of the questionnaire method is to gather a large amount of information, both factual and subjective, from a large number of individuals (Paugam, 2012). The questionnaire aims to verify formulated assumptions by analyzing collected responses and data crossing. The interviewer has to target the appropriate population, create the questionnaire by formulating clear questions divided into several sections, and then administer it. The method of diffusion chosen for this research was the Internet.

3.2.2. The added value of the method

The added value of the survey methodology lies in the fact that it is a mixed method that links qualitative and quantitative approaches within the same research. An exploratory study, conducted through a qualitative approach, is often an essential prerequisite for any quantitative study in order to define the research question, clarify theoretical concepts or research hypotheses (Baumard and Ibert, in Thiétart, 2008). The exploration part can be linked to a qualitative approach and the verification part to a quantitative approach (Brabet, 1988, in Thiétart, 2008).

The qualitative approach provides precise information and knowledge about a phenomenon thanks to the expert interviews. This step enables the forecasting of the questionnaire preparation, and thus to better orient and formulate the questions.

The quantitative approach identifies trends and provide indicators. "*Numbers have become an argument, so their production and meaning have become an important issue*" (Paugam, 2012). The statistical results provide quantified data, which helps the researcher to measure the extent of the studied phenomenon and to formulate well-founded answers to the initial research question.

3.3. Data collection

As explain above, this thesis uses quantitative data obtained thanks to the online questionnaire to address the research question. However, as exploratory expert interviews were conducted, qualitative data were also collected and analyzed in accordance with the survey methodology principles.

Data collection is an essential part of any research work. The subsequent processing of the collected data through methodical instrumentation will produce results and improve, or renew, existing theories (Baumard and Ibert, in Thiétart, 2008).

The collection of primary data offers the researcher the opportunity to confront directly the "reality" he has chosen to study. This requires the control of a complex system of interactions with the research field (*Ibid.*, 2008). Secondary data collection involves access to existing databases. Primary and secondary data are complementary throughout the research process. The incompleteness of primary data can be corrected by secondary data to better understand the background or to compare the research field with external information (*Ibid.*, 2008). Primary data helps the researcher to attribute internal validity to his or her research, while secondary data attributes external validity to the accomplished work (Lugen, 2017).

This thesis is based on both primary and secondary data collection.

3.3.1. The exploratory interviews

Primary data

According to Evrard et al (2000, in Thiétard, 2008), qualitative data are variables measured on non-metric nominal and ordinal scales. This thesis uses exploratory expert interviews and their transcripts as part of primary data used to form the subsequent quantitative study. The exploratory interviews are semi-structured and were all conducted in French as both interviewees and the author are French-speaking natives. The author used the transcripts from 5 interviews, which are available in appendices 3 to 7. The transcriptions were made in French, however, as the thesis is in English, translation had been made if needed in the main body of text. Interviews lasted between 35 minutes and 1:15 hour. All interviewees agreed to be quoted on the basis of these interviews.

At the beginning of each interview, the author explained the topic of the thesis and the general structure of the interview. The questions asked were formulated in advance and included in an interview guide (available in appendix 1) that constitutes the master plan for the dialogues. The interview process was the following: during the first part, the author asked personal questions to the interviewee in order to better know his or her educational and professional background, then the interview concentrated on theoretical concepts and more specifically on Foucault, Deleuze and Zuboff theories, on surveillance and control systems nowadays, on links that can be observed between GAFAM and monitoring practices, on interviewee's point of view related to the reasons why individuals are not aware of GAFAM surveillance and control, and their neglect of the consequences of ICT's and digital services' use. The last part of the interview dealt with potential solution and further evolutions of the situation.

The tools used to conduct the exploratory interviews were mobile phone for teleconferences, Skype for videoconferences and Apple MacBook recorder.

The primary data collected thanks to the exploratory interviews were used to better frame the research topic and to organize the literature review in a relevant manner. This exploratory study was conducted to clarify theoretical concepts and formulate assumptions in order to anticipate the quantitative study on which this research is based, and on which the initial assumptions will be

confirmed or disproved. Primary data collected through exploratory interviews are therefore not included in the results section (4. Results), but rather enrich and guide the literature review (2. Literature review).

Sampling

To conduct the exploratory interviews, the author selected five experts, i.e. five personalities known for their knowledge of the studied subject. The five experts were both academics and private sector professionals.

The experts in the “Academics” group are people who have dealt with surveillance and/or control issues in their previous research work, and who have in-depth knowledge of the theories and concepts of Michel Foucault, Gilles Deleuze and Shoshana Zuboff.

The experts in the "Knowledgeable" group are people from the private sector who, in their daily work, face challenges related to personal data for different reasons (GDPR issues, cyber security, advocacy); some of whom have written books to raise public awareness on the dangers related to personal data; are promoters of the free web and alternative solutions to GAFAM.

The following tables exhibit the two groups of interviewed experts in alphabetical order (transcribed interviews are available in appendices 3 to 7).

Table 1: Interviewees – Academics

Identity	Occupation	Date of issue	Place of issue	Duration	Number in the thesis appendix
Aurélie LECLERCQ-VANDELANNOITTE	Researcher in Management Sciences and Professor at IESEG Business School	23/05/2019 at 10:00 am	Teleconference call	35 min	1

Jérémy AROLES	Assistant Professor in Organization Studies in the Business School of Durham University	12/06/2019 at 11:00 am	Skype	1.00 hour	4

Table 2: Interviewees – Knowledgeable

Identity	Occupation	Date of issue	Place of issue	Duration	Number in the thesis appendix
Marc TAKABACHET	Sales Executive Finance & Risk, SAP France	24/05/2019 at 3:00 pm	Teleconference call	1 hour	2
Nina CERCY	Cybersecurity Consultant, EY Author of *Numérique : Reprendre le contrôle*	N°1: 04/06/2019 at 12:15 pm	Teleconference call	N°1: 1.10 hour	3
		N°2: 06/06/2019 at 9:30 pm		N°2: 45 min	
Tristan NITOT	VP Advocacy, Qwant	21/06/2019 at 2:00 pm	Skype	1.15 hour	5

Secondary data

Secondary data collection involves access to existing databases. The author collected secondary data concerning surveillance and control methods in academic journal articles (online or provided by their authors), books, reports, official websites of some researchers or organizations (Quadrature du Net, Legal Place, GDPR-info), radio broadcasts and newspaper articles.

Secondary data were collected at different moments of the research process: firstly, before the exploratory interviews in order to gather knowledge and identify the major issues of the subject, which helped the construction of the interview guide (appendix 1); secondly, during the interview process, as all interviews were not conducted at the same time, the author could supplement her bibliographical knowledge by following experts' recommendations; thirdly, during the construction of the online questionnaire; and finally, during the data analysis process in order to contrast the results with theoretical concepts and highlight the limitations of the research.

3.3.2. The online questionnaire

Primary data

According to Evrard *et al*. (2000, in Thiétart, 2008), quantitative data are collected with interval and proportion scales. In order to collect quantitative data which are the 'official' primary data of this thesis, the author created an online questionnaire. The objective of the questionnaire is to verify formulated assumptions (see 2.4 Resulting assumptions) and to provide quantitative conclusions about the digital practices and habits of GAFAM users.

For this purpose, an online questionnaire was constructed using the Google Forms tool. The content of the questionnaire (available in appendix 8) is divided into 8 parts, each of which deals with a distinct topic and contains blocks of several questions (from 5 to 12 questions). The type of question chosen are closed-ended, with the exception of one open-ended question introduced in

part 5, which is used to collect specific evidence about the respondent's personal experience. Closed-ended questions include behavior, knowledge, intent and opinion questions, as well as an identification part that includes the respondent's descriptive characteristics. The questionnaire offers a variety of response options ranging from simple answers (yes / no; agree / disagree) to a larger sample of answers (for example: several times a day / several times a week / several times a month / rarely / never). In the context of opinion questions, the option “I don't know” is also possible.

The online questionnaire is anonymous and self-administered. The chosen method of distribution is the Internet as the tool used to support the questionnaire is a digital tool (Google Forms).

Before distributing the questionnaire to the targeted population, a pre-test was conducted by administering the questionnaire to 5 people in order to gather their opinions about the clarity, coherence and neutrality of the questionnaire.

Following the pre-test, the questionnaire was distributed from the 15th till the 28th of July 2019 on Facebook and LinkedIn social networks and was sent by email to a group of author’s relatives and colleagues.

The online questionnaire collected 250 responses.

Sampling

As GAFAM services and devices are widespread and used by the entire population, regardless of age, level of education or socio-professional category, the author wanted to carry out a representative sample of the entire French population, without focusing on a specific age group. The survey is therefore aimed at a sample comprising a wide range of individuals aged 18 to 65 years and over, all socio-professional categories combined.

However, for time and resource reasons, it was impossible for the author to construct a truly representative sample based on probability or quota sampling techniques. Since the questionnaire was published on social networks, it was difficult to control the age groups of the respondents. (Limitations of the targeted population are outlined in Section 5.5 Limitations).

Given the available tools and limited time, the author therefore chose a convenience sampling, which is a sample taken from a group of people easy to contact and reach. The sample of this thesis is composed of individuals who were available and wished to respond to the questionnaire following its publication on social networks or after receiving it by e-mail.

Secondary data

Secondary data used for the online questionnaire are the same as the ones used for the exploratory interviews, specified in section 3.3.1. The exploratory interviews – Secondary Data.

All the secondary data collected in order to prepare and conduct the interviews and organize the literature review were useful to create the online questionnaire and to improve it.

3.4. Data treatment and analysis

3.4.1. The exploratory interviews

Thanks to the recordings, the author was able to write down the transcript of each interview. Transcripts were read few times in order to identify keywords and relevant points of view for the thesis. The analysis of these exploratory interviews enabled the author to better organize all sections of the literature review and to better steer the research. However, data collected and treated thanks to the exploratory interviews were not used for the results section of this thesis (4. Results).

3.4.2. The online questionnaire

Thanks to Google Forms tool, the 250 responses collected were recorded and listed in an Excel file. Thus, the chosen analyzing tool for this research was Microsoft Excel.

The analysis of the results initially consisted of a simple reading of the answers to each question in order to analyze the type of respondents (sex, age, socio-professional category, level of education) and to learn about the major habits and trends highlighted thanks to the quantitative results.

Then, the author linked different responses in order to find correlations between the observed phenomena, by varying certain variables such as age or level of education. To do so, the author used cross tabulations (i.e. linking of two variables) and multivariate analysis, (i.e. the linking of several variables simultaneously) by using Excel's pivot tables.

Finally, the author compared the results obtained with those expected by formulating the five assumptions in order to confirm or disprove them.

4. RESULTS

The results presented in this section are the data collected through the online questionnaire thanks to Google Forms tool. 250 responses were collected. Microsoft Excel was used in order to analyze them and establish correlations. Detailed results of the questionnaire are available in appendix (see appendix 9: Results of the online questionnaire).

4.1. Assumptions to be tested

Following the literature review and presented scientific points of view, five assumptions were formulated in section 2.4 Resulting assumptions and need now to be tested in order to confirm or disprove them. The formulated assumptions are the following:

- **H1**: Individuals transmit their personal data to GAFAM through modern 'electronic collars', which follow them everywhere.
- **H2**: Individuals are unaware of the value of their data.
- **H3**: Individuals are dependent and addicted to GAFAM.
- **H4**: The lack of alternatives reinforces GAFAM's power.
- **H5**: Individuals unknowingly consent to GAFAM surveillance and control.

4.2. Modern electronic collars ownership

The most representative incarnation of the modern electronic collar is the smartphone, which concentrates a lot of personal data and can be carried everywhere.

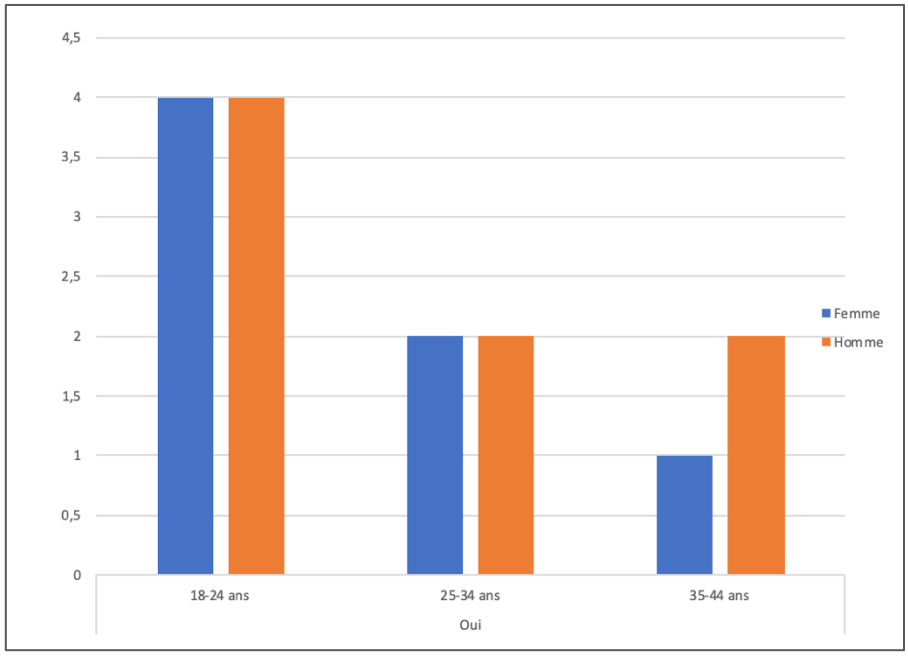
99.2% of respondents own a smartphone, i.e. 249 people out of 250. In addition, 91.2% of respondents said they always keep their smartphone close to them, 64.8% said they use it several

times an hour and 34.4% several times a day, which allows GAFAMs to constantly track them and collect the generated data.

99.6% of respondents use their smartphone to make calls or send SMS messages; 95.2% to listen to music, watch videos or take pictures; 95.6% to check their emails; 93.6% to do Internet searches; 92% to go on social networks, 88.8% to use GPS and 78.4% to use mobile applications. About 40% also use their smartphone to make purchases and to pay with mobile payment apps. All these uses leave many digital traces that are collected and processed by GAFAM.

Another object that can be perceived as a modern electronic collar is the connected watch. However, only 15 out of 250 respondents have one. They are mainly young people aged 18-24 (8 respondents) or individuals between 25 and 44 years old (7 respondents), both man and woman. 55.6% of them use the connected watch only occasionally. Regarding the uses, 80% of respondents use their connected watch for sports activities and 60% to have continuous access to their health data. All this information is automatically transmitted to GAFAM, which have thus access to people's health check-up and physical conditions, which are very personal or even confidential information.

Figure 2: Holders of connected watch by sex and age



Although few respondents have a connected watch (which makes it impossible to interpret this unrepresentative result), all the participants have a smartphone that they constantly use (which generate data) and always carry with them. This makes possible the confirmation of the first

assumption which is: “Individuals transmit their personal data to GAFAM through modern "electronic collars", which follow them everywhere”.

4.3. Personal data value

One can notice that individuals seem unaware of the value of their data and of the implicit contract they sign with digital companies when they use their services, since 48.2% of respondents say they never read the general conditions of use, 33.5% only rarely read them and 12% from time to time. As Nitot argues, individuals therefore consent to an unequal exchange with GAFAM without realizing that they provide data for free, in exchange of an unexpansive service, since they accept without reading the signed contract.

In addition, 53% of respondents accept that websites record their personal data to pre-fill online documents: this is therefore a conscious and voluntary action. Individuals give their data voluntarily for greater comfort and speed during their browsing. 39% of respondents never check the status of cookies, 23.5% only rarely do so and 18.7% from time to time, while cookies track and extract personal data when browsing online.

However, there is a paradox: while most respondents say they never read the general conditions of use or very rarely, 74.5% of respondents say they are not in favor of GAFAM using their personal data to offer personalized services, 72.5% do not support GAFAM using their personal data to offer discounts and 72.9% do not support the donation of their personal data to digital companies to benefit from free services. Even though they accept the sharing of personal data through the terms of use, individuals are not at the same time in favor of processing and analysis of their data by digital companies.

Figure 3: Proportion of users who do not accept the use of data for personalized services among those who accept the general conditions of use

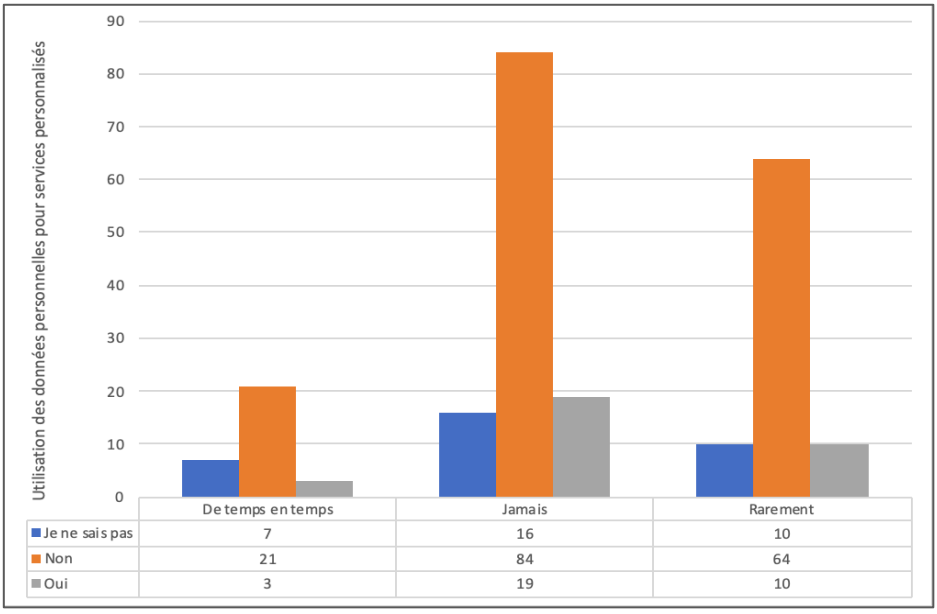


Figure 3 shows that of the 121 respondents who never read the terms of use, 84 do not support the use of personal data by GAFAM to provide them with personalized services and of the 84 respondents who rarely read the terms of use, 64 do not support the use of personal data by GAFAM to provide them with personalized services.

Figure 4: Proportion of users who are against giving data to receive free services among those who accept the general conditions of use

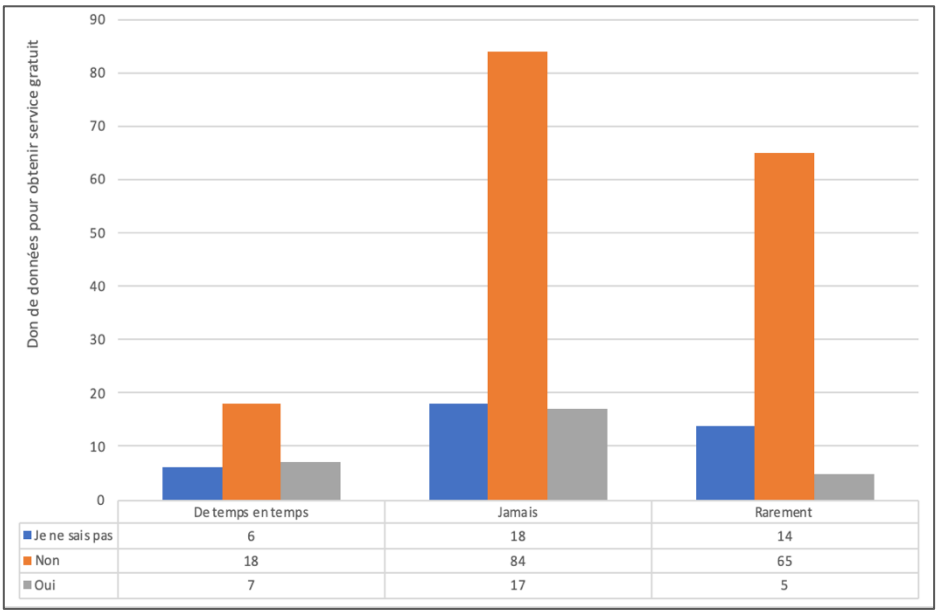


Figure 4 shows that of the 121 respondents who never read the terms of use, 84 are not in favor of giving their personal data to digital companies in order to benefit from free services and of the 84 respondents who rarely read the terms of use, 65 are not in favor of giving their personal data to digital companies in order to benefit from free services.

These two cases are paradoxical, since individuals contradict themselves: they accept the conditions of use that explain that their data will be collected in exchange of a free service, but when questions are formulated in another way, they no longer agree with what they gave their consent before. It can therefore be said that individuals are unaware that they voluntarily offer their data to GAFAM and are not aware of the real value of their data as well.

Nevertheless, 71.3% of respondents believe that personal data have a monetary value, but only 30.3% believe that it is a market good. According to respondents, data would therefore have a monetary value but are not objects that can be monetized.

Figure 5: Monetary value of personal data depending on the perception of data as a market good

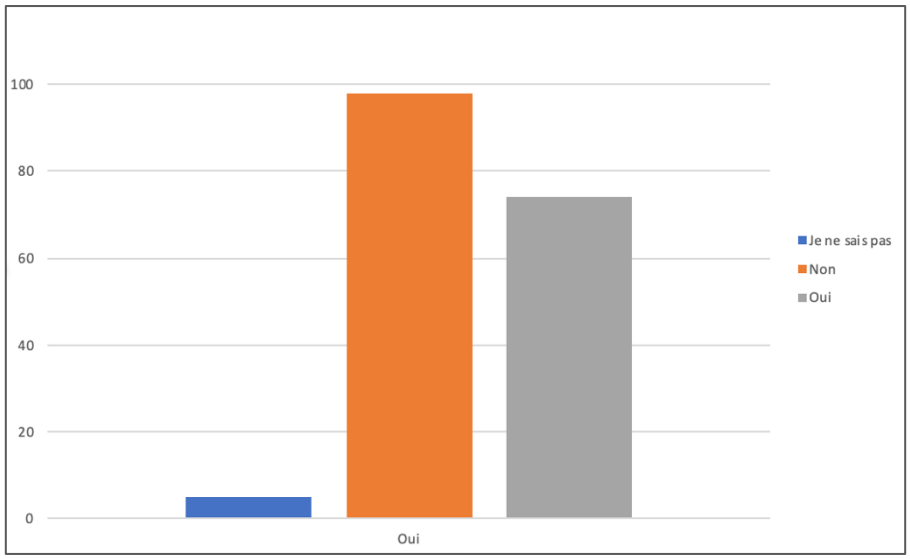


Figure 5 shows that among the 177 respondents who believe that personal data have a monetary value, 74 believe that it is a market good like any other, while 98 believe that data is not a marketable good. This shows that individuals have an idea of the value of their data.

In addition, respondents are concerned about the protection of their data. Indeed, 67.3% of respondents believe that they do not sufficiently protect their data online and 63.3% hide their identity from time to time in order not to disclose their personal information.

Thus, the attitude of individuals towards their data is paradoxical: they are both aware that data has a financial value and may be exchanged for a sum of money, they are concerned about the protection of their data online and try to hide their identity, but at the same time they accept the terms of use without ever reading them and do not control their browsing settings. In view of the divergent arguments, it is impossible to confirm or disprove the second assumption which is: "Individuals are unaware of the value of their data".

4.4. GAFAM addiction

GAFAM business model is based on the attention economy, which is gradually being transformed into the addiction economy. Indeed, 64.8% of respondents say they use their smartphone several times per hour and 34.4% several times a day.

Regarding the use of digital services and more specifically Google services: the majority of respondents use Google Search (217 people) and Gmail (143 people) several times a day, while Google Maps is used mainly several times a week (118 people) and Google Drive several times a month (74 people). The number of people who do not use Google Search and Google Maps is residual, only 18 respondents never use Gmail and 34 never use Google Drive. The majority of respondents therefore use Google's services very frequently.

Concerning Facebook services, the uses are daily: the ¾ of respondents use Facebook and Messenger several times per day, and half of the respondents use Instagram and WhatsApp several times a day. Only 17 people never use Facebook and 19 never use Messenger, while ¼ of respondents never use Instagram. Overall, Facebook services are also used very frequently.

The majority of users rarely uses Amazone's services, only ¼ of respondents uses the company's services several times a month, nearly ¼ never uses them and only 2 people out of 250 use these services every day which is residual.

There are many disparities for Apple's services: 1/3 of respondents never use the brand's services, only 42 people use it every day and 52 people several times a month.

Finally, regarding Microsoft, 70 people use these services every day, ¼ of respondents do it rarely and 38 people never.

Thus, the most commonly used services are therefore those of Facebook and Google, whose business model is entirely based on capturing attention.

In addition, 72.5% of respondents believe that GAFAM services are essential to their daily lives, but only 26.7% believe they are irreplaceable. This implies that GAFAMs would be substitutable by other actors or that respondents do not consider themselves dependent on these services and could do without them. In addition, if GAFAM services were to be charged for, only 39.4% people would be willing to pay to use them.

Figure 6: Proportion of users who would be willing to pay for using GAFAM services among those who consider these services as irreplaceable

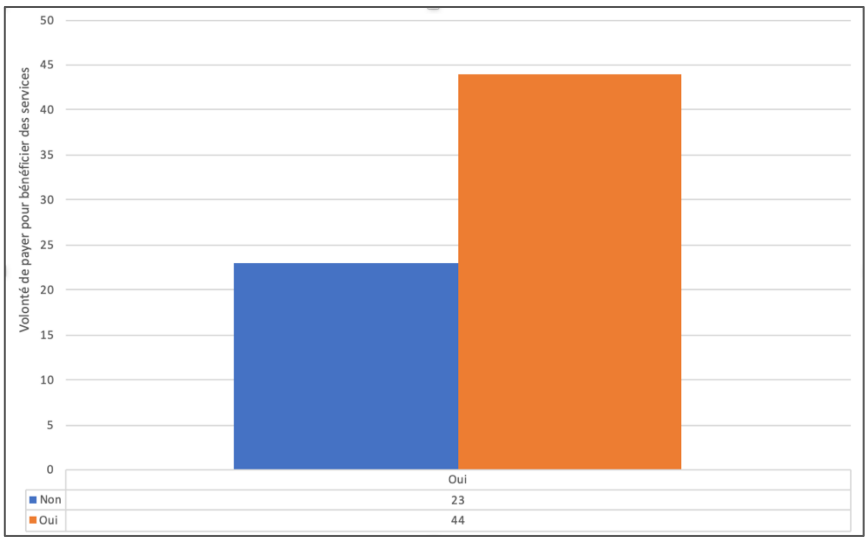


Figure 6 shows that among the 26.7% of respondents who think that GAFAM services are irreplaceable, 44 would be willing to pay for these services if they were no longer free, which means only 17.6%. Users therefore do not seem to be addicted to digital services from this point of view.

Nevertheless, 85.7% of respondents think that smartphones can cause harmful effects, and 50.8% think the same about connected watches. It can be assumed that addiction is one of these

harmful effects. Respondents would therefore recognize the addictive nature of digital services. On the contrary, 47.8% of respondents believe that GAFAM have a positive impact on their lives and 44,2% think that new technologies' impact on their lives is very beneficial, so they do not seem to see any danger.

In addition, there is a paradox: while the majority of respondents use GAFAM services every day, and perceive these services as essential or even irreplaceable, 67% of respondents do not trust these companies. Only 7.6% of respondents say they have a relatively high level of trust. Concerning the degree of confidence for each of the 5 actors:

- Google: while on average 115 respondents use its services daily, 95 say they do not trust the company at all,

- Facebook: while 160 respondents use its services several times a day, 133 say they do not trust this actor at all,

- Amazon: while 119 respondents say they rarely use Amazon and 52 do never use it, 107 say they do not trust the company at all

- Apple: only 42 respondents use its services several times a day and 89 do never use it, however 90 respondents say they do not trust the company at all,

- Microsoft: while 70 respondents use it every day and 38 do never use it, 69 do not trust the company at all.

In addition, 73% of respondents do not trust social networks, while as seen above, a large number use them every day. No respondents indicated that they trust social networks, only 9 people say they have a relatively high level of trust by assigning a score of 4/5. 71% of respondents also do not trust connected objects, while 9.2% trust them relatively well by assigning a score of 4/5.

The massive and recurrent use of GAFAM services suggests that individuals are dependent on those actors. However, the very strong lack of trust prevents the author from validating the third assumption. It would seem that the cause of the high use of digital services is due to something other than dependence. We can consider the lack of alternatives or the impact of the sociability network that keeps users inside, professional constraints can also force individuals to use certain tools. The third assumption: "Individuals are dependent and addicted to GAFAM" cannot be confirmed nor displayed as the reality of behaviors is not so polarized.

4.5. The lack of alternatives

The lack of major competitors against GAFAM confine users in their habits without leaving the possibility of trying other alternative services. While 73.3% of respondents do not find that GAFAM services are irreplaceable, respondents do not seem to know of any alternative solutions. Indeed, 68.5% do not know of any applications or software that are respectful as regard to the collection of personal data. Apart from the Mozilla web browser, which according to the respondents is substitutable for GAFAM services (240 votes), as well as Linux and Qwant, which are only moderately substitutable (177 votes for Linux and 123 for Qwant), the other alternatives exposed in the questionnaire are not substitutable for GAFAM services according to the respondents. Their answers can be interpreted in two ways: the proposed solutions are not known by respondents who indicate that they are not substitutable, or respondents actually believe that these solutions are not at all substitutable.

Moreover, 63.7% of respondents said they do not know any free software. More generally, 41 participants find that free softwares are moderately substitutable for GAFAM, 14 respondents believe that free softwares are fully substitutable and 11 respondents find that free softwares are not at all substitutable. The low rate of respondents does not allow to obtain a representative result and at the same time highlights the real ignorance of users for alternative solutions. Furthermore, 36.3% of respondents think that GAFAM has no competitors, 19.1% do not know.

Figure 7: Proportion of users who think that GAFAM are irreplaceable among those who think they do not have competitors

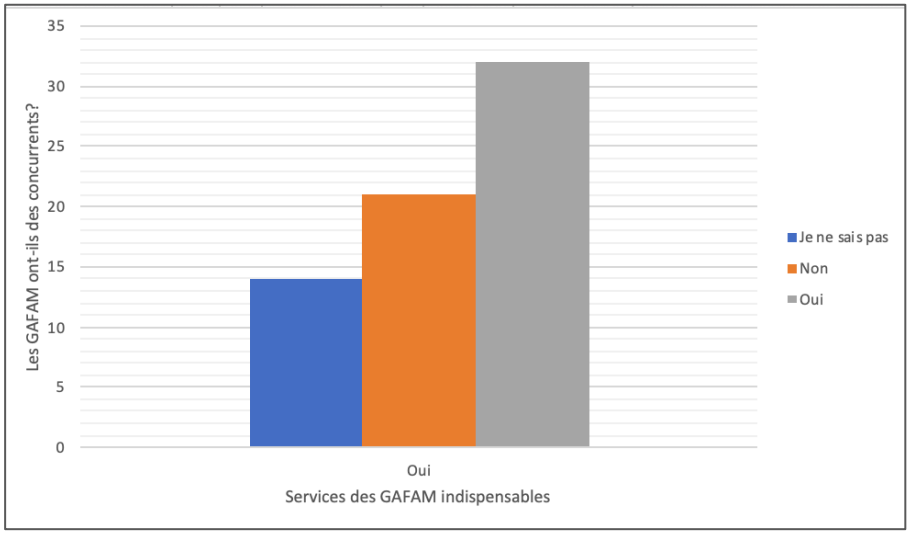


Figure 7 shows that among those respondents who believe GAFAM are irreplaceable (67 respondents), 21 believe that GAFAMs have no competitors, 32 believe that they do and 14 do not know.

Figure 8: Proportion of users who think that GAFAM have competitors among those who are familiar with free software

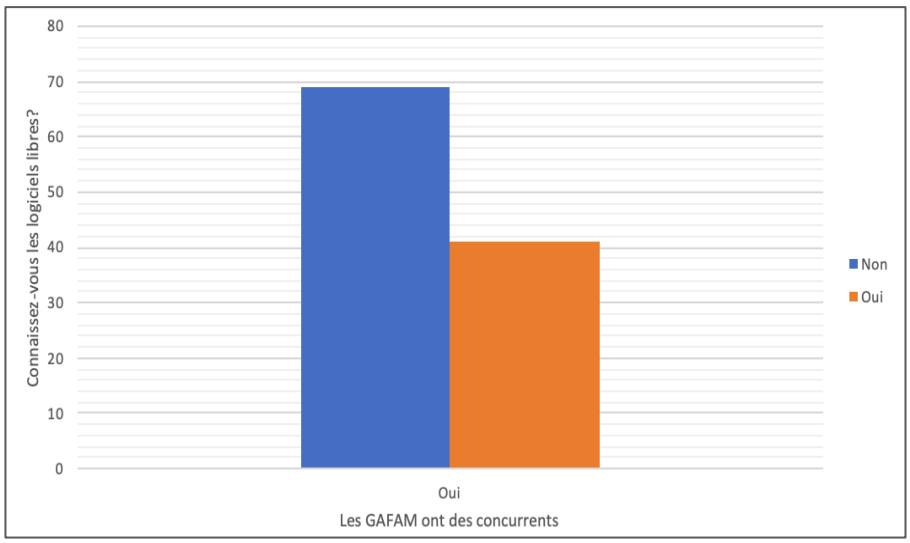


Figure 8 shows that among users who think that GAFAM has competitors (110 respondents), only 41 are aware of free software. We can then consider which other competitors can respondents think of, future or existing solutions? In any case, it appears that individuals are not familiar with existing alternative solutions, which does not help them to escape GAFAM control.

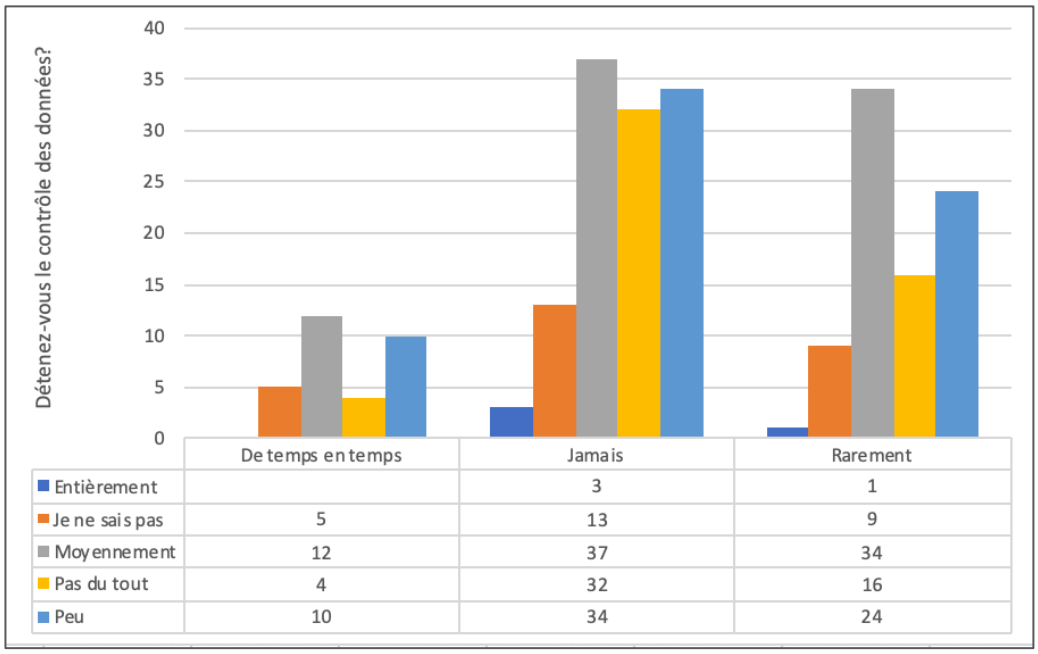
In addition, 98% of respondents believe that GAFAM have an impact on society. Respondents therefore recognize the power exercised by digital companies, which, although being private sector actors, manage to have a global hold on their users. In addition, 90.4% of respondents believe that GAFAMs should be more closely monitored. This further underscore the recognition of GAFAM's power. Responders therefore find that digital companies hold too much power and therefore it is necessary to act through the legal body to regulate their practices.

Thus, the fourth assumption which is: "The lack of alternative reinforces GAFAMs' power", can be validated.

4.6. The consent to surveillance and control

As exposed in section 4.3 Personal data value, 48.2% of respondents never read the general conditions of use, 33.5% only rarely and 12% from time to time. They automatically accept without being aware of their content. However, by accepting the conditions, they unconsciously submit to GAFAM surveillance and control, since they agree to be monitored in all their movements and to transmit their personal data to GAFAM algorithms, which can thus produce behavioral predictions. In addition, 35.5% of respondents think they have moderate control over their data, 29.5% think they have a little control, 21.9% do not have any control at all and 11.6% don't know.

Figure 9: Percentage of users who accept the general terms and conditions of use among those who believe they do not have control over their data



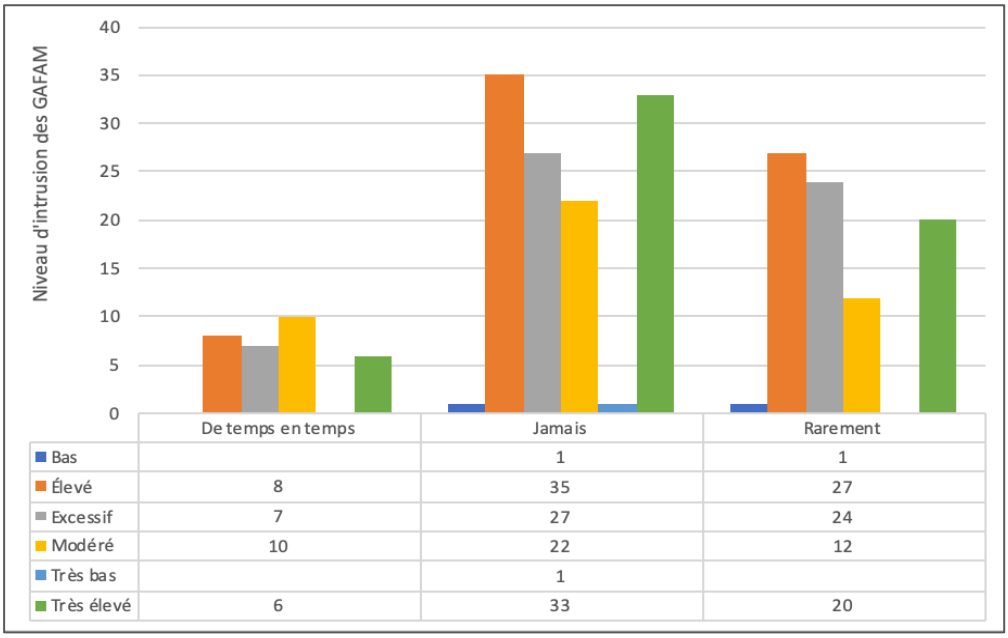
	De temps en temps	Jamais	Rarement
Entièrement		3	1
Je ne sais pas	5	13	9
Moyennement	12	37	34
Pas du tout	4	32	16
Peu	10	34	24

Figure 9 shows that among respondents who accept the conditions of use without ever reading them, 37 respondents think they hold their data moderately, 34 think they have a little control and 32 think they do not have control at all; among those who read the conditions of use very rarely, 34 respondents think they hold their data moderately, 24 a little and 16 not at all; and finally among respondents who read the conditions of use only occasionally, 12 respondents think they hold their data moderately, 10 a little and 4 not at all. However, one has noticed that 3 people who accept the terms of use without ever reading them, think they have full control over their data.

Nevertheless, this figure is very low and not representative. It is rather paradoxical to see that individuals are concerned about controlling their data even though they give to GAFAM the permission to collect and use them. This paradox underlines the unconscious nature of this phenomenon.

In addition, 26.3% of respondents find that the degree of GAFAM intrusion into their private lives is excessive, 25.1% think it is very high, 28.7% it is high and 18.7% moderated.

Figure 10: Proportion of users who accept the general conditions of use among those who believe that the level of GAFAM intrusion into private life is too high



	De temps en temps	Jamais	Rarement
Bas		1	1
Élevé	8	35	27
Excessif	7	27	24
Modéré	10	22	12
Très bas		1	
Très élevé	6	33	20

Figure 10 shows that among respondents who accept the conditions of use without ever reading them, 27 respondents find the level of GAFAM intrusion into their private lives to be excessive, 33 find it very high and 35 find it high; among respondents who rarely read the terms of use, 24 respondents found the level of GAFAM intrusion into their private lives to be excessive, 20 found it very high and 27 found it high; and among respondents who accepted the terms of use by reading them from time to time, 7 respondents found the level of GAFAM intrusion into their private lives to be excessive, 6 found it very high and 8 found it high. Thus, individuals perceive the consequences of GAFAM surveillance and control, and it annoys them, but it is possible in part because of their initial consent.

Moreover, 201 respondents believe that social networks are not at all suitable or secure for transmitting sensitive information, indicating that they fear being tracked or observed. The same is

true for 170 respondents who think that instant messaging is not suitable for transmitting intimate data, 100 respondents also think that email is not suitable. Finally, respondents find that the "least bad" option is the telephone call or SMS, except that these tools are also used by GAFAM to collect data and monitor individuals. Social networks are perceived as the least suitable, probably because of multiple media scandals. However, this mistrust of individuals calls into question their unconsciousness of the surveillance phenomenon. If individuals want to protect themselves and are suspicious of GAFAM tools, it is because they may understand the issues behind the simple use of digital services. Individuals seem lucid about the dangers.

This is especially true since 48.2% of respondents strongly agree with the statement "If it is free, it is because you are the product", 21.5% agree and 17.5% do moderately agree. Only 6.8% of respondents disagree. In total, almost 72% of respondents agree with the idea that they are the product of a transaction between actors they do not know through their personal data. Individuals therefore understand, in a very simplified approach, the functioning of surveillance capitalism.

Thus, individuals may unconsciously consent to surveillance because they accept the conditions of use, but they are fully aware later on of the data collection that takes place for the benefit of GAFAM. The fifth assumption is therefore not fully validated, as it cannot be deduced whether individuals become aware of the existence of monitoring and control before or after accepting the conditions. Nevertheless, they are at least partially aware, which is a significant discovery.

5. DISCUSSION

5.1. Theoretical inputs

The analysis of the results showed that individuals are aware of the financial value of their personal data. They know their data is collected to be resale to others. In this sense, individuals then understand in a very simplified way the beginnings of surveillance capitalism, of which they are also the actors. However, as Tristan Nitot pointed out, they do not realize the scope of what the definition of personal data encompasses. As a result, they can only partially protect themselves against the GAFAM offensive. They remain unaware of the unequal exchange in which they participate, the transaction they agree to do each time they use a digital service. In reality, they are only identifying one part of the problem for the moment. Individuals do not realize that every time they accept terms and conditions of use without thinking, without paying attention to their content, they deal a “pact with the devil”, they unconsciously accept to give their privacy. However, later on, they find that GAFAM are too intrusive and refuse to allow them to process their data in order to offer personalized services. The position of users revealed by the quantitative results highlights the inconsistency of their discourse. Without all the elements to get to the heart of the matter, individuals cannot really mobilize themselves. Information asymmetry persists, and this is what must be countered by educating individuals about the extent of the data capture problem. But above all, it is necessary to empower users as they fully participate in surveillance capitalism, and it is their duty to be aware in order to be able to protect themselves and act.

This work therefore shows that there is some awareness of the surveillance phenomenon among the public, but users still need to be made more aware.

5.2. Methodological inputs

Methodological inputs of this thesis lie in the choice of the survey methodology. As during the collection of secondary data, a lack of quantitative evidences related to the topic has been noticed, the author wanted to address this problem by providing quantitative insights about the digital practices of GAFAM users. However, in order to fully understand the issues of the research subject, the author did not want at the same time to limit her work to a simple collection of quantitative data. Thus, the survey methodology which mix qualitative and quantitative methods has been chosen.

This approach firstly provides precise information and knowledge about the studied phenomenon. It enabled to frame the subject, define the research question, clarify theoretical concepts and formulate research assumptions thanks to the qualitative method of exploratory expert interviews.

The quantitative approach and the collection of quantified output through the online questionnaire made it possible to identify global trends, to understand individuals' perception of GAFAM and their habits in using digital services. This method helped the author to confirm or disprove research assumptions and to formulate well-founded answers to the initial research question.

Thus, the survey methodology was the appropriate method to deal with this subject as qualitative approach explored the subject and quantitative approach verified if the theory can be applied to practice and the real world. This methodology mixes two methods that are complementary and thus gives more legitimacy to the drawn conclusions.

5.3. Empirical inputs

The research carried out confirmed the author's hunches and certain assumptions.

Indeed, all the individuals interviewed have modern electronic collars embodied by smartphones or, to a lesser extent, connected watches that follow them in their slightest movements, and continuously generate data and traces, recovered by GAFAM.

Individuals make extensive use of digital tools and services, with a preference for Google and Facebook services that are used by the majority of respondents several times a day. Apple and Microsoft services are also used several times a day or week but by a smaller proportion of respondents. Amazon services, on the other hand, are used only "rarely" by the majority of respondents. Nevertheless, it is difficult to say whether or not individuals are addicted to GAFAM, as the majority of respondents find that those services are not irreplaceable and would not be ready to pay if these services became paid for. In addition, respondents show a high level of mistrust of digital companies, the degree of trust granted is very low for each actor and individuals want GAFAM to be closely supervised by public authorities.

Moreover, the research conducted raised the lack of knowledge on the respondents about alternative solutions. Indeed, individuals are not aware of the existence of free software and other workarounds. The lack of information prevents them from turning to alternative solutions and thus from leaving the GAFAM enclave. It is therefore necessary to promote the existence of digital services that are respectful of personal data and privacy, so that people can gradually move away from GAFAM towards new, more ethical innovations.

The current lack of alternatives reinforces the power held by GAFAM. Respondents recognize the power of digital platforms and agree that they influence today's society. Nevertheless, they are skeptical about these actors and want their activities to be supervised.

Concerning the value of personal data, individuals agree that they have a financial value and can therefore be the subject of a transaction, nevertheless only 1/3 of respondents think that data is a market good like any other. In the majority of cases, individuals perceive the particular status of personal data and are aware of the need to protect it. They are also wondering about the themes of privacy protection and control; one can imagine that they gradually want to take charge of the management of their own data instead of leaving it in the hands of a third party.

Finally, on monitoring and control issues, respondents are aware of the dangers they face, recognize that digital tools are not the best means of communicating intimate content and are therefore suspicious of GAFAM surveillance and tracing. Nevertheless, one step remains neglected

by all respondents: acceptance and submission to the terms and conditions of use, without being aware of the content of this "contract". Individuals have still not realized the importance of this step, which requires their voluntary consent for monitoring and massive data collection. It is necessary for individuals to make more efforts to protect themselves in virtual space. This for example requires a control of navigation settings and cookies.

Thus, although aware of certain aspects of GAFAM functioning, individuals must be more sensitizes to all the issues involved in this phenomenon.

5.4. Management recommendations

The management recommendations that can be made to conclude this research are at three levels: individual, collective and institutional.

Individual level

It appears as obvious that with all the benefits offered by GAFAM and new technologies (opening up, access to information, instant communication, sharing of knowledge, etc.), it is impossible to tell people to stop using all connected services overnight. Nevertheless, it is their duty and responsibility to take charge of their digital sovereignty and destiny. Individuals should ask themselves more questions about the free nature of the offered services, about what makes GAFAMs financially profitable instead of choosing the easy solution by avoiding the problem. As in any international problem, individual awareness is necessary to make a difference since it is not acceptable to have only the choice between submitting to GAFAM power or giving up the use of their services and thus being excluded from network of sociability. It is necessary to reverse the feeling of submission to the machine and to the invisible guardian inside the panopticon tower, and to regain power over personal data. Harcourt (2015) speaks of digital disobedience, which is indeed a possible approach. Individuals should refuse to use services that harm them and focus on those that respect them. It is therefore their duty to find out about the existing alternatives and to protect

themselves at their own level by controlling cookies, for example, or managing browsing settings. It is necessary to counter complacency, to enquire in order be aware of the danger and to be more vigilant in virtual space.

Collective level

At the same time, things must evolve to generate a collective mobilization, not a gathering of anti-GAFAM activists. The “struggle” cannot be individual, because the problem is not individual but global. Joint actions are needed to make of privacy an asset for digital services. If users join forces and simultaneously boycott GAFAM services, it can have a significant impact on these companies. If users start to choose existing alternatives such as free operating systems, this will give to others the opportunity to develop new innovations. Individuals may then consider to soon be spoilt for choice among solutions that respect their privacy and free will. Collective mobilization is necessary, as GAFAM surveillance and control is a global problem that concerns all individuals: 249 respondents out of 250 interviewed have a smartphone. No one is safe even if they think they are. It is therefore necessary to work towards digital services that respect their users.

Institutional level

Finally, it is the duty of the States, and with regard to this study of the French State, to supervise GAFAM and their business models, and to limit their power by reducing the knowledge they have of their users. This does not only involve GAFAM taxation. European regulations are a good beginning, but it is necessary to go beyond and work even harder to protect privacy. The State must respect its part of the Social Contract and has to submit the companies that operate on its territory instead of submitting itself to them. Especially since France is the country of Human Rights, it would therefore be consistent for France to set an example on this international issue. In addition, the State should educate and transmit a digital culture to citizens to introduce them to the dangers of virtual space and open their eyes on invisible and intangible problems. It is necessary to

explain to individuals the existence of surveillance made by digital platforms and encourage them to limit the traces they leave on the Internet.

Thus, joint actions are needed to combat GAFAM surveillance and control: changing individual behavior and making users more responsible; developing global awareness and working towards digital disobedience; and finally imagining deeper institutional reorientations that will lead to digital education for citizens and legislative changes. Nevertheless, the ideal solution to counter surveillance capitalism remains the invention of a more viable economic counter-model than the pseudo-free one, which would no longer be based on personal data.

5.5. Limitations

The research carried out has some limitations that need to be presented. The limits mainly concern data collection and data analysis.

5.5.1. Data collection

Secondary data and exploratory interviews

During the bibliographic research and the literature review writing, the author had to make choices by focusing on certain sources, targeting some documents at the expense of others. Therefore, interesting secondary data, that could have contributed to and have been cited in this thesis, were not selected, as it was impossible to read everything.

In addition, the author was able to conduct only five exploratory interviews, which provided very interesting and useful elements for the research but are not representative of all the points of view existing on the subject. Indeed, many experts did not respond to requests for interviews even

though their arguments would have been very enlightening and relevant (these include employees of La Quadrature du Net and researchers who have published papers on digital surveillance issues).

The use of GAFAM services to denounce GAFAM practices

It is very paradoxical to note that this research denouncing GAFAM practices of control and surveillance, and of massive data extraction uses their services to carry out this thesis. Indeed, the author has an Apple MacBook computer and used: Google Search for secondary data researches; Microsoft Word to write this thesis; Gmail and LinkedIn to contact the experts to be interviewed; Apple MacBook recorder and Skype to conduct the exploratory interviews; Google Forms tool as a support for the online questionnaire, Facebook and LinkedIn social networks to distribute the questionnaire and Microsoft Excel to analyze the quantitative results. This clearly shows the constant use and predominant place of these actors in individuals' daily lives.

The online questionnaire

As explained in section 3. Research Methodology, the chosen sampling technique – the convenience sampling - does not allow to construct a truly representative sample. Since the questionnaire was published on social networks, it was therefore difficult to control the age groups of the respondents, knowing that the people likely to have access to it are in fact author's social network "friends" and are therefore mostly the same age. To counter this bias and try to heterogeneize respondents, the author sent the questionnaire by email to a group of relatives and colleagues having different ages and different socio-professional backgrounds, but this did not fully balance the respondents' profiles.

The author compared the results of the questionnaire with the official data published by INSEE (Institut national de la statistique et des études économiques) in 2016 (see Table 3: Comparison of the collected quantitative data with the official INSEE data for 2016). Imbalances are observed: some parts of the population are over-represented, while others are under-

represented. These differences are explained by sampling errors as well as by the absence of economic, social, and geographical targeting.

The lack of representativeness is a significant limitation, because as Paugam (2012) states: "*a poorly designed sample may lead to misrepresentation. Its quality is therefore a major requirement*".

Table 3: Comparison of the collected data with the official INSEE data (2016)

Variables		**Questionnaire**	***Total in France***	***Spread (points)***
Sex	Female	62,5%	*51,5%*	***+ 11***
	Male	37,5%	*48,5%*	***- 11***
Status	Executives and high-level intellectual professions	30,4%	*17,5%*	***+ 12,9***
	Employees	13,5%	*27,5%*	***- 14***
	Intermediate professions	2,8%	*26%*	***- 23,2***
	Craftsmen, shopkeepers and heads of companies	3,6%	*6%*	***- 2,4***
	Without employment (students, unemployed)	41,4%	21%	***+ 20,4***
	Retirees	2,4%	*6,9%*	***- 4,5***
	Other	6%		
Study level	A-level	7,2%	*15%*	***- 7,8***
	A-level+1			
	A-level+2	7,6%	*12%*	***- 4,4***
	A-level+3	10%	*10%*	***0***
	A-level+4	8,8%		
	A-level+5	64,1%	*16%*	***+ 48,1***
	PhD	2,4%	*1%*	***+ 1,4***
Class of age	18-24	51%	*10%*	***+ 41***
	25-34	26,3%	*11,8%*	***+ 14,5***
	35-44	9,2%	*12,4%*	***- 3,2***

	45-54	5,2%	*13,5*	***- 8,3***
	55-64	6,4%	*12,6%*	***- 6,2***
	65+	2%	*20%*	***- 18***

In addition, the limited diffusion time (two weeks from the 15th till the 28th of July 2019) is also a limitation of this research, since it can be assumed that a longer time period could potentially have brought higher results.

5.5.2. Data analysis

The use of Microsoft Excel as analysis tool

Although it has provided very useful information for the research conducted, Microsoft Excel is not the most efficient tool for performing quantitative analysis. More sophisticated tools do exist and would have generate more relevant correlations. However, the very limited Excel skills of the author did not allow her to achieve a very thorough work. The author has tried to do her best to manipulate the results and obtain meaningful indicators.

Moreover, some issues have not been analyzed at all or not in sufficient depth, because it was beyond the author's skills to cross-check some complex data.

Author's knowledge of quantitative techniques is also a limitation, as it was the first quantitative research carried out and it was not a well mastered approach for her. Some methodological mistakes could have been made and the analysis of the final results may be limited.

Framing effect

It is possible that by carrying out the questionnaire, the author unintentionally induced certain types of answers, even if precautions were taken to formulate the questions in the most neutral way. The language, form, choice of answers may have influenced the respondents.

In addition, author's close family and friends who have participated to the questionnaire may have been influenced in their responses, as these people were familiar with the research subject and the author's opinions. Their views on the subject may have been influenced by the author's earlier arguments. This unconscious bias could have led to polarize the answers and hence, may have distorted the empirical reality of participants' opinions. Thus, the data collected and analyzed may be biased and therefore not fully representative.

Halo effect

It is possible that questionnaire results may present a *Halo effect* (theorized by Thorndike in 1920 and Asch in 1946), which is a cognitive bias that affects the way people interpret information. A question or response modality may have changed their interpretation of the following questions or all response modalities. Thus, the data collected and analyzed may be subject to this bias, which does not make them fully representative.

Social desirability bias

According to Lugen (2017), it is impossible to know if individuals were sincere in their answers. They may have wanted to answer "in the good way" instead of giving their real point of view. This bias refers to the fact that respondents may want to give a positive image of themselves and therefore respond as they think it would be appropriate to, rather than give their personal opinion. The data collected and analyzed may be subject to this bias, which does not make them fully representative.

The misunderstanding of question 6 part 5 of the online questionnaire

The author received some feedback from those who completed the questionnaire and some people indicated that they had doubts about the interpretation of question 6 part 5 of the questionnaire: “For each proposal, indicate the level of sensitivity of the information”. Some people understood the “level of sensitivity” as the ability of GAFAM and its algorithms to access information or not, while others understood it as the confidentiality of the information that is necessary or not to protect. Given the misunderstanding and the raised doubt, the author decided not to analyze this question.

« I don’t know » issue

As Bourdieu (1973) points out, the assumption that everyone should have an opinion consists of ignoring the “non-responses”, and “*eliminating non-responses means to impose on the opinion survey the implicit philosophy of the electoral survey*”, namely not to take into account blank ballots. For this reason, the author gave respondents the opportunity to choose the “I don't know” option. However, it is difficult to interpret the meaning of these “non-responses”. The « I don’t know » option is present in 10 questions, and the rate of choice of this answer sometimes falls below 7% or exceeds 42%. A good understanding and interpretation of these “non-responses” would have been necessary but is beyond the skills of the author.

5.6. Future research avenues

The collection of secondary data and the exploratory interviews provided the author with further avenues that could not be addressed in this thesis, as it goes beyond the scope of the research. However, it opens up for future research avenues.

Links between economic and political surveillance

GAFAM are private companies that operate worldwide and are thus global actors. They hold very accurate information in large quantities about their users who are at the same time citizens. Access to this “gold mine” may be perceived as an opportunity by sovereign States who could wish to seize these gigantic databases. As early as in 2013, the Snowden case revealed the existence of American and British surveillance systems, which are based on metadata capture and tracking of people’s activities on the Internet. One might then wonder which would be the consequences of a potential collaboration between GAFAM and the secret services of the States. Especially since the American Government is already requesting information from Google and Apple on targeted individuals for various security reasons, as Nina Cercy says. She points out that what is not known, I the fact that GAFAM agree to share confidential information with the American Government most of the time. The knowledge of digital companies is so extensive that they have become potential strong partners for political authorities. It would therefore be interesting to consider a study on this possible collaboration, while the Chinese government is about to set up the Social Credit System - a national citizen rating system based on digital mass surveillance tools and Big Data. By joining forces with the country's two largest technology companies - Alibaba and Tencent - no information will escape the Chinese government.

The question of responsibility

As highlighted in the last section of the literature review, the issue of responsibility remains open and deserves to be further explored. All the stakeholders of surveillance capitalism have their share of responsibility as they fuel the new system of capturing and transmitting nowadays value, which is personal data. However, they are not always aware of it, as are the users themselves, who accept the conditions set by the GAFAM, but do not have a macro vision of the situation and the extent of the phenomenon. There is also the question of the States’ responsibility, which for the moment do not sufficiently regulate the practices of digital companies, however it is their duty to put in place efficient legislation to protect against surveillance. Privacy should be a political issue

in the same way as social protection, economic policies or international relations, because it is a prerequisite for a well-functioning Democracy.

GAFAM surveillance within private companies and other organizations

It would also be interesting to study GAFAM surveillance in private companies that use digital services on the same basis as ordinary citizens. The company in which the author is doing her apprenticeship provides Apple tools to all employees; the company in which the author is on a mission is equipped with Microsoft services; more generally, Google and Facebook services are used on a daily basis in the workplace to access information or to communicate with collaborators. This raises the question of the transmission of confidential data to GAFAM, which can then very easily decipher the company's strategy.

6. CONCLUSION

6.1. A brief synthesis

This research provided a better understanding of digital habits and individuals' perceptions of GAFAM and their practices. It appears that the latter are aware of the issues surrounding personal data and wish to strengthen the protection and control of their data online. Although they may wish to counter GAFAM services, they are not yet sufficiently aware of the existence of more ethical alternatives. Finally, although the monitoring process is broadly understood, individuals still do not protect themselves enough and leave many traces behind in the virtual universe. They need to take more responsibility and question their role as users in today's surveillance capitalism.

6.2. Closing personal remarks

I enjoyed working on this subject as I find it captivating and very topical. I realized how much we all lack digital literacy, how unaware we are of the dangers of the web and vulnerable to GAFAM, and especially how little we question ourselves about the world around us.

This work made me want to work on my own scale for the protection of privacy by raising awareness among my family and friends and by focusing more on alternative solutions. In this way, I try to prevent my entourage from being the privileged accomplice of digital companies in their surveillance and control activities. I remain convinced that, it is by transmitting information and warning everyone around, that individual habits may change, and collective mobilization can result.

In addition, I also want to orient my professional project towards cyber security professions in order to act jointly with other professionals in favor of a more respectful Internet.

So that web utopia - the universal space open to everyone - does not turn into dystopia.

7. REFERENCES

7.1. Publications

Charmet, A. (2016). Preface to *Surveillance : Les libertés au défi du numérique : Comprendre et agir*. Caen: C&F éditions.

Damasio, A. (2016). *La zone du Dehors*. Paris: Gallimard.

Foucault, M. (1975). *Surveiller et punir : naissance de la prison*. Paris: Gallimard.

Granai, G. (1967). Techniques de l'enquête sociologique, in George Gurvitch, *Traité de sociologie*, tome premier. Paris, Presses Universitaires de France, 1967, pp. 135-151.

Harcourt, B. E. (2015). *Exposed. Desire and Disobedience in the Digital Age*. Cambridge: Harvard University Press.

Huxley, A. (2006). *Brave new world*. New York: Harper Perennial.

Kantorowicz, E. H. (2016). *The king's two bodies: A study in medieval political theology*. Princeton, NJ: Princeton University Press. (Original work published 1957).

La Boétie, E. de. (2010). *Discours de la servitude volontaire*. Bordeaux, (Eds.) Mille et une nuits. (Original work published 1576).

O'Neil, C. (2016). W*eapons of Math Destructions: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.

Nitot, T. (2016). *Surveillance : Les libertés au défi du numérique : Comprendre et agir*. Caen: C&F éditions.

Nitot, T., & Cercy, N. (2016). *Numérique : reprendre le contrôle*. Framasoft.

Orwell, G. (2013). *1984*. Paris: Gallimard. (Original work published 1949).

Razac, O. (2008). *Avec Foucault, après Foucault : Disséquer la société de contrôle*. Paris: L'Harmattan.

Thiétart, R. A. (2008) (Eds). *Méthodes de recherche en management*. Edition Dunod, Paris.

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

7.2. Scientific articles

Amintas, A. (2002). *Une généalogie des techniques de contrôle : une lecture de Michel Foucault*. Retrieved from https://halshs.archives-ouvertes.fr/halshs-00584424

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance a conversation* (Polity Press). Retrieved from http://nbn-resolving.de/urn:nbn:de:101:1-201412266662

Belk, R. W., & Llamas, R. (2013). *The Routledge companion to digital consumption*. London; New York: Routledge.

Boulay, J. (2016). Le pouvoir panoptique des technologies et systèmes d'information : définition, mesure et implications. *Systèmes d'Information et Management*, *12*(4). Retrieved from: https://aisel.aisnet.org/sim/vol12/iss4/2

Bourdieu, P. (1973). L'opinion publique n'existe pas. *Les temps modernes*, 318. Retrieved from: http://www.homme-moderne.org/societe/socio/bourdieu/questions/opinionpub.html

Caluya, G. (2010). The post-panoptic society? Reassessing Foucault in surveillance studies. *Social Identities*, *16*(5), 621-633. https://doi.org/10.1080/13504630.2010.509565

De Vaujany, F. X., Aroles, J., & Leclercq-Vandelannoitte, A. (2019). The complex question of responsibility in 'more-than-human' assemblages. 3rd Dauphine Phenomenology Workshop (DPW). *Machinism and animality: Experiencing work and management in the digital era.*

Deleuze, G. (1990). Post-scriptum sur les sociétés de contrôle. *L'autre journal*, *1*. Retrieved from https://infokiosques.net/spip.php?article214

Doyle, A. (2011). Revisiting the synopticon: reconsidering mathiesen's « the viewer society » in the age of web 2. 0. *Theoretical Criminology*, *15*(3), 283-299. https://doi.org/10.1177/1362480610396645

Festré, A., & Garrouste, P. (2015). The 'Economics of Attention': A History of Economic Thought Perspective. OEconomia, (5-1), 3-36. https://doi.org/10.4000/oeconomia.1139

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605-622. https://doi.org/10.1080/00071310020015280

Humphreys, A. (2006). The consumer as foucauldian "object of knowledge". *Social Science Computer Review*, *24*(3), 296-309. https://doi.org/10.1177/0894439306287975

Isaac, H. (2018). La donnée numérique, bien public ou instrument de profit ? *Pouvoirs*, *N° 164*(1), 75-86

Jaeger, M. (2009). Du principe de responsabilité au processus de responsabilisation. Vie sociale, 3(3), 71-81. doi:10.3917/vsoc.093.0071

Kessous, E. (2011). L'économie de l'attention et le marketing des traces. Text presented at the conference « *Web social, communautés virtuelles et consommation* », 79e Congrès de l'ACFAS (Université Bishop's et Université de Sherbrooke). Retrieved from: http://manuel.boutet.free.fr/Kessous2011attention.pdf

Leclercq-Vandelannoitte, A. (2017). Victime ou coupable ? Repenser le rôle du contrôlé dans la relation entre contrôle, information et technologies de l'information. *Systemes d'information management*, *Volume 22*(2), 49-80.

Leclercq-Vandelannoitte, A., & Isaac, H. (2013). Technologies de l'information, contrôle et panoptique : Pour une approche deleuzienne. *Systèmes d'information & management*, *18*(2), 9. https://doi.org/10.3917/sim.132.0009

Lianos, M. (2003). Social Control after Foucault. *Surveillance & Society*. Retrieved from http://www.surveillance-and-society.org/

Lugen, M. (2017). Petit guide de méthodologie de l'enquête. Université Libre de Bruxelles. Retrieved from : https://igeat.ulb.ac.be/fileadmin/media/publications/Enseignement/Petit_guide_de_méthodologie_de_l_enquête.pdf

Lyon, D. (2007). Surveillance, security and social sorting: emerging research priorities. *International Criminal Justice Review*, *17*(3), 161-170. https://doi.org/10.1177/1057567707306643

Lyon, D. (2007). *Surveillance, power, and everyday life*. https://doi.org/10.1093/oxfordhb/9780199548798.003.0019

Lyon, D. (2010). Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies. *International Political Sociology*, 4(4), 325-338. https://doi.org/10.1111/j.1749-5687.2010.00109.x

Lyon, D., Haggerty, K. D., & Ball, K. (2012). *Routledge handbook of surveillance studies*. Abingdon, Oxon ; New York : Routledge.

Mathiesen, T. (1997). The viewer society: Michel Foucault's « panopticon » revisited. *Theoretical Criminology*, *1*(2), 215-234. https://doi.org/10.1177/1362480697001002003

Milburn, P. (2007). Surveiller et punir au XXIe siècle : Les nouvelles technologies du contrôle social en France. *Journal des anthropologues*, (108-109), 159-182. https://doi.org/10.4000/jda.1087

Paugam, S. (2012). L'enquête sociologique en vingt leçons. In: Serge Paugam éd., *L'enquête sociologique*. Paris cedex 14, France: Presses Universitaires de France. doi:10.3917/puf.paug.2012.01.0002.

Paquette, J. (2018). De la société disciplinaire à la société algorithmique : considérations éthiques autour de l'enjeu du Big data. *French Journal For Media Research.* Ethics, Media and Public Life. Retrieved from http://frenchjournalformediaresearch.com/lodel-1.0/main/index.php?id=1439

Ricœur, P. (1994). Le concept de responsabilité. Essai d'analyse sémantique. *Esprit*. Retrieved from: https://esprit.presse.fr/article/ricoeur-paul/le-concept-de-responsabilite-essai-d-analyse -semantique-11196

Richards, N. M. (2013). The Dangers of Surveillance. *Harvard Law Review*. Available at SSRN: https://ssrn.com/abstract=2239412

Rouvroy, A. (2017). La vie n'est pas donnée. *Etudes Digitales*. Retrieved from https://www.academia.edu/31846143/La_vie_nest_pas_donnée

Rouvroy, A. (2018). De la surveillance au profilage. Philosophie Magazine, Hors-Série N°36. Foucault. Le Courage d'être Soi. Retrieved from https://www.academia.edu/36177927/De_la_surveillance_au_profilage_Philosophie_magazine_Hors-s%C3%A9rie_N_36._Foucault._Le_courage_d%C3%AAtre_soi._2018_

Sabot, P. (2012). Une société sous contrôle ? A propos d'Olivier Razac, Histoire politique du barbelé (2000 ; rééd. Champs-Flammarion, 2009) ; Avec Foucault, après Foucault. Disséquer la société de contrôle (L'Harmattan, 2008). *Methodos. Savoirs et textes*, (12). Retrieved from http://journals.openedition.org/methodos/2941

Salès-Wuillemin, E. (2006). Méthodologie de l'enquête, in : M., Bromberg et A., Trognon (Eds.) *Psychologie Sociale 1*, Presses Universitaires de France, 45-77.

Schneier, B. (2006). The eternal value of Privacy. Retrieved from Wired website: https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html

Singh, S. & Lyon, D. (2013). Surveilling consumers: the social consequences of data processing on Amazon.com. In: Russell W. Belk & Rosa Llamas, *The Routledge Companion to Digital Consumption*. Routledge, London. https://doi.org/10.4324/9780203105306

Slobogin, C. (2005). Transaction Surveillance by the Government. *ResearchGate*. Retrieved from https://www.researchgate.net/publication/228274446_Transaction_Surveillance_by_the_Government

Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, *90*(4). https://doi.org/10.15779/Z382H8Q

Solove, D. J. (2007). « I've Got Nothing to Hide » and Other Misunderstandings of Privacy. *San Diego Law Review*, *44*. Retrieved from https://scholarship.law.gwu.edu/faculty_publications/

Webster, W. R., Krieger-Lamina, J., Leleux, C., & Cas, J. (2013). *Social Perspectives of Surveillance and Democracy. Increasing Resilience in Surveillance Societies*. University of Stirling. Retrieved from https://www.researchgate.net/publication/264217485_Social_perspectives_of_surveillance_and_democracy

Willcocks, L. P. (2006). Michel Foucault in the social study of ICTs: critique and reappraisal. *Social Science Computer Review*, *24*(3), 274-295. https://doi.org/10.1177/0894439306287973

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

7.3. Reports

Ball, K., Lyon, D., Murakami Wood, D., Norris, C., & Raab, C. (2006). *A report on the surveillance society. For the Information Commissioner by the Surveillance Studies Network*. Retrieved from https://www.researchgate.net/publication/241917099_A_Report_on_the_Surveillance_Society

Rouvroy, A. (2016). *Des données et des hommes. Droits et libertés fondamentaux dans un monde de données massives.* Conseil de l'Europe. Centre de Recherche Information, Droit et Société. Retrieved from http://www.crid.be/pdf/public/7689.pdf

7.4. Sitography

Auffray, C. (2019). Chiffres clés : les systèmes d'exploitation sur PC. [Online], Retrieved from ZDNet website: https://www.zdnet.fr/actualites/chiffres-cles-les-systemes-d-exploitation-sur-pc-39790131.htm?p=3

Charmet, A. (2015). Google, le rêve de vivre sans État. [Online], Retrieved from Club de Mediapart website: https://blogs.mediapart.fr/edition/les-invites-de-mediapart/article/300715/google -le-reve-de-vivre-sans-etat

Clarke, R. (1987). Information Technology and Dataveillance. [Online], Retrieved from http://www. rogerclarke.com/DV/CACM88.html

Clarke, R. (2006). What's « Privacy » ? [Online], Retrieved from http://www.rogerclarke.com /DV/Privacy.html

Clarke, R. (2016). Introduction to Dataveillance and Information Privacy, and Definitions of Terms. [Online], Retrieved from http://www.rogerclarke.com/DV/Intro.html

Coëffé, T. (2018). Chiffres Google – 2018. [Online], Retrieved from BDM website: https://www.blogdumoderateur.com/chiffres-google/

Day, M., Turner, G., & Drozdiak, N. (2019). Amazon Workers Are Listening to What You Tell Alexa. [Online], Retrieved from Bloomberg website: https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio

Dekonink, B. (2019). Facebook admet à son tour avoir écouté les conversations de ses utilisateurs. [Online], Retrieved from LesEchos website: https://www.lesechos.fr/tech-medias/hightech/facebook-admet-a-son-tour-avoir-ecoute-les-conversations-de-ses-utilisateurs-1124314

Hern, A. (2019). Apple contractors 'regularly hear confidential details' on Siri recordings. [Online], Retrieved from The Guardian website: https://www.theguardian.com/technology /2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings

Hervé, L. (2019). Les 50 chiffres à connaître sur les médias sociaux en 2019. [Online], Retrieved from BDM website: https://www.blogdumoderateur.com/50-chiffres-medias-sociaux-2019/

Marchand, L. (2018). Apple en sept chiffres démesurés. [Online], Retrieved from LesEchos website: https://www.lesechos.fr/finance-marches/marches-financiers/apple-en-sept-chiffres-demesures-136070

NASDAQ Companies. (2019). [Online], Retrieved from Nasdaq website: https://www.nasdaq.com/screening/companies-by-industry.aspx?sortname=marketcap &sorttype=1&exchange =NASDAQ

Nitot, T. (2016). Une société sous surveillance n'est plus une société libre. [Online], Retrieved from BDM website: https://www.blogdumoderateur.com/tristan-nitot-societe-surveillance -societe-libre/

7.5. Radio broadcasts

Andrade, A., & Mira, E. (2019). Le prix du gratuit : Gratuité, données, publicité. [Online], Retrieved from France Culture website: https://www.franceculture.fr/emissions/entendez-vous-leco/le-prix-du-gratuit-34-publicites-donnees-gratuite

Bourmeau, S. (2016). Ni Foucault 2.0 ni Debord 2.0. [Online], Retrieved from France Culture website: https://www.franceculture.fr/emissions/la-suite-dans-les-idees/ni-foucault-20-ni-debord-20

Delorme, F., Allezard, C. (2016). Le monde pris en filature : Google, Facebook, Amazon... l'espion dans la poche. [Online], Retrieved from France Culture website: https://www.franceculture.fr/emissions/culturesmonde/le-monde-pris-en-filature-24-google-facebook-amazonlespion-dans-la-poche

Greewald, G. (2014). Why privacy matters. [Online], Retrieved from TED website: https://www.ted.com/talks/glenn_greenwald_why_privacy_matters

Jaron, L. (2018). How we need to remake the internet. [Online], Retrieved from TED website: https://www.ted.com/talks/jaron_lanier_how_we_need_to_remake_the_internet

8. APPENDICES

Appendix 1 – Interview guide and interview summary

Formal structure	Formal substructure	Duration expected
Part 1	1.1 Self-introduction and presentation of the research question 1.2 Description and explanation of subject research 1.3 Interviewee introduction	15 min
Part 2	2.1 GAFAM practices and the use of ICTs 2.2 Mass surveillance and Foucault/Deleuze theoretical approaches	20 min
Part 3	3.1 Data merchandizing 3.2 Surveillance capitalism and Shoshana Zuboff theoretical approach	15 min
Part 4	4.1 Privacy and personal rights 4.2 Sovereignty and digital autonomy	15 min
Part 5	3.1 Conclusion and perspectives 3.2 Closing remarks and thanks	8 min

Part 1

Thème 1 : Présentation de l'interviewé

1. Pouvez-vous me parler de vous, de votre parcours et de votre carrière ?
2. En quoi consiste votre poste en tant que … ? / Pouvez-vous me présenter vos sujets de recherche ?

Part 2

Thème 2 : Données personnelles et contrôle des individus

1. Qu'est-ce qu'une donnée personnelle ?
2. Dans quel but sont stockées les données personnelles ? (Cf. GAFAM)
3. Comment reconnaitre une donnée pertinente ?
4. En quoi la collecte de données personnelles est-elle dérangeante voire dangereuse ?
5. Quel est votre avis sur la collecte, stockage, chiffrage et exploitation des données personnelles ?
6. Concentration des données en silos : quels risques ?
7. Comment sont analysées les données ? Selon quels critères ?

Thème 3 : Surveillance de masse

1. Les GAFAM nous surveillent-ils ? Surveillance invisible
2. Est-on réellement surveillé ou seulement tracé ? Quelle différence entre surveiller et tracer ?
3. Peut-on dresser un parallèle entre les pratiques des GAFAM et les théories de Michel Foucault ? Panoptique, biopouvoir, savoir/pouvoir, société disciplinaire, intériorisation du contrôle et des normes
4. Peut-on dresser un parallèle entre les pratiques des GAFAM et les théories de Gilles Deleuze ? Société de contrôle, société de traces, « collier électronique », prison à ciel ouvert
5. Pourquoi les gens s'asservissent-ils volontairement aux géants du numérique ?
6. Surveillance mène au contrôle : que faire pour réveiller les masses ?

Part 3

Thème 4 : Marchandisation des données

1. Que pensez-vous de ce nouveau modèle économique basé sur les données personnelles où l'utilisateur est le produit/bien marchand ?
2. Que pensez-vous du fait que les GAFAM influencent les envies et désirs des foules ?
3. Que penser de la monétisation et du marchandage des données personnelles ? Parallèle avec les théories de Shoshana Zuboff

Part 4

Thème 5 : Vie privée et droits individuels

1. Selon vous, les individus sont-ils sensibilisés à ces sujets ?
2. La souveraineté sur les données numériques : quels enjeux ?
3. Que pensez-vous du profilage : analyse prévisionnelle du comportement, porte-t-elle atteinte aux droits et aux libertés fondamentales des personnes ?
4. Que pensez-vous du RGPD, est-ce une solution ?
5. Droit à la portabilité : les individus peuvent-ils ainsi retrouver la souveraineté sur leurs données ?
6. Selon vous, la portabilité offre-t-elle plus de liberté aux individus ?
7. Pourquoi les gens ne voient-ils pas l'intérêt de se réapproprier leurs données ? Est-ce le résultat d'un manque de responsabilité de leur part ? Pourquoi tant de désintérêt ?
8. Argument du « rien à cacher » difficile à déconstruire : que faire ?

Part 5

Thème 6 : Conclusion / Ouverture / Remerciements

1. Quelles évolutions possibles de la situation actuelle ?
2. L'internet libre est-il une solution ?
3. Qui d'autre selon vous devrai-je contacter ? Avez-vous des contacts à me recommander ?
4. Remerciements

Appendix 2 – Interview summary

Identity	Occupation	Date of issue	Place of issue	Duration	Number in the thesis appendix
Aurélie LECLERCQ-VANDELANNOITTE	Researcher in Management Sciences and Professor at IESEG Business School	23/05/2019 at 10:00 am	Teleconference call	35 min	1
Marc TAKABACHET	Sales Executive Finance & Risk, SAP France	24/05/2019 at 3:00 pm	Teleconference call	1 hour	2
Nina CERCY	Cybersecurity Consultant, EY Author of *Numérique : Reprendre le contrôle*	N°1: 04/06/2019 at 12:15 pm N°2: 06/06/2019 at 9:30 pm	Teleconference call	N°1: 1.10 hour N°2: 45 min	3
Jérémy AROLES	Assistant Professor in Organization Studies in the Business School of Durham University	12/06/2019 at 11:00 am	Skype	1.00 hour	4
Tristan NITOT	VP Advocacy, Qwant	21/06/2019 at 2:00 pm	Skype	1.15 hour	5

Appendix 3 – Interview Transcript #1

Interviewer: Zuzanna Sonenberg
Interviewee: Aurélie LECLERCQ-VANDELANNOITTE, Researcher in Management Sciences and Professor at IESEG Business School
Interview Setting: Interview conducted via teleconference call on May 23rd, 2019, at 10:00 am CET, with the support of Apple MacBook recorder.

(Start of Interview)
(Presentation of the interviewer and the research topic, see Appendix 1 – Interview guide)

Pouvez-vous me parler un peu de vous ?
Avec plaisir, moi aussi je suis un ancienne de Dauphine, du DEA 101 à l'époque. Dès le départ j'aimais bien la théorie de Michel Foucault, je trouvais que c'était vraiment une pensée très riche et puis j'avais voulu l'appliquer à ma thèse, donc voilà j'en suis venue à un sujet de thèse dans lequel je pouvais appliquer la pensée de Michel Foucault, donc étudier le contrôle en lien avec les systèmes d'information mobiles à travers la perspective foucaldienne, et c'est au cours de ma thèse que j'ai rencontré François Xavier de Vaujany parce qu'il était membre de mon jury de thèse et qu'il m'a beaucoup conseillé aussi. Donc voilà, depuis j'ai travaillé sur toutes ces notions, sur la pensée de Michel Foucault, le contrôle. Mais là c'est vrai que ça fait quelques années que je m'en détache un petit peu, parce que maintenant avec François Xavier on travaille sur les nouvelles pratiques du travail, mais j'ai toujours certaines parties de mes recherches avec Foucault, et j'essaie toujours d'appliquer sa pensée. En tout cas je pense que, même s'il y a déjà eu beaucoup beaucoup de choses d'écrites dessus, il y a toujours à faire, que les évolutions technologiques et sociétales qu'on constate sont beaucoup à acquiescer à un cadre conceptuel très riche. Je ne peux que vous encourager à comprendre et appliquer ces notions.

Pourriez-vous me dire, selon vous, quels seraient les liens entre les théories de Michel Foucault et les GAFAM ? Personnellement les premiers liens que j'avais établis avant de commencer mes recherches c'étaient les notions de surveillance, de panoptique…
Oui bien sûr, je pense qu'en effet on pourrait prendre des notions dans la pensée de Foucault qui pourraient illustrer, conceptualiser un peu ce que font les GAFAM. Les points saillants sont ce que vous dites, un système de surveillance omniprésent, parfois inconscient même. C'est vrai que les utilisateurs ne se rendent même pas compte de cette surveillance, utilisateurs qui sont à la fois des « objets de savoir », des « objets de pouvoir » mais également des « objets de savoir », il y a vraiment cette notion de pouvoir / savoir qu'on retrouve dans ce modèle. Après concernant le système de surveillance de masse, vous avez certainement vu le livre de Zuboff de 2019, je pense

que c'est bien d'y faire référence aussi, pour cette logique de captation des données à l'insu des utilisateurs la plupart du temps, parce que souvent il n'y a pas toujours de grande prise de conscience de la nature des données qu'on livre, ou alors inconscience de l'implication que cela va avoir.

Pourrait-on alors qualifier les GAFAM de cyber-panoptique ? Une sorte d'évolution de la société disciplinaire vers un monde plus liquide et une sorte de cage dorée où on ne se rend plus compte de la surveillance opérée ?
Oui tout à fait, c'est une sorte de cage dorée, qui n'est pas forcément visible, qui n'est pas architecturale au sens physique du terme comme l'employait Foucault, mais sur l'aspect conceptuel, oui complètement. C'est d'ailleurs un prolongement avec Deleuze, donc lier les deux c'est très bien aussi.

Pouvez-vous me parler des liens que l'on peut faire avec Deleuze ?
C'est l'idée de société de contrôle. Deleuze a prolongé la pensée de Foucault, en expliquant qu'aujourd'hui on est moins dans une société disciplinaire qu'une société de contrôle, et cette société de contrôle est vraiment un prolongement de la société disciplinaire. Je pense notamment à l'article de Willcocks qui résume toute la pensée de Michel Foucault, où à la fin l'auteur explique pourquoi aujourd'hui, malgré cette société liquide, malgré ce que disait Munro qui critiquait pas mal la pensée de Michel Foucault, et il mettait en opposition l'idée de réseau par rapport à l'idée du panoptique, mais Willcocks montre bien comment la pensée de Foucault et son prolongement avec la pensée de Deleuze est toujours très actuelle et permet de comprendre comment la discipline s'affranchit des contraintes spatiales et temporelles, devient invisible et conduit à une autodiscipline qui est quasi intégrée, vue comme normale par les individus. A la fin de l'article, il y a toute une partie où il explique que… Parce que Bauman critiquait aussi les écrits de Foucault à un moment : dans cette société liquide, le panoptique n'a plus vraiment sa place, on n'est plus dans cette architecture de surveillance, mais justement le panoptique va bien au-delà de ça. C'est plutôt une métaphore de la société disciplinaire, de surveillance telle qu'on l'observe aujourd'hui et encore plus évoquée avec les GAFAM.

Et que penser des « colliers électroniques » de Deleuze ? Je pensais faire un parallèle entre les TIC, les smartphones et les « colliers électronique » …
Complétement, complétement. On parle de prison à ciel ouvert. Deleuze montre comment on est passé à des sociétés de contrôle, par exemple de la prison au bracelet électronique, au ciblage électronique, la continuité des enfermements de l'institution pénitentiaire qui est toujours là, elle est réelle, elle est massive, omniprésente et insidieuse. Ça se relie complètement.

Et que penserez alors Michel Foucault des GAFAM s'il était encore en vie aujourd'hui ?
C'est une excellente question, c'est vrai que Michel Foucault est mort juste avant toute cette ère digitale, cette ère de l'information. Il parlait de technologie mais pas au sens qu'on entend aujourd'hui, c'étaient plus des technologies disciplinaires. Qu'est-ce qu'il en penserait… C'est difficile, je pense qu'il serait heurté quand même, un petit peu comme l'est Zuboff. Le système de

surveillance massive qui est mis en place par ces sociétés, je trouve que c'est une illustration complète de sa pensée, ça montre à quel point il a été visionnaire je trouve. Même si certains disent que c'est la fin du panoptique, qu'on est à une époque qui décloisonne, notamment le panoptique, bin non c'est la métaphore qu'il faut voir, ce système de surveillance à l'échelle mondiale qui est mis en place, une mise en matière totale d'un individu pris comme « objet de savoir » et « objet de pouvoir », et le pire dans tout ça c'est que c'est insidieux, c'est une forme d'adhésion implicite, insidieuse à un système invisible dont on ne se rend pas forcément compte.

Et si je revenais à cette notion de savoir / pouvoir, est-ce que le pouvoir des GAFAM serait un pouvoir totalisant et disciplinaire ou bien un micro pouvoir ? Car Michel Foucault parle d'un ensemble de micro-pouvoirs qui encadrent la société pour remettre les déviants dans le groupe social. Quel serait ici le rôle des GAFAM ?

Moi j'ai plutôt l'impression qu'on est dans un système bien organisé, de surveillance totale. Alors ce n'était pas forcément l'objectif de départ, c'est ça qui est étrange dans cette histoire, c'est qu'au départ ce n'était pas vu comme tel et puis au final, Google a évolué et puis on se rend compte que c'est devenu un cyber panoptique, un super panoptique digital. Je suis d'avis comme Zuboff que c'est un pouvoir quasi totalisant. Je me souviens que Zuboff prend l'exemple du jeu Pokemon Go, où elle montre que l'utilisateur à son insu ne sait pas que ça sert à quadriller des espaces qui ne l'ont pas encore été, qu'on invite l'utilisateur à se rapprocher d'enseignes qui ont au préalable signé des contrats avec Google, puis dès que la personne se rapproche, l'entreprise va être payée, au moindre rapprochement. Fin c'est quand même assez global, assez totalisant, totalitaire. Je vois cette logique-là. Après l'idée de micro pouvoir c'est peut-être dans l'essaimage des mécaniques de pouvoir qu'on trouve aujourd'hui un peu partout, on a diverses instituions qui vont encadrer le comportement de l'individu, c'est en ça qu'on peut voir des micro-pouvoirs. Après avec les GAFAM, on est vraiment dans une logique de surveillance de masse.

Quand Michel Foucault parle de biopouvoir et de gestion de la vie, pourrait-on dresser un parallèle avec les GAFAM, sachant qu'ils opèrent une sorte de gestion algorithmique de nos vies ?

Oui, aussi, c'est vrai. Je connais un petit moins le biopouvoir, mais je pense que c'est aussi une question de « la gestion des moindres parcelles de la vie » comme dit Foucault. Gestion à travers des algorithmes, une connaissance fine des moindres désirs et envies des individus, de ses comportements, le profilage des individus. Après je ne sais pas quelle fin pourrait illustrer ça. La question de la finalité… C'est plus difficile d'y répondre car ce n'est pas comme le pouvoir pastoral qui veut le bienêtre, le salut dans l'au-delà de l'individu. C'est plus une logique pécuniaire qu'il y a derrière. Mais après sur l'aspect de la gestion de la vie des individus, on y est complétement.

Vous m'avez parlé à plusieurs reprises de Zuboff, que pensez-vous de ce nouveau modèle économique basé sur les données personnelles, où l'utilisateur devient le bien marchand ?

Ça fait très peur. Ça pose quand même beaucoup de questions par rapport à notre devenir, à notre sociabilité individuelle et collective dans l'évolution de ce modèle, dans ce qu'on est capable de faire en retour. C'est vraiment problématique. Le vrai problème c'est qu'il n'y a pas encore de

réelle prise de conscience je trouve, la plupart du temps les gens, les jeunes, les enfants ne se rendent pas forcément compte de ce qu'il se passe, du fait d'être sur internet. Je ne pense pas qu'il y ait une grande prise de conscience au niveau mondial, des répercutions et implications possibles de ce modèle de captation de données.

Avez-vous identifié des solutions ? Qu'est-ce qu'il faudrait faire ?
C'est une bonne question et c'est très difficile d'y répondre. Il faudrait un électrochoc, une prise de conscience collective, prendre conscience des implications que cela amènerait à tout un chacun de revoir ses comportements, puis à remplacer ces dispositifs.

Est-ce que l'utilisation de services de l'internet libre, de moteurs de recherche comme Qwant, serait une solution ?
Oui oui bien sûr, je connais plusieurs personnes qui le font maintenant, moi-même je le fais quand j'y pense. C'est plus un réflexe qui doit s'institutionnaliser, parce qu'on a tellement l'habitude de passer par Google ou par d'autres plateformes qui sont devenues des standards que voilà, c'est une démarche qui doit changer. Mais oui clairement, pour moi passer par d'autres plateformes c'est une belle piste.

Pourquoi selon vous les personnes adhèrent si facilement aux GAFAM ?
Il n'y a pas beaucoup de choix je trouve. Ça parait tellement comme une évidence que… On ne se pose même plus la question de faire autrement. C'est une réalité pour beaucoup de monde.

Quelles sont les impacts que cette surveillance a sur nos libertés et droits individuels ?
C'est une atteinte à la liberté de chacun de penser d'une certaine façon. Quelque part nos comportements sont comme dictés, puis la captation de données fait qu'aujourd'hui ces plateformes nous connaissent mieux que nous-même, elles vont anticiper nos besoins. Je pense que c'est clairement une atteinte à la vie privée, même si elle n'est pas reconnue comme telle par les GAFAM, mais clairement ça en est une.

Est-ce que les choses vont changer ?
J'espère, je trouve qu'il le faut, c'est nécessaire. Je ne sais pas comment vu qu'on est tellement embarqué dans ce système difficile à changer, mais il faut vraiment qu'il y ait une prise de conscience pour faire changer les choses. Alors peut-être que c'est en train de changer. On voit quand même émerger je trouver quelques critiques notamment d'anciens de Google. Il y avait un article dans Le Monde d'un ancien de Facebook qui expliquait qu'on avait dépassé la limite du tolérable. Peut-être qu'il y aura donc une prise de conscience à ce niveau-là, puis qu'il y aura des actions prises pour essayer de nous dire que la captation de données, ou que au moins l'utilisateur en ait conscience, qu'il y ait vraiment une prise de conscience au niveau globale.

Le problème c'est que les GAFAM sont des entreprises américaines qui échappent…

Oui complètement, c'est vrai que je n'ai pas du tout abordé ce point mais c'est vrai qu'il y a une mainmise américaine, un colonialisme américain sur les données des individus au niveau mondial. C'est assez effrayant.

Je pensais faire un parallèle également avec la Chine, avec cette société de surveillance poussée à l'extrême dans un pays où il y a certes une dictature…
Oui complètement, c'est une super idée. Je ne sais pas si François Xavier vous a passé un petit article sur lequel on a travaillé, dans lequel on n'utilise pas Foucault mais Ricœur parce que c'est sur la notion de responsabilité individuelle et collective, mais peut-être que ça peut vous permettre d'ouvrir un petit peu le débat à la fin. Ça peut vous être utile.

Quels liens pourrait-on faire entre la pensée de Ricœur et la surveillance ? Vu que vous parlez de la notion de responsabilité, ce serait pour voir qui est responsable de tout ça ?
C'est ça, c'est qu'aujourd'hui on est dans des assemblages de plus qu'humains. Les algorithmes, l'intelligence artificielle font partie intégrante de notre expérience et aujourd'hui questionnent, interpellent quant à la question de la responsabilité individuelle et collective. On explique dans l'article à quel point il est difficile aujourd'hui de séparer notre expérience au monde, d'identifier ce qui revient en termes de responsabilité à la technologie et à l'individu lui-même ou à la notion de collectif. Par exemple, quand Google a créé son assistant qui prend des rendez-vous automatiquement chez un coiffeur, ou alors lorsqu'ils ajoutent des intonations humaines et que ça leurre complètement l'individu en face qui croit qu'il a à faire avec un être humain alors que c'est juste une machine. Aujourd'hui on est de plus en plus impliqué dans le digital dans nos actions quotidiennes, c'est en ça que vous pouvez peut-être faire un lien avec votre recherche à la fin. Aujourd'hui toute action passe par la technologie et ça interpelle quant à ces questions de responsabilité individuelle et collective. Après c'est vraiment une ouverture sur Ricœur, faites-en ce que vous voulez, c'était pour illustrer cette notion de responsabilité.

Merci beaucoup, c'est très intéressant. Une autre question que je me posais en vous écoutant, c'est comment expliquer ce paradoxe où une part au moins de la population est un peu sensibilisée à cette surveillance, notamment avec l'affaire Snowden, Wikileaks etc., mais ils restent quand même très attirés vers les services numériques ?
C'est vrai que je ne me l'explique pas non plus, mais c'est un vrai paradoxe. Ça interpelle notre nature humaine, c'est assez choquant presque de voir que les usages n'ont pas beaucoup changé par rapport à avant même s'il y a eu ces révélations. C'est assez surprenant mais les causes, les racines, les raisons de ce paradoxe sont très dures à expliquer, après ça relève peut-être de la psychologie humaine, des comportements moutonniers ou des habitudes de chacun, le fait qu'on n'ait pas le choix peut-être. C'est vrai qu'il n'y a pas beaucoup de changement dans les usages alors que bon, plus que jamais il serait question de remettre en cause ces usages individuels et collectifs.

Pensez-vous que les internautes croient vraiment qu'Internet est gratuit et que tous les services auxquels nous avons accès sont réellement gratuits ?

Ça dépend à qui on s'adresse mais je pense qu'une grande majorité… Peut-être que je me trompe, il faudrait faire un sondage mais hormis quelques personnes qui sont sensibilisées à cette problématique, qui ont lu des choses dessus, qui sont au courant de ces affaires, je ne suis pas sûre qu'il y ait une grande prise de conscience au niveau mondial. Moi quand j'en parle à mes étudiants, ils le savent oui mais sans avoir conscience de toutes les implications je trouve.

Donc finalement on rejoint cette question de responsabilité, car c'est à la fois inconscient mais aussi irresponsable de la part des gens ?
Oui complètement.

C'est donc peut-être les individus qui ne se questionnent pas suffisamment ?
Oui aussi complètement, et qui agissent sans penser au-delà, sans penser aux conséquences de leurs actes je trouve. On le voit beaucoup avec les réseaux sociaux, les jeunes fin c'est assez dramatique ce qu'il se passe et ça fait peur aussi je trouve. Quand on voit tout ce harcèlement qu'il peut y avoir sur les réseaux sociaux et sur Internet, ce sont des problèmes assez nouveaux mais extrêmement graves, et ça pose vraiment la question de la responsabilité dans les usages de chacun et de l'importance sociale et affective qu'on accorde à ces outils. Donc je trouve que c'est une bonne idée d'ouvrir sur cette notion de responsabilité.

Merci beaucoup d'avoir accepté de répondre à mes questions !
N'hésitez pas à me recontacter si vous avez encore des questions, en tout cas vous êtes entre de bonnes mains avec Monsieur de Vaujany, et vraiment n'hésitez pas si vous avez d'autres questions, en plus vous avez mon numéro. En tout cas j'ai hâte de lire votre mémoire.

Appendix 4 – Interview Transcript #2

Interviewer: Zuzanna Sonenberg
Interviewee: Marc TAKABACHET, Sales Executive Finance & Risk, SAP France
Interview Setting: Interview conducted via teleconference call on May 24th, 2019, at 3:00 pm CET, with the support of Apple MacBook recorder.

(Start of Interview)
(Presentation of the interviewer and the research topic, see Appendix 1 – Interview guide)

Pouvez-vous me parler un peu de vous ?
Moi je m'appelle Marc Takabachet, je suis chez SAP depuis 9 ans maintenant, sur des sujets et thématiques qui sont autour de la gouvernance, le risque et la conformité (GRC). Ce sont des thématiques qui porte sur le contrôle interne, le contrôle permanent, la gestion des risques, l'audit interne, tout ce qui est fraude, cyber sécurité, voilà c'est sur ces sujets là que j'interviens, au sens où moi mon job de tous les jours c'est d'aider nos clients et aussi nos partenaires à mieux comprendre comment nous SAP on peut les aider avec nos logiciels, vu qu'on est un éditeur de logiciels. Et sur ce sujet que je viens d'évoquer de gouvernance interne des organisations, on peut proposer des logiciels pour les aider, voilà. Et je suis très intéressé et ouvert au débat sur votre sujet. Donc voilà un peu qui je suis. Et donc je vois, j'ai des rendez-vous avec la plupart des membres du SBF 120, CAC40 inclus évidemment, sur ces thématiques, donc des gros groupes comme Danone, Alstom, Sanofi, que sais-je et ainsi de suite, et des groupes un peu moins connus du secteur public, type ministère des finances, la défense, pôle emploi, donc voilà, ça fait finalement un panel d'entreprises assez large. Voilà pour un peu qui je suis.

Pourquoi est-ce que vous vous êtes spécialisé dans cette branche de contrôle interne, fraude, cyber sécurité ?
Je suis tombée dedans il y a assez longtemps, il y a 14/15 ans, avec le scandale qu'il y a pu y avoir avec ENRON, pour vous repositionner un peu c'était un scandale de collusion interne entre, c'est à l'époque où Arthur Andersen existait encore et a été dissout à la suite de ce scandale, puisque Arthur Andersen était à la fois jugée partie, il y avait à la fois les consultants de la partie consulting d'ENRON, les arthuriens qui conseillaient en terme de stratégie, de développement et déploiement des activités d'ENRON, qui conseillaient le management d'ENRON, et de l'autre côté, une autre branche d'Arthur Andersen qui certifiait en tant que commissaire aux comptes, les comptes d'ENRON. Donc là on a quelque chose qui n'existe plus aujourd'hui, mais qui existait à l'époque, qui était donc d'être jugé partie, d'être à la fois conseil et à la fois de certifier les sujets des thématiques qu'on venait de conseiller. Cela a donc déclenché un gros scandale en 2004, avec un

lanceur d'alerte à l'époque, qui n'était pas plus positionné que ça, mais qui était à la CFO, donc à la direction financière d'ENRON, qui a dit « il se passe quelque chose », et là la SEC, le gendarme du marché du NYSE, la bourse new yorkaise, est intervenu en mode « il se passe des choses bizarres », et depuis, il y a eu une nouvelle loi qui est sortie de Sarbanes et Oxley, la loi SOX, qui a beaucoup impacté. La première étape était de dissoudre Arthur Andersen, ça n'existe plus, vous avez aujourd'hui une des parties qui est Accenture et le reste je ne sais plus ce que c'est, et il a était fait mention d'une interdiction réglementaire légale de faire à la fois du consulting et du commissariat aux comptes. Sachant ce contexte, moi ça m'a pas mal influencé, je fais pas mal d'informatique assez généraliste et avec l'arrivée de cette thématique bin j'étais assez intéressé et donc je suis tombé dedans. C'était très intéressant, il y a pleins de choses à faire. Ce sont des sujets pas forcément simples mais très intéressants. Donc je suis venu pas par hasard mais c'était un sujet d'actualité à l'époque et encore aujourd'hui, parce qu'on parle de GDPR aujourd'hui entre autres, en tout cas c'est une thématique assez large qui soulève beaucoup de questionnements à long terme. Donc voilà c'est un sujet qui me plait depuis des années.

Donc la cyber sécurité et la RGPD sont votre cœur de métier ?
Oui, c'est un sujet qui pour nous est hyper impactant, en tant qu'éditeur, en tant que SAP, c'est un sujet qui est très impactant. Pour la GDPR, nous sommes nous considérés comme sous-traitant de l'information donc nous avons des obligations réglementaires assez fortes, puisque les logiciels que nous développons et qui sont implantés, installés par nos clients se doivent d'être GDPR compliant depuis le 25 mai 2018, que ce soit on premise ou en cloud, c'est une thématique qui fait pas mal de buzz en ce moment. Cela a généré beaucoup beaucoup de discussions et de stress avec nos clients pour voir comment on gérait la chose. C'était effectivement hyper tendu et ça posait beaucoup de questions, c'était une vague assez forte de d'interrogations de la part du client pour avoir de l'information. Et après sur la partie cyber sécurité, c'est un sujet sans fin puisqu'à chaque fois que vous traitez un sujet, que vous faites de l'innovation, vous avez toujours des gens qui ne sont pas bien intentionnés et qui veulent accéder à ce qui est le cœur de toute entreprise c'est-à-dire ses données, sa data. Donc ce sont des sujets de fort intérêt pour moi.

Puisque la RGPD a généré beaucoup de questionnements, qu'est-ce qui a posé le plus de problèmes et qu'est-ce que cela veut dire pour une entreprise de se mettre en conformité avec la RGPD aujourd'hui ?
Si je réponds à la deuxième partie sur la conformité, la RGPD au sens informatique du terme c'est assez complexe puisqu'il y a 99 articles, fin il y a énormément de choses, qui accède à la donnée, jusqu'à la cyber sécurité en passant par le DPIA, le registre et ainsi de suite. Tous les prérequis, toutes les demandes, les révisions de la part de la RGPD sont contraignantes par nature puisque ce n'est pas comme ça que fonctionnent forcément les sociétés aujourd'hui. Si je prends le cas de la cyber sécurité, dans le cadre de la RGPD vous avez 72h pour expliquer ce qui a été fait, comment ça a été fait, quelle sont été les procédures, les solutions mises en place pour protéger et alerter, ce n'était pas la norme chez le client. Ça c'est un sujet important pour nous parce que 72h pour répondre quand on est un groupe d'une certaine envergure, c'est limite impossible, 72h c'est un délai très court, donc ça a changé, la RGPD a changé la façon dont l'information est traitée dans

les organisations, parce que ça demande des choses, ça demande à modifier la gestion, le traitement, le stockage, l'archivage, l'effacement des données, qui n'étaient pas typées comme le demandait la RGPD. Dans tous les streams, tous les articles et toutes les stipulations de la RGPD, les entreprises se sont confrontées à un monde nouveau, auquel elles n'étaient pas forcément préparées, et qui leur demandait énormément d'efforts pour se mettre en conformité et à minima dire « on a un projet sur l'archivage, sur l'effacement, et voilà comment on va faire ». Pour le client ça a été un choc car il n'a pas été préparé à ça. Ni les équipes IT, ni les AMOA (assistance à maîtrise d'ouvrage) métier, ni les mandataires sociaux, ni le management. Personne n'était clairement au fait des impacts pour eux en tant que clients. Après en interne chez SAP, nous sommes considérés comme sous-traitants de l'information, donc nous devons fournir à nos clients des solutions GDPR compliant. C'est très compliqué, car ça veut dire que SAP développe des solutions qui intègrent les prérequis, or il y a quand même un temps de développement, un temps de tests, un temps de mise à disposition de ces logiciels auprès des clients, qui est un temps contraint, et qui a effectivement obligé SAP à beaucoup beaucoup bosser pour se dire « au 25 mai, moi SAP je propose des solutions qui sont RGPD compliant ». SAP a fait l'effort. Maintenant que les clients aient implémenté notre solution en temps et en heure, c'est un autre débat et c'est une question de responsabilité entre la mise à disposition, le développement des solutions par SAP, leur mise à disposition et la capacité des clients à les avoir implémentés. Ça revient au premier débat de « est-ce que le client ça les a choqués ? », oui ça les a choqués, parce que c'est un sujet sur lequel ils n'étaient pas prêts.

C'est quoi exactement une donnée personnelle ? Comment pourrait-on la définir et à quel moment on sait que la donnée devient pertinente ?

C'est LA question, LE sujet car tout peut être considéré comme de la data personnelle. C'est bien le problème, car à un moment donné est-ce que c'est une information unique, unitaire dans un champ, est-ce que c'est un mix de deux informations dans deux systèmes différents et le fait de les découper ça en devient des données personnelles… C'est le vrai sujet. Le vrai problème a été de typer, c'est d'ailleurs le premier chantier du client, d'arriver à analyser, à faire ce scoping et savoir qu'est-ce qu'une donnée personnelle pour l'organisation. Beaucoup de sociétés ont dit « moi je ne fais pas du B2C donc je n'ai pas de clients, donc je ne stock pas de données personnelles de clients externes, par contre je stock de la donnée personnelle de mes employés, et là le sujet est effectivement interne donc je dois gérer tout ce qui est flag de certaines données dans mes systèmes : le numéro de sécurité sociale, le profil marital ». Ça va très vite, c'est un mix enfin des définitions officielles existent, mais au niveau informatique c'est un peu plus complexe, car est-ce que c'est vraiment un champ unitaire dans un coin, est-ce que c'est la combinaison des deux, donc forcément derrière si on le voit d'un côté informatique, il faut une base de données qui les stock, qui les archive, qui les efface, et ça veut dire quand même qu'on doit aller assez loin dans la recherche de quelle est cette donnée personnelle, où elle est et comment elle est faite. Après chaque client a sa perception de la donnée personnelle, car effectivement, soit ils ont fait l'analyse eux-mêmes, ils ont un peu regardé ce que disait la CNIL, deux trois choses de cette nature, ils ont passé deux trois coups de fil à des avocats spécialisés, qui leur ont donné une définition claire par rapport à leur contexte business, et donc finalement il y a des définitions qui ne sont pas toujours stables. La définition chez Danone ne sera pas celle de chez Saint-Gobain, ne sera pas celle du Ministère des

Finances ou dans une petite structure. Et cela a des impacts aussi puisque certains vont vouloir être hyper conservateurs et dire que tout est une donnée personnelle donc je vais absolument tout verrouiller. C'est le sujet majeur, c'est à partir du moment où on a défini ce qu'est la donnée personnelle dans l'organisation, et avec ce que j'ai dit, qu'avec chacun on obtient des définitions à géométrie variable, là on peut commencer à pouvoir lancer le projet de GDPR au sens très opérationnel et à pouvoir coordonner les équipes puisque chacun va être impacté. Donc, ça c'est le nœud du problème : comment moi dans mon organisation je définis la donnée personnelle. Et je garantis que les entreprises n'ont pas toutes les mêmes définitions. La réalité elle est là, il y a les textes et la réalité de ce qu'on nous dit tous les jours.

Ces données personnelles sont stockées où exactement ?
Alors, ces données, si on parle un peu d'architecture fonctionnelle technique, si on est dans une société qui fait du B2C, c'est-à-dire qu'elle a des clients, vous allez retrouver des informations sur la partie applicative de type CRM donc Customer Relationship Management, un outil comme Salesforce ou ce genre de chose qui gère le CRM, qui capture les données de mes clients, parce que je fais du B2C donc je stock de la donnée dans le système applicatif, et sous ce système applicatif vous allez avoir des bases de données de type Oracle, IBM, ainsi de suite puisqu'on stock de la donnée sur ces bases de données, mais ce sont deux univers différents. Vous avez la partie applicative et la partie base de données, c'est toujours comme ça que ça fonctionne, vous avez toujours un applicatif et une base de données. Et dans du B2B, vous avez des systèmes de facturation. Vous êtes Danone et vous achetez votre matière première à une société et vous allez la transformer. Donc est-ce qu'on a véhiculé de la donnée personnelle ? Pas forcément, mais le peu de donnée qu'on va avoir va être dans des systèmes plutôt financiers ou de reporting. Là aussi, on va se retrouver avec cette logique d'architecture avec l'applicatif (finance, reporting) et une base de données en dessous. Donc la donnée, elle va se retrouver dispersée, vraiment c'est incroyable, mais elle va retrouver dispersée dans énormément de systèmes, puisqu'après elle va aussi devoir faire des systèmes de réplication, vous allez devoir aussi pour des raisons de sécurité (crash d'un serveur et ainsi de suite, votre base de données disparaît), la bonne pratique c'est d'avoir un système redondant donc avec un serveur quelque part qui va copier le premier serveur juste au cas où, voilà. Vous allez archiver, et vous allez le faire tellement de fois qu'à un moment donné, la donnée va se distribuer dans votre système d'information, donc elle va se retrouver un peu partout. On va être surpris de la retrouver à droite à gauche. Je discutais récemment avec une compagnie d'assurance et ils m'ont dit qu'une donnée chez eux est redistribuée dans 18 systèmes. C'est extraordinaire quand on y pense, donc voilà c'est un peu partout. L'info est finalement stockée de manière, je dirai, assez diffuse.

C'est intéressant, car très souvent on entend parler de la concentration de la donnée en silos et des risques que cela entraine, cela interpelle au contraire quand vous dites qu'au contraire la donnée est dispersée. Mais en fait elle est dispersée au sein d'un même et unique acteur ?
L'aspect silo existe quoiqu'il arrive, vous avez effectivement si on prend une organisation B2C qui fait du marketing, et bien le marketing va avoir ses bases de données concernant les clients, la partie facturation va certainement avoir un peu près la même base, et chacun va travailler en silos, et pour

peu que vous fassiez du télémarketing, le fichier du marketing peut sortir du marketing pour être envoyé à un tiers qui va travailler sur le truc, et si vous faites un événement, le fichier sera envoyé de nouveau, donc vous voyez, c'est pour ça que je parlais de diffusion. On peut être en silos tout en étant diffusé. Si on ne prend que le marketing, il n'y a pas qu'une base de clients au service marketing, ça peut être ailleurs, profiter à droite à gauche pour des opérations marketing, des partages aussi avec des partenaires, on peut avoir du cobranding, et si vous êtes Danone vous donnez votre base de données à un tiers qui vend des gâteaux et des yaourts, et pour le cobranding il aura fallu partager la base de données marketing. La base de données est donc extraite du silo marketing et on l'a diffusée à un tiers qui n'est juridiquement pas Danone mais qui est un tiers avec une responsabilité différente, et même si on a des accords de confidentialité bin à un moment donné tout ça ça circule. C'est compliqué.

Et au moment où ça circule, est-ce que ça devient de la vente de données ? Est-ce qu'on monétise ce transfert de données ?

C'est une bonne question, ça dépend de l'objet de l'échange de cette donnée. Si on est sur une opération marketing de cobranding, on ne va pas vendre cette base de données, on a envie de l'enrichir. Si je m'appelle Danone et que je donne, je partage cette base de données avec un tiers qui fait des gâteaux et des yaourts, on va compléter cette base de données unique en disant « c'est mieux de mutualiser, il a des clients, j'en ai d'autres, il faut un yaourt, un gâteau pour faire un repas complet c'est super, mais on va mixer les deux bases de données et on va faire du cobranding. Au départ chacun avait la sienne, à la fin on a une même et unique base. Qu'est-ce qu'on fait de cette seule et unique base ? On se la partage ? On garde chacun ses petits ? » L'idée c'est qu'est-ce qu'on a eu comme accord au préalable avant cet échange ? Si c'est du cobranding, alors on met chacun en pot, chacun donne sa data. Si c'est Danone qui vend cette base de données à un tiers, bin là je viens de dire « vendre » donc là il la vend tout simplement, là il monétise sa base de données, c'est un asset et là on devrait parler de toute la notion, car on entend beaucoup de data lake, les données non structurées, qui ne sont pas forcément dans des systèmes SAP, Oracle, Microsoft, qui sont dans des systèmes type Hadoop et compagnie, avec des terrains de données, et là il y a de la matière. Si je prends l'exemple de Carrefour avec ses tickets de caisse, les point of sets. Une caisse c'est un point of set, elle enregistre le nombre de yaourts et de gâteaux qui sont partis. Qu'est-ce que je fais de cette donnée ? Est-ce que je vais expliquer à Danone que j'ai vendu X yaourts à Michel, à Paul, à Jacques, est-ce que je vais remonter cette information ou est-ce que moi Carrefour je vais garder cette information, ou est-ce que je vais aller voir le producteur des yaourts et des gâteaux en lui disant « tiens dans ce point de vente je vends tant de yaourts et tu as intérêt à vendre tes gâteaux à Michel, Paul et Jacques ». Et bien là je fais de la vente, donc tous les schémas sont possibles. Tout dépend du pacte qu'on a au début. La donnée est volatile, elle se partage. Qu'est-ce qui protège votre donnée et la mienne ? Et bien pas grand-chose. Et encore là on parle d'une donnée relativement libre. Lorsque je passe en caisse je donne mon nom. En fin de compte je m'en fiche de le donner, j'ai acheté des yaourts et des gâteaux, génial. Mais effectivement, quelques jours plus tard je reçois une pub de quelqu'un qui vend des gâteaux, alors que moi on ne m'a rien demandé. En plus on me dit tiens vous êtes un homme, de quel âge, vous habitez où, quelle CSP ? Et c'est

parti, et là on ne m'a pas forcément demandé mon consentement au sens GDPR. Donc c'est complexe, le consentement c'est un truc complétement dingue.

Oui car cette donnée volatile pose beaucoup de problèmes. Au niveau éthique et déontologique cela pose problème…
Carrément, bien sûr, évidemment c'est de là que partent tous les débats sur les réseaux sociaux. Est-ce qu'on est d'accord pour que cette donnée soit détenue ? Est-ce que je fais part de ma vie, est-ce que je poste sur un réseau social, est-ce que j'ai envie que ce soit monétisé, partagé, envoyé à un tiers, sans que je le sache d'ailleurs, donc sans mon consentement. On est effectivement à un moment critique de cette gestion de la donnée, parce que la data is the oil of the future, c'est vraiment le pétrole de demain. Enfin le pétrole d'aujourd'hui et de demain. Et si on ne me demande pas mon consentement et pas forcément mon avis, alors là effectivement quelqu'un va l'utiliser et vouloir en faire une opération financière. C'est peut-être moyennement éthique et pas du tout déontologique donc là on entre dans un problème sociétal plus large, ce n'est pas que de l'informatique, c'est autre chose.

Mais alors est-ce que la RGPD protège réellement les individus contre tous ces excès et ce problème sociétal ?
Je pense que c'est encore un peu trop tôt, on voit qu'au niveau du déploiement de la RGPD on est en phase 2, la phase 1 a été la nomination d'un DPO et d'un DPIA pour projeter une image de conformité et de compliance. La phase 2 dans laquelle on est aujourd'hui, qu'on expérimente, qui met dans une posture où le client doit opérer dans les systèmes, vérifier que telle et telle data est bien flaguée, et si elle est personnelle elle ne doit pas sortir, donc doit être masquée à tel endroit pour tel ou tel opérateur. On est au début puisqu'on est post 25 mai 2018, un an quasiment après sa sortie, est-ce qu'il y a énormément d'amendes ? Pas tellement finalement. Il y en a eu quelques-unes mais ça n'a pas été une vague réelle. Il y a eu quelques affaires effectivement mais ce n'est pas une vague monumentale d'amendes. Le régulateur est plutôt là à dire « je vais éduquer, je vais expliquer et je vais y aller doucement ». Après il y a eu des cas où il a fallu qu'il intervienne, mais pas tant que ça, donc on est dans une phase 2 où le client se dit « ok comment je fais ? », et là on verra les conséquences de RGPD pour la protection de la donnée. C'est encore trop tôt, il faut laisser encore un peu de temps pour voir si RGPD protège réellement ou si c'est juste une tarte à la crème et que les GAFA et les opérateurs passent à travers. Pour l'instant on n'a pas tapé du poing sur la table contre les GAFA.

Si j'en reviens à SAP, l'entreprise collecte et stocke des données personnelles, quelle est la fin de cette pratique précisément ?
Il y a deux dimensions de SAP, il y a un aspect particulier comme on est un éditeur de logiciels. Quand on considère les solutions SAP implantés par le client, c'est la responsabilité du client de mettre en place les versions mises à jour conformes à la RGPS. Et après si on parle de SAP en tant que société, avec 100 000 personnes dans le monde, oui SAP collecte des données concernant mes collègues mais ce sont deux sujets différents. Votre question c'est par rapport aux logiciels développés par SAP ou par SAP en interne ?

Plutôt au niveau de SAP en interne, vu que l'entreprise collecte beaucoup de données sur ses employés, comment cela se passe, vous devez donner votre accord ?
Je sais qu'on a des DPO en interne par pays, on en a une en France. La collecte des données personnelles des collaborateurs, salariés est plutôt stricte, ou du moins son usage car les DPO font attention à ça. Mais il n'y a pas eu de communication formelle sur l'usage qui pourrait être fait des données personnelles qui sont les nôtres.

Et est-ce que SAP fait du profilage ? Car c'est un des thèmes de la RGPD.
Pour les employés ou les clients ?

Est-ce que vous en faites tout court et si oui dans quel cadre ?
Le profilage est assimilé au département marketing. Techniquement, avec l'arrivée de GDPR, je sais qu'on a demandé à notre base clients, l'autorisation, individuellement, pour savoir s'ils souhaitaient rester dans les bases marketing de SAP. Cet effort a été fait, de d'abord demandé le consentement pour pouvoir ensuite travailler et envoyer, par profilage ou segmentation marketing, des informations à nos clients. La conséquence a été effectivement une perte assez certaine de contacts puisqu'un grand nombre en a profité pour nous demander de les supprimer de nos bases. Donc cela a été une conséquence assez directe de la RGPD. Mais je dirais qu'au départ il faut vraiment faire cette dichotomie, de quel type de société on parle, si on est vraiment dans du B2C c'est-à-dire qu'on est une société qui s'adresse directement à des clients finaux, ce n'est pas forcément le cas de SAP. Nous on vend des logiciels à des sociétés qui elles ont des clients directs, on fait plutôt du B2B2C. Donc on a des clients comme Sanofi, qui vend du doliprane à ses clients, on a Danone qui vend des yaourts et tout ce qu'il veut, et ainsi de suite, ou alors que du B2B, Safran c'est du B2B, il vend des moteurs et des pièces d'avion mais il n'a pas de client individuel, au regard du personae, c'est que du B2B. Donc selon la typologie de société, l'histoire de la donnée personnelle n'est pas la même. Les clients qui font du B2C, nous demandent à ce qu'on puisse les aider à masquer ou au moins à tracer l'accès aux données, et lorsque la donnée n'a plus d'utilité au sens légal, là il y a une histoire d'archivage et d'éventuel effacement. Or effacer une donnée aujourd'hui c'est hyper compliqué. Avec les délais de rétention, il la faut pour telle norme, au niveau fiscal il faut la garder tant d'années, si je prends la PHP c'est 50 ans, la DGSI par le ministère des finances c'est pareil, le fisc ne veut pas supprimer des données. Donc il faut vraiment se poser la question au départ de quel typologie de société on parle, car on parle de RGPD et de ses conséquences, et en fonction de la société ce ne seront pas du tout les mêmes conséquences. Un industriel qui fait du B2B, on a un sujet RGPD interne avec les données des employés. Si on est dans du B2C, là on doit se poser la question, en plus du sujet head chart, de la relation avec le client et de la gestion de leurs données.

Si je peux me permettre quelques questions plus personnelles, quel est votre ressenti à titre personnel vis-à-vis du profilage, à cette collecte de données massive ? Comme vous l'avez dit, la donnée est le pétrole d'aujourd'hui et de demain.

A titre vraiment perso, je trouve ça intrusif. Ce n'est pas la situation que je veux pour le monde de demain. L'objectif n'est pas d'aller dans ce sens-là. C'est assez choquant, de voir que nos data, tout ce que je fais, soit stocké, manipulé au sens prix, transformé puis diffusé. C'est un sujet qui pose des questions structurantes.

Est-ce que les gens autour de vous sont sensibilisés sur ces questions ?
Je pense qu'on a de plus en plus de sensibilisation. Ce n'était pas forcément le cas il y a quelque temps, mais avec tous les scandales, les gens sont un peu près briefés, enfin je pense. J'ai l'impression que les gens comprennent que mettre une donnée quelques part peut amener à des conséquences manipulatoires. C'est effectivement là qu'on observe la dérive, la société de l'information, la société de data ouverte dans laquelle on se trouve est un peu ubuesque. Les gens n'imaginent pas quelles conséquences ça peut avoir, le profilage sur l'orientation qui peut être utilisé par certains industriels, certains partis politiques donc oui c'est inquiétant. Cela m'inquiète et je trouve cela pas normal.

Est-ce que dans votre entourage des choses sont mises en place pour se « rebeller » contre ce système ?
Je pense qu'entre la prise de conscience et la prise d'action, il y a quand même un délai synétique de la réaction qui prend quand même un certain temps. Je trouve que la majorité n'a pas fait de correction. Si on considère qu'un réseau social collecte trop de données et s'en sert comme il le veut sans qu'il n'y ait réellement de contrôle, je dirai qu'il faut dans ce cas la prendre le point et se dire qu'il faut que j'arrête d'utiliser ce réseau social, or ce n'est pas forcément toujours le cas. Il y a la prise de conscience, mais après il y a la prise d'action. J'ai l'impression qu'il y a une décorrélation, une désynchronisation entre les deux (prise de conscience et action).

La RGPD parle du droit à la portabilité, est-ce que grâce à ce droit on pourrait retrouver une souveraineté sur nos données ? Est-ce une solution ?
Il faut qu'elle soit dans l'action et qu'elle se soit vraiment effectuée, donc que les gens soient au courant, qu'on puisse l'exécuter correctement et qu'il y ait un vrai contrôle de cette portabilité, qu'il y ait un feedback régulier et permanent, pas seulement un petit flag pour nous dire « oui j'accepte ». Sur les sites, vous cliquez et acceptez plus ou moins n'importe quoi, c'est global mais pas forcément partiel. Ça a été trop facile pour certains sites marchands ou de réseaux sociaux de dire aux participants qu'ils doivent accepter tout d'un coup. Il faudrait un retour, il faudrait un retour factuel. Je reviens sur l'exemple de SAP, le département marketing de SAP, qui a fait l'effort de contacter tous ses clients par mail en demandant l'autorisation de garder leurs coordonnées etc. Et comme je vous dis, il y en a quelques-uns qui ont dit non. Mais ce n'est pas le comportement de tous. C'était un comportement raisonnable car on est dans du B2B. Après dans du B2C, dans le cadre de réseaux sociaux, on ne le fait pas forcément, la démarche est peut-être différente, on ne veut pas que les gens disparaissent du réseau.

Avez-vous le sentiment d'être surveillé, d'être sous surveillance ? Vu qu'on est dans une « société de traces » où tout est traçable.

Surveillé je ne sais pas si c'est le bon terme, mais tracé oui j'aime bien. Il faudrait faire un personae c'est-à-dire à dire la journée type de quelqu'un comme moi : je prends le métro le matin, je badge, donc j'ai déjà donné une data. J'ai dit à quelle heure je rentrais dans un lieu défini et à quelle heure j'en sortais puisque je rebadge en sortant. C'est déjà une information, je ne suis pas libre d'entrer dans un endroit puis de ressortir dans tel autre. J'ai donné une data en badgeant ma carte Navigo et il y a tout dedans : on sait qui je suis, on sait à quelle heure à quel endroit je suis sorti, sur le quai du métro il y a des caméras, même si on ne m'a pas spécialement demandé mon avis sur le traitement de l'image et ce qu'on allait en faire. C'est sûrement pour des raisons de sécurité, je l'entends il n'y a pas de problème. Je sors dans la rue à Levallois, c'est la ville où il y a le plus de caméras en France, pareil, à quel moment est-ce qu'on m'a demandé mon avis pour me prendre en photo. Et finalement on m'a tracé jusqu'à mon arrivée à SAP où je badge à nouveau, je monte dans l'immeuble, je rebadge à l'étage où je travaille. Je me connecte, il y a une information qui dit à quelle heure je me suis logué. Je vais sur des applications, on peut savoir sur quelles applications je me suis logué. Le midi je paie en carte bleue, on sait ce que j'ai mangé et à quelle heure j'y suis allé. Si je vais prendre un café au Starbucks à un moment donné, hop je laisse à nouveau mes données. Vous voyez, si je fais la liste, si je vous disais que je ne suis pas tracé je serais un abruti fini. C'est pour ça que pour moi surveiller versus tracer ça n'a pas la même connotation, ça n'a pas le même impact. Tracé oui, plus que certaine au vu de l'exemple que je viens de vous indiquer. En une journée, on pourrait prendre un fichier Excel et voir combien de fois et à quel moment, à quelle durée j'ai été tracé du moment où je suis sorti de chez moi, au moment où je suis rentré. Et encore quand je vais rentrer et que je vais regarder la télé, on va aussi pouvoir potentiellement me tracer puisque vous avez des trucs en VOD, en streaming etc. Et encore là on n'est pas en Chine, on n'a pas de caméra biométrique ni d'index social. Là-bas on est arrivé dans un système fasciste, il n'y a pas photo, là-bas ils sont surveillés. Mais en France, je viens de vous décrire ma journée type, j'ai quand même l'impression que j'ai laissé des traces et des logs (pour parler informatique) partout. Ça a pris 2 min et on peut déjà se dire que j'ai été tracé, retracé sans aucun problème. Est-ce que l'étape d'après c'est de m'offusquer, me dire « je fais quoi ? », je ne sais pas. En tout cas tracé oui, surveillé je ne sais pas, peut-être à certains endroits.

Les GAFAM nous tracent plus qu'ils ne nous surveillent ?

Tout va être relié à la sémantique de ce qu'on va mettre derrière surveiller et tracer. Tracer c'est limite passif. C'est comme le radar sur l'autoroute, vous êtes passé, vous étiez à 135km, voilà le flash s'est déclenché. Voilà la machine envoie une amende, c'est tracé, c'est surveillé. Jusqu'au moment où j'étais à 130km il n'y avait pas de problème avec le radar. Ensuite je suis passé à 135 et j'ai été flashé, on m'a envoyé une amende et là je suis vraiment surveillé. Avant j'étais juste tracé, « tiens il est passé là », tant que je n'ai pas été flashé je ne suis pas sous surveillance. Au moment où je suis flashé, là je suis sous surveillance. Tout dépend de la définition qu'on met derrière surveiller et tracer, ça n'a pas la même connotation, ça n'a pas le même impact. Mais effectivement, aujourd'hui les GAFAM c'est quoi leur job ? C'est de collecter de la data, d'en faire une masse qui est monétisable, avec ou sans votre consentement, et de travailler avec ça, d'en faire une data qui doit être segmentée, saucissonnée et distribuée. Après, pour surveiller/tracer, il faut vraiment voir cette histoire de radar, jusqu'où c'est fait sciemment.

Informatique égale information en fait ?
Ah oui informatique égale information oui. Si on vous dit le contraire c'est qu'il y a un problème. L'informatique c'est l'industrie de l'information. Une donnée c'est une information qui a été travaillée et enrichie. Ça devient quelque chose qui est exploitable. Les GAFAM sont pile là-dedans, il n'y a pas de débat.

Les GAFAM utilise cette mécanique en la déviant un peu alors ?
La data c'est un asset, c'est leur oil à eux. Total a des barils de pétrole et les GAFAM ont des bidons de datas, et vous n'allez pas retirer les barils de pétrole à Total, il fait quoi après ? Il ferme. Vous n'allez pas retirer les piles de data aux GAFAM, ils meurent dans la foulée. La data c'est le cœur de tout, surtout chez eux. C'est leur asset principal. Tout ce qu'ils proposent, les services etc., c'est autour de la data, rien d'autre.

Quelle serait alors la solution ? Car on ne va pas faire marche arrière.
Il faut que ce soit fait de manière éthique, de manière contrôlée et contrôlable, de sorte que vous et moi ayons la capacité de traiter correctement cette data. Il n'y a pas de mid term, il faut pouvoir rendre la chose auditable et opposable aux tiers, qu'ils puissent choisir ce qu'ils acceptent et ce qu'ils n'acceptent pas. Autrement on est dans une dérive très claire. Il faut absolument pouvoir avoir la main dessus.

Pensez-vous que c'est réalisable ? Où tôt ou tard il y aura toujours des perversions car l'homme tend vers le profit et va vouloir monétiser les données récoltées ?
C'est une question philosophique, je n'ai pas vraiment de réponse. Là-dessus, c'est assez complexe, qui pourrait le dire, je suis sec là. Ce n'est plus de la gouvernance de données, ce n'est plus de l'informatique, c'est beaucoup plus large, ce sont des questions philosophiques, sociétales. Revenir en arrière non, les gens l'ont accepté. Après il y a eu tellement de scandales par le passé qu'il faut effectivement peut-être réguler un peu et GDPR était dans ce cadre-là. Maintenant est-ce qu'ils ont les moyens, est-ce qu'il y a eu des warnings auprès des GAFAM. Je ne sais plus lequel a déplacé à un moment l'un de ses serveurs pour sortir de la zone euro et pour éviter d'être sous GDPR. Vous voyez le niveau, plus ils peuvent échapper à ce genre de trucs car c'est contraignant, car ça leur enlève une emprise, mieux ils se portent. Revenir en arrière non mais arriver à quelque chose de plus équilibré oui, que chacun ait conscience individuellement de l'impact que peut avoir la donnée personnelle au sens large. C'est un asset et ça les gens l'oublient. Mais votre donnée personnelle est votre asset et pas celui d'un GAFAM, c'est ça le point important. La data personnelle est par essence notre. Ce qui est abjecte c'est de considérer qu'on n'a plus la main dessus et qu'elle devient la propriété pleine et entière des GAFAM, ça ce n'est pas acceptable.

La tendance pour les prochaines années sera une plus forte sensibilisation et plus de réglementations ?
Oui, il le faut. Ce sera la course de la régulation et du contrôle versus des processus échappatoires de la part des GAFAM pour passer à travers les mailles du filet. Nous devons reprendre la main

sur les données personnelles et les GAFAM doivent accepter de redonner du contrôle. C'est un jeu d'équilibre. On est à un moment intéressant structurellement je dirai, car jusqu'à présent on ne se posait pas de questions, là on a une prise de conscience. Maintenant on se pose la question de « comment faire ? », avant ce n'était pas le cas. C'est là où le moment dans lequel on se trouve est intéressant, car maintenant on se pose la question. Pendant personne ne se posait cette question, on était tous content de pouvoir échanger des trucs à droite à gauche. D'un coup, on s'est aperçu qu'on avait perdu la main. Et là on se pose la question de reprendre la main. Il y a une prise de conscience qu'il n'y avait pas avant, car on vivait dans l'euphorie de la nouveauté. Nous on vit cette prise de conscience avec nos clients et je pense que les GAFAM le vivent avec leurs clients. C'est un moment particulier.

Merci beaucoup.

Appendix 5 – Interview Transcript #3

Interviewer: Zuzanna Sonenberg
Interviewee: Nina CERCY, Cybersecurity Consultant, EY and author of *Numérique : Reprendre le contrôle*
Interview Setting: Interviews conducted via teleconference call on June the 4th, 2019, at 12:15 pm CET and June the 6th, 2019, at 9:30 pm, with the support of Apple MacBook recorder.

Interview n°1

(Start of Interview)
(Presentation of the interviewer and the research topic, see Appendix 1 – Interview guide)

Pourriez-vous me parler un peu de vous ?
Aujourd'hui je suis consultante en cybersécurité chez EY. J'ai commencé à m'intéresser au sujet des données personnelles en 2015 un peu près et je suis entrée par le même angle que vous, moi j'ai découvert ça par l'angle de la surveillance de masse, notamment en lisant Alain Damasio. En lisant votre message je me disais qu'il y avait des inspirations damasienne qui étaient assez évidentes. Voilà, donc je suis entrée dans ce sujet comme ça, sachant qu'à l'origine j'étais plutôt partie de l'autre côté, moi je voulais travailler chez Google, je voulais faire de l'intelligence artificielle il y a encore 5 ou 6 ans, et pour le coup la lecture du *La zone du dehors* ça a vraiment été une claque, notamment sur l'aspect social de la surveillance, pas seulement sur l'aspect économique ou sur l'espionnage. Le fait de se rendre compte qu'on ne peut pas dire qu'on s'en fiche, qu'on ne peut pas dire qu'on n'est pas concerné, qu'on ne peut pas dire qu'on n'a rien à cacher, et que ce sont des sujets qui ont un impact sur nous quelle que soit notre position dans la société, quelle que soit notre ville, les choses qu'on fait, les choses qu'on a envie de faire. J'ai continué à creuser en m'intéressant aux logiciels libres, et par cette voie j'ai trouvé des gens qui étaient super intéressés par ces sujets, parce qu'en fait le logiciel libre ça reprend pas mal de thématiques qui sont assez proches de celles de la surveillance de masse à savoir le contrôle, et en se réappropriant également le fonctionnement du logiciel et l'hébergement du logiciel, la façon qu'on a de préserver notre vie privée ou de la déléguer à certains acteurs, typiquement les GAFAM, qui nous proposent des services qui ont comme principale caractéristique d'être super efficaces et gratuits. Qui n'en aurait pas envie, évidemment. Mais ça c'est ce qu'il fait réfléchir au modèle économique, sur cette économie de l'attention qui est pour moi la pierre angulaire du problème.

Le modèle économique de l'attention ?

Oui c'est ça, le modèle économique du captage de l'attention. Aujourd'hui, selon moi, la surveillance ne se fait pas dans un objectif de surveillance. Elle est ensuite instrumentalisée par des États, qui vont profiter de la captation des données effectuée par les GAFAM. Aujourd'hui je pense honnêtement que quand Google dit qu'il est très concerné par la vie privée de ses utilisateurs et quand Facebook le dit aussi, d'une certaine façon c'est sincère, au sens où eux, peu leur importe d'avoir accès à la vie privée de leurs utilisateurs. Ce qui les intéresse, c'est d'être capable d'en déduire des corrélations sur ce qu'ils sont, ce qu'ils veulent, ce qu'ils vont acheter, et ensuite de vendre cette attention aux véritables clients que sont les annonceurs. C'est pour ça que pour moi, il y a cet aspect économique qui joue énormément, au sens où on s'est habitué à utiliser des services dont on est des clients, donc où il va y avoir cette relation de clientèle. Aujourd'hui c'est quelque chose qui a complètement disparu, je ne peux pas dire les GAFAM parce que ce n'est pas tout à fait vrai, c'est surtout le cas pour Google et Facebook, les autres ont finalement un modèle économique plutôt différent et la surveillance chez eux est quasiment secondaire.

Vous voulez dire que pour Google et Facebook est secondaire ou pour les autres ?
Non non non, pour les autres. Pour Google et Facebook elle est absolument primaire car c'est là-dessus que repose leur modèle économique. Pour moi aujourd'hui Google et Facebook ont un système qui est assez clair. Ils font l'intégralité quasiment de leurs revenus avec de la publicité. Pour pouvoir faire de la publicité efficace, il faut la cibler. Pour pouvoir cibler, il faut surveiller les gens, il faut capter un maximum de données sur eux, car c'est ça qui permet ensuite de produire de l'attention qualifiée pour leurs clients qui sont les annonceurs. Si je regarde du côté d'Amazone, d'Apple et de Microsoft, on est dans un modèle qui est assez différent. Chaque fois qu'Apple vend un iPhone, il gagne un peu d'argent, donc ils n'ont pas fondamentalement besoin de ce modèle de captation de l'attention. C'est pareil pour Amazone et c'est pareil pour Microsoft qui ont eu un modèle économique de vente de la licence de logiciels qui normalement suffit à leur rentabilité. Chez eux l'attention vient dans un second temps, où ils ont compris l'intérêt pour les utilisateurs (et je dis bien utilisateurs et pas clients), d'avoir des services qui soient personnalisés. Et ils ont envie de proposer cette même personnalisation et pour cela ils essaient de capter un grand nombre de données. Mais aujourd'hui cette captation de données chez eux n'est pas à la racine dans la façon dont ils font de l'argent. Donc pour moi ce sont deux univers un petit peu différents. Finalement, ce qu'on pourrait leur reprocher aujourd'hui, c'est d'avoir centralisé cette captation de données. Parce que finalement aujourd'hui les GAFAM, que ce soit le cœur de leur modèle économique ou pas, c'est quand même eux qui captent la très très grande majorité des données produites par les utilisateurs. Et ensuite ces données peuvent être récupérées, notamment par les gouvernements, des annonceurs qui ne sont pas uniquement des annonceurs dans un but marketing. Typiquement, vous êtes un parti politique, vous avez envie de cibler très précisément les gens qu'il va falloir convaincre de voter pour vous. Donc cela a des conséquences sociales qui dépassent largement les conséquences de qui a un modèle économique qui repose sur la surveillance et de qui a un modèle économique qui repose sur la vente de matériel.

C'est très intéressant, car je n'avais jamais fait cette dichotomie entre Google, Facebook d'un côté et Amazone, Apple, Microsoft de l'autre. Néanmoins, tous concentrent beaucoup de

données personnelles en silos et cela est dangereux. Il ne se les partagent pas entre eux mais uniquement avec des publicitaires, c'est bien ça ?
Oui, alors il y a plusieurs choses dans ce que vous dites. La première est qu'effectivement pour l'utilisateur il y a ce problème d'avoir de la concentration de données chez chacun de ces acteurs, mais ce sont des acteurs qui n'interagissent pas, vous faites peut-être référence à Cozy Cloud. Et cela va contre l'intérêt de l'utilisateur parce que ces acteurs n'ont pas intérêt à coopérer. Finalement, on se retrouve à avoir des acteurs qui veulent chacun proposer le meilleur service, mais les données de Facebook pourraient enrichir les données de Google, qui pourraient enrichir les données d'Apple et c'est un terrain occupé aujourd'hui par les grands acteurs. Ensuite, il y a cet autre aspect, qui est celui de la centralisation. Le problème de la centralisation c'est qu'elle met une énorme barrière à l'entrée pour les nouveaux acteurs. Au sens où aujourd'hui, pour proposer un service aussi performent que celui de Google, il y a une énorme barrière à l'entrée qui est de réussir à capter autant de données que Google a réussi à capter en vivant à perte pendant des années. Parce que Google a mis 7 ans je crois à être rentable et à trouver un modèle économique viable. D'ailleurs c'est assez intéressant si vous regardez les papiers de recherche qui sont écrits par les fondateurs de Google, quand ils ont commencé à lancer l'idée et qu'ils cherchaient un modèle économique, ils se sont dit que le seul modèle économique viable serait celui qui repose sur l'économie de l'attention, où on capterait les données et on vendrait des profils à des annonceurs, mais ça c'est vraiment le pire qui pourrait arriver, et ça aurait des conséquences sociales désastreuses. Ça c'est leur papier de recherche en 2008 quoi.

Est-ce qu'on peut revenir sur Cozy Cloud dont vous m'avez parlé juste avant ?
Oui bien sûr, Cozy Cloud c'était l'entreprise pour laquelle j'ai écrit *Numérique : reprendre le contrôle*. J'y étais en 2016 et c'est là où j'ai commencé à travailler avec Tristan qui était lui aussi chez Cozy. Et Cozy, ce qu'ils voulaient faire à l'époque, parce que ça a un peu évolué, c'était de proposer un domicile numérique en se disant qu'un utilisateur produit pleins de données personnelles et ces données personnelles peuvent lui rendre service. En revanche, il les produit chez Google, chez Facebook, mais aussi chez son assureur, chez son énergéticien etc. et finalement est-ce qu'on n'aurait pas intérêt à avoir un lieu où toutes ces données pourraient être rapatriées, et lui ensuite pourrait décider de les recroiser comme bon lui semble pour pouvoir en tirer le meilleur en termes de valeur. Je ne vais pas vous cacher que ça n'a pas été un franc succès, ils ne sont pas en super position économique aujourd'hui, parce qu'effectivement c'est une idée super intéressante d'un point de vue économique, des usages, de la réappropriation de l'autonomie numérique. Mais aujourd'hui, manifestement, les utilisateurs ça ne les intéresse pas plus que ça. Après qui sait, si ça se trouve dans 2/3 ans c'est une idée qui va marcher à mort, ce n'est pas impossible, mais c'est vrai qu'aujourd'hui apparemment le niveau de maturité des utilisateurs n'est pas particulièrement intéressé par cette réappropriation.

Pouvez-vous me dire dans quel cadre avez-vous décidé de co-écrire ce livre ? Comment avez-vous fait pour vous lancer dans ce projet et quelles étaient vos motivations initiales ?
Pour approfondir un petit peu, à l'origine c'était surtout parce qu'on participait avec Tristan à l'Open Source Summit qui a lieu à Paris tous les ans, et lui était vice-président de la chaire

souveraineté numérique. C'était une année où l'Open Source Summit avait très envie de faire quelque chose de plus pérenne que simplement une conférence. Ils avaient envie de produire des livres blancs, de produire des projets etc., et du coup comme c'était un sujet qui m'intéressait et qu'en plus à l'origine j'ai une formation qui est littéraire, quand j'ai rencontré Tristan, on s'est dit que ce serait un super projet à avoir que d'écrire ce livre au nom de Cozy Cloud mais pour l'Open Source Summit. Pour moi cela a été une chance énorme car c'étaient des sujets que je connaissais on va dire de loin, c'étaient des sujets qui m'intéressaient et pour le coup ça m'a permis de rencontrer énormément d'acteurs qui non seulement ont des positions super intéressantes sur le sujet, mais qui ont des positions qui sont parfois contradictoires.

Comment avez-vous sélectionné les participants, les personnes que vous avez interrogées ?
C'était un peu un mélange au sens où il y avait certaines personnes, typiquement on a eu l'occasion d'interroger la présidente de la CNIL, franchement sur les données personnelles, ça ne se refuse pas. Donc on y allait sans forcément savoir quelle allait être sa position. Donc on n'a pas prévu dès le départ un enchainement de positions, qui nous permettrait d'avoir une vue globale de ce paysage-là. Je pense que ça s'est fait avec nos deux sensibilités, les personnes qu'on connaissait et qu'on trouvait pertinentes à interroger sur ces sujets. Moi typiquement je voulais à tout prix qu'on ait Damasio, parce que je trouve que, bien sûr que la partie régulation, la partie économique sont des parties qui sont super importantes, mais si on n'a pas quelqu'un pour nous rappeler le « pourquoi on fait tout ça ? », et des vraies raisons de modèle de société qu'on veut construire, ça aurait manqué. Donc on voulait parcourir un peu tous ces sujets du plus concret, donc qu'est-ce qui fonctionne aujourd'hui économiquement, qu'est-ce qui fait de l'argent, qu'est-ce qu'on vend ; au pourquoi est-ce qu'on fait tout cela, contre quoi on se bat, pourquoi est-ce que la souveraineté et l'autonomie numériques sont des sujets importants, et pour moi si on n'a pas un modèle de société derrière, qui n'est pas forcément celui de Damasio d'ailleurs, car bien qu'il soit très intéressant, on n'est pas obligé de partager l'ensemble de ses positions, mais voilà, la question du « pourquoi est-ce qu'on veut récupérer notre autonomie numérique ? », si c'est juste pour dire « bah les GAFAM c'est pas bien », franchement pour moi ça n'a aucun intérêt. Si on n'a pas de contre modèle de société ou au moins si on n'y réfléchit pas, et bien continuons à utiliser Google, ils nous rendent un super service.

Si je reviens à la concentration des données, globalement qu'est-ce qui dérange dans le fait que les données soient concentrées en silos ? Quels sont les risques pour les utilisateurs ?
Pour moi le risque principal, c'est que les données personnelles, ce n'est pas un objet comme les autres. Déjà ce n'est pas un objet, c'est l'émanation d'un sujet, ce sont les traces numériques d'une personne, et aujourd'hui le fait de les concentrer comme si c'étaient des objets, pour moi cela va à l'encontre même de ce que sont les données personnelles. Une donnée ce n'est pas simplement quelque chose qu'on produit, c'est quelque chose qui en dit très long sur nous, c'est quelque chose qu'on a mais qu'on est aussi, et que pour moi on ne peut pas vendre. Je trouve que la vision de « on peut vendre ses données personnelles » est complètement à côté de la plaque. Bien sûr que ça intéresse des gens d'acheter des données, mais ce n'est pas pour autant qu'elles ont vocation à être vendues ni qu'elles ont un statut qui leur permet d'être vendues. Il y a une autrice que je trouve

absolument incroyable et qui est très éclairante sur le sujet, c'est Antoinette Rouvroy, qui a écrit notamment un article qui est absolument passionnant sur le statut des données personnelles. Et du coup pour moi aujourd'hui, le principal problème que pose la centralisation, c'est qu'on se trouve dans une situation de dépendance par rapport à quelques acteurs qui nous imposent leurs conditions, qui nous imposent le type de relations qu'ils veulent avoir avec nous. Typiquement, la dernière fois que je cherchais un restaurant, Google Maps m'a proposé de calculer mon taux d'affinité avec ce restaurant. Moi je trouve ça super flippant. Qui est Google pour savoir mieux que ma famille, mieux que mes amis, mieux que moi-même si je vais avoir un degré d'affinité avec ce restaurant. Et pour moi la centralisation c'est pleins de problèmes dans un problème de base. Le problème de la centralisation c'est qu'elle donne énormément de pouvoir à un seul acteur. Ce n'est pas pour rien qu'on est en démocratie aujourd'hui, car il y a toujours des dérives quand on donne énormément de pouvoir à un seul acteur. C'est une règle du pouvoir. Après le problème de la centralisation se décline de pleins de manières. Économiquement, c'est un problème parce que ça donne du pouvoir à quelques acteurs, qui ne sera pas compensé par la possibilité d'émergence d'innovations. Aujourd'hui, chaque GAFAM a la possibilité de racheter l'intégralité des entreprises qui pourraient leur faire de l'ombre sur un secteur ou sur un autre. Et c'est ce qu'ils font d'ailleurs. Ils intègrent énormément ces entreprises. Et aujourd'hui c'est ce qui permet à Facebook de dire « oulala on a eu des scandales, mais heureusement, les gens migrent sur Instagram ». Instagram ça appartient à Facebook. Donc à partir du moment où les GAFAM possèdent la quasi-totalité des entreprises qui marchent et qu'ainsi ils sont en mesure d'imposer leur modèle et de racheter une innovation qui pourrait avoir choisie un autre modèle… C'est le cas de WhatsApp par exemple, le créateur à l'origine voulait uniquement de la communication chiffrée de bout en bout. Pour lui, la vie privée était une valeur cardinale. Ce qu'il a fait d'ailleurs en revendant WhatsApp c'est qu'il a investi dans la fondation Signal, qui est l'équivalent de WhatsApp chiffré qui n'appartient à personne. Donc finalement Facebook rachète WhatsApp, ils lui disent « oui bien sûr, on ne monétisera jamais les données, mais il va falloir trouver un modèle économique », ils le cherchent, ils ne trouvent pas, donc au bout d'un certain temps le fondateur s'en va, et Facebook aujourd'hui veut monétiser WhatsApp. Et il veut le monétiser à base des données qui sont échangées sur WhatsApp qui sont en lien avec les comptes Facebook. La centralisation pour moi c'est ça. C'est le fait qu'on ait tellement d'argent concentré au même endroit, tellement de pouvoir concentré au même endroit, qu'il n'y a pas d'alternative possible en fait.

Ce que vous décrivez ce ne serait pas la théorie de Shoshana Zuboff du capitalisme de surveillance ? De ce nouveau capitalisme du XXIème siècle qui repose sur les données personnelles ?

Oui oui oui clairement, de toute façon je pense que c'est assez incontournable comme position et de fait aujourd'hui on ne peut qu'être dans un capitalisme de surveillance parce que finalement la surveillance bénéficie à tout le monde, sauf aux principaux concernés qui sont les surveillés. Mais il y a un alignement qui est, je pense, assez inédit, entre des entreprises qui veulent surveiller pour vendre, des États qui veulent surveiller pour contrôler et des personnes qui ont toujours été habituées à évaluer la qualité d'un service, la pertinence d'utilisation d'un service à l'aune du rapport qualité prix, et à qui on propose aujourd'hui un prix totalement intangible, dont on croit

qu'il est nul, parce que finalement on ne débourse pas d'argent de la manière dont on est habitué pour obtenir un service et qui propose en même temps une qualité de service qui est exceptionnelle et qu'on paie en fait avec notre attention. Je souscris totalement à cette thèse, on est dans un capitalisme de surveillance, qui est en plus un capitalisme quasiment étatique et c'est ça qui est intéressant, car les entreprises ont finalement presque plus de pouvoir que les États mais finalement elles rendent service aux États qui ont juste à se servir ensuite quoi. Et ça pour moi c'est la deuxième partie de ce qui est problématique dans la centralisation. Moi je veux bien croire que Google ait les meilleures intentions du monde, mais à un moment Google n'est pas tout seul, Google est sur un territoire, il appartient au niveau légal à la législation d'un État qui sont les États-Unis, du coup quelle que soit la volonté de Google, s'il veut continuer à prospérer sans que l'État ne leur mette des bâtons dans les roues, ils ont intérêt à coopérer, et je ne dis pas collaborer mais coopérer, avec ces États. On peut toujours dire « ce n'est pas grave, on fait confiance à l'État », mais d'une part, l'arrivée au pouvoir de Trump a bien fait déchanter tous ceux qui avaient cette théorie, et d'autre part, un État ça bouge et une entreprise aussi. Ce n'est pas parce qu'on fait confiance à un instant T qu'on peut ensuite se dire que d'une part, la confiance pourra toujours rester la même, et d'autre part, que ce qu'on a déjà donné à l'entreprise ne pourra pas lui servir quand on ne lui fera plus confiance. Le RGPD a permis d'internationaliser les conséquences des décisions des utilisateurs et leurs droits, donc notamment le droit à la suppression. Mais enfin aujourd'hui, qui exerce son droit de suppression ? Moi je n'en connais pas. Et je pense pourtant que je fréquente des Ayatollah de la vie privée.

Est-ce que le RGPD ça change quelque chose alors ? Est-ce une solution ? Vous venez de dire que les GAFAM sont sur le territoire américain et son soumis à la législation américaine, qui est différente de la législation européenne, donc finalement ils font remonter toutes les données jusqu'à eux et se fichent de nos règles à nous. Est-ce que ce ne serait pas une sorte de colonialisme américain des données personnelles ?

Pour moi le RGPD est la moins mauvaise des solutions. Je pense que c'est essentiel de faire un travail de sensibilisation auprès des gens. C'est un travail qui est extrêmement long et assez peu fructueux, là cela fait quelques années que je l'observe et sans dire que les gens s'en fichent, parce que ce n'est pas vrai, ils ne s'en fichent pas, les gens ne sont pas bêtes, ils comprennent assez bien ce qui est en jeu, il suffit de leur expliquer un tout petit peu pour ceux qui ne sont pas familiers de ces domaines, mais globalement ils comprennent bien, ils n'ont pas l'impression de pouvoir en sortir parce que pour eux c'est très binaire, et c'est vrai que c'est très binaire, c'est aussi le souhait des GAFAM que ce soit très binaire, pour eux c'est soit ils sont obligés de renoncer à tout, et souvent ils ne peuvent pas renoncer à tout, et franchement, je ne vais pas les en blâmer. Donc pour moi la sensibilisation ce n'est pas la manière la plus fructueuse. Si je regarde Framasoft, leur nouvelle façon de faire aujourd'hui, ce n'est plus de se centrer sur les conférences dans un maximum de lieux, devant un maximum de publics qui ne sont pas avertis, c'est plutôt de s'intéresser aux acteurs qui sont déjà un peu désalignés par rapport à la société actuelle. Donc, ils vont aller voir des mouvements comme Alternativa, des mouvements écologistes, parce qu'ils savent que c'est un public qui sera facile à sensibiliser et surtout que c'est un public qui est prêt à faire des efforts pour être aligné avec ces convictions. Et ensuite, ce public va se charger d'essaimer

avec leurs mots, avec leurs façons de voir, avec leurs convictions politiques et leurs façons de porter le message et c'est une très bonne chose. Framasoft a un cœur de métier qui est assez numérique, mais finalement ce n'est pas toujours ça qui porte le mieux auprès de gens pour qui le numérique c'est juste un outil, ce ne sont pas forcément des valeurs, uniquement un outil, et cela permet de passer d'un point A à un point B, ça permet de mieux se diriger, de se faciliter la vie. Le passage à faire lorsqu'on sensibilise des gens pour qu'ils passent de l'immense confort que leur apportent les GAFAM à des solutions alternatives qui sont parfois un peu âpres, ou pas de solution du tout… Je suis bien placée pour en parler, moi je suis très sensibilisée à ces questions et pourtant j'ai encore un compte Gmail. Les cordonniers les plus mal chaussés c'est une réalité. Et du coup je me sens très très mal placée pour aller faire la morale et la leçon aux gens sur les scandales. Dans la grande majorité des cas, ils sont au courant. Juste fondamentalement ce n'est pas assez tangible pour eux, pour qu'ils aient vraiment envie de changer leur mode de fonctionnement. Donc pour moi, avoir une instance législative européenne, qui donne des règles et des amendes, c'est ce qu'on peut faire de plus efficace. Je ne dis pas que c'est une solution idéale parce qu'on voit que ça n'a pas toujours les conséquences qu'on veut, ça ne va pas forcément aussi vite que ce qu'on voudrait, mais n'empêche que fondamentalement, je préfère savoir qu'il y a des gens qui sont payés pour faire respecter nos droits, plutôt que de compter sur les gens pour faire respecter leurs droits, ils n'ont pas toujours l'espace mental pour le faire quoi.

Donc si je comprends bien, selon vous, la majorité des personnes est sensibilisée à ces questions, est consciente du fait que les GAFAM plus ou moins nous surveillent, nous tracent, nous traquent ?

Je pense que ce n'est pas aussi binaire que ça, au sens où je pense que la majorité des personnes se rendent compte qu'il y a un problème avec le numérique aujourd'hui. Mais après ça peut être pour des raisons assez différentes. Typiquement, il y a des gens qui ne sont pas du tout sensibilisés au principe de la captation de données et qu'ensuite ces données peuvent être utilisées par les gouvernements ou autres contre eux, mais qui vont dire « moi je me rends bien compte que je passe trop de temps sur Facebook ». Finalement, on en revient à un sujet commun, c'est-à-dire pourquoi est-ce qu'ils passent trop de temps sur Facebook ? Parce que Facebook repose sur une économie de l'attention. Pourquoi ça repose sur une économie de l'attention ? Pour capter des données. Cependant, je ne me fais pas d'illusions, si on demande à une personne lambda dans la rue si elle est sensibilisée aux questions de réappropriation des données numériques, d'autonomie numérique, de centralisation des données, la réponse dans la grande majorité des cas c'est non. En revanche, si on demande aux gens s'ils font confiance à Google, s'ils font confiance à Facebook, s'ils font confiance à Amazone etc., je pense, et d'ailleurs je ne me contente pas de le penser, il y a pas mal de sondages qui sont sortis là-dessus, je crois que c'est 80% des gens qui ne font pas confiance à ces grands acteurs. Et c'est tout le paradoxe, 80% des gens ne leur font pas confiance et pourtant 100% des gens utilisent leurs services.

Est-ce que vous pensez que les GAFAM nous surveillent ? Est-ce que le mot est bien employé ? Ou est-ce qu'ils nous tracent plutôt ? Est-ce qu'on doit faire une différence entre ces deux mots et lequel est le plus approprié ?

Ça dépend vraiment de comment est-ce qu'on définit les termes. Si dans surveillance on met le côté volontaire d'avoir quelqu'un derrière soi en permanence, je pense qu'effectivement le terme n'est pas bien choisi. Et je pense que la grosse distinction entre les deux, c'est que quand on surveille quelqu'un, l'important c'est l'objet de notre surveillance. On ne surveille pas dans l'absolu. On surveille toujours quelqu'un en particulier. Alors que pour Google, ce serait totalement indifférent si deux personnes échangeaient leurs téléphones. Fondamentalement, ça reviendrait exactement au même. Eux ce qu'ils veulent, ce sont des patterns de comportements, des comportements qui sont récurrents. Après, que ces comportements appartiennent à Madame Michu, Monsieur Michu etc. peu importe finalement. La seule chose qu'ils veulent, et c'est pour cela que je trouve que la lecture d'Antoinette Rouvroy est super intéressante de ce point de vue, car elle dit qu'il faut arrêter de parler de données personnelles parce que le combat ne se vit pas à un niveau personnel, le problème n'est pas personnel, le problème ce n'est pas moi, mes petites données, et ce que les méchants GAFAM en font, c'est un problème qui est social. Le problème c'est qu'aujourd'hui, en agrégeant les comportements, on peut pousser les gens à cliquer sur tel lien, à acheter telle chose, mais ce n'est pas en défendant mes petites données à moi que ça va changer. Donc pour elle l'enjeu est beaucoup plus global, au niveau social, et c'est pour ça qu'elle parle de traces, elle ne parle pas de surveillance. Elle ce qui l'inquiète c'est qu'on peut lire énormément de choses des traces qu'on laisse et les GAFAM ne s'en privent pas, et ils essaient de faire en sorte de pouvoir capter toutes ces traces. Après je pense que vous avez raison, le terme de surveillance n'est pas adéquat, c'est vrai qu'il est à côté de la plaque en fait. En revanche, ce que les GAFAM font, peut servir à nous surveiller. Ce n'est pas parce qu'eux ne le font pas qu'ils ne donnent pas les moyens à d'autres de le faire.

Et qui sont ces autres qui le font ?
Typiquement je pense que le gouvernement américain c'est un assez bon exemple, sans faire de théorie du complot, c'est une autorité publique qui demande des informations à Google quand ils ont des problèmes. Quand ils ont eu ce problème, est-ce que c'était après un acte terroriste je ne sais plus, il y a quelques années ils ont demandé à Apple de déverrouiller un iPhone de quelqu'un qui était le principal suspect dans une affaire de terrorisme. Pour le coup, le gouvernement ne s'en cache pas. Ce qu'on sait moins en revanche, c'est à quel point les GAFAM sont OK pour leur filer ces données. Je sors souvent ce chiffre dont il faudrait que je revérifier la source d'ailleurs, mais je crois que c'était le chiffre en 2014, quand Google a commencé à faire ses rapports de transparence sur le nombre de requêtes qu'il recevait de la part du gouvernement américain, Google répondait positivement dans 86% des cas. Mais vérifiez-le, ne le prenez pas pour argent comptant non plus.

Mais alors si le terme « surveillance » que l'on voit souvent dans ce cadre-là, ne serait plus approprié, cela voudrait dire qu'on ne peut pas dresser de parallèle avec les théories de Michel Foucault ? Je pensais notamment à la théorie du panoptique.
Pour moi la différence avec le panoptique de Foucault, c'est que la structure qu'imagine Foucault est déjà éminemment politique. On sait qu'on veut que les gens n'aient pas certains comportements dans le panoptique. Le fait qu'ils se sentent surveillés, cela les pousse à, à moindres coûts, faire en sorte qu'ils n'aient pas ces comportements, parce qu'on ne sait jamais si on peut être surveillé ou

pas. En revanche, dans le cadre des GAFAM, c'est plutôt l'inverse. Je ne sais pas si vous vous souvenez, dans l'interview de Damasio, à un moment il parle de la très grande liberté putative des GAFAM, où les GAFAM ne veulent pas finalement nous empêcher de faire quoique ce soit. Ils ne veulent surtout pas qu'on se censure, ce qui les intéresse c'est au contraire qu'on ait un maximum de liberté dans les choses qu'on a envie de chercher, parce que finalement ça leur permet de cerner plus finement nos centres d'intérêt et ensuite de vendre plus cher notre profil. Donc pour moi c'est finalement la limite de cette comparaison, c'est que le panoptique est quand même fait pour avoir un effet dissuasif. Les GAFAM pas du tout. Et finalement ce qui est marrant, ce que j'observe très souvent, c'est que le moment où les gens commencent à avoir peur quand on leur parle de surveillance, c'est le moment où Google va montrer qu'il surveille. Par exemple, il y a quelques semaines, les gens se sont rendus compte que si on va sur Google.com/purchases on trouve une liste de tous les achats qu'on a fait sur internet ces dernières années. Pourquoi on les a ? Tous simplement, parce que lorsqu'on achète quelque chose sur internet, on reçoit un mail, et ce mail, c'est un mail contenant ce qu'on a acheté et ensuite il le liste. Google le faisait déjà avant, il l'a toujours fait. La seule chose qui a changé, c'est que maintenant il en a fait une liste. En général, ce qui blesse les gens, c'est de lire leur historique, de regarder leurs déplacements, de voir que Google a effectivement une liste de tout ce qu'ils ont acheté. Mais fondamentalement, je pense que Google ne fait pas ça pour les faire flipper. Google fait plutôt ça pour leur rendre service. Ce qui fait peur aux gens c'est de voir qu'on les trace, mais finalement être tracé ils s'en fichent tant qu'ils ne s'en rendent pas compte. Moi finalement c'est ce que j'obtiens et j'ai du mal à l'expliquer d'ailleurs, c'est qu'il y a une espèce d'angoisse générale à chaque fois qu'il y a quelque chose comme ça qui sort, mais à chaque fois j'ai envie de dire « mais attendez, ce qui vous angoisse c'est juste qu'on vous le mette sous les yeux, mais vous vous en fichiez tant que vous ne l'aviez pas sous les yeux ». Et c'est pareil, par exemple les gens ont confiance en leur banque et ils lui confient de l'argent. On aurait envie de dire « si vous avez confiance en votre banque pour lui confier votre argent, confiez-leur vos données personnelles, parce que finalement ce sont des acteurs de confiance, parce qu'ils n'ont pas d'intérêt économique à les révéler, contrairement à Google qui a un intérêt à vendre votre profil ». Mais finalement pour les gens, Google c'est très lointain pour eux, alors que la banque c'est un endroit où ils vont régulièrement, ils ont leur conseiller bancaire, et donc plus on rapproche ça d'eux, et plus on leur dit « non mais donnez vos données à quelqu'un en qui vous avez confiance », moins ils ont envie de le faire, parce que là d'un coup ils se rendent compte de la valeur de ce qu'ils mettent entre les mains de quelqu'un d'autre. Tant que c'est Google, c'est totalement désincarné. C'est pour ça que j'ai été très très foucaldienne à un moment sur cette question, je le suis un peu moins aujourd'hui. Parce que finalement l'intérêt de Google aujourd'hui c'est de montrer le moins possible qu'il nous surveille tandis que le panoptique est censé montrer à moindre coût que tout le monde est sous surveillance.

Et concernant le biopouvoir, une gestion algorithmique de la vie des individus via les GAFAM, serait-ce adéquat ?

Ça je pense que c'est beaucoup plus adéquat et beaucoup plus intéressant. Moi c'est plus sur le panoptique que j'ai des réserves. Ce que j'aime bien chez Foucault c'est qu'il y a une désincarnation du pouvoir, le pouvoir est dans les structures, on n'a pas besoin d'un grand méchant

pour qu'il y ait du pouvoir. Et je trouve que c'est très vrai aujourd'hui, et finalement on a un encouragement des gens à adopter le comportement qui correspond à leur profil. Peu importe qu'est ce comportement, Google se fiche de vous vendre des chaussures rouges ou des chaussures bleues, la seule chose qu'il veut, c'est faire en sorte que vous ayez un comportement d'achat qui soit cohérent avec le profil qu'il a dressé de vous. Pour moi il est là le pouvoir, il est éminemment économique. La question du pouvoir politique, c'est une question sur laquelle je me suis moins penchée donc je suis moins dans la réflexion et plus dans l'improvisation, mais évidemment aujourd'hui on voit avec Facebook qu'il y a des incitations à des comportements politiques aussi, qui sont peut-être beaucoup plus proche de Foucault. Mais je suis moins à l'aise pour parler de ça.

Et le lien entre savoir et pouvoir ? Les GAFAM entassent tellement de connaissances sur nous que finalement l'utilisateur devient un objet de savoir grâce au profilage notamment, on va un peu « conduire les conduites » des individus et les manipuler ?
Je suis tout à fait d'accord mais je trouve qu'il y a quand même une question qui est importante à soulever si on part dans ce sens-là, c'est que d'accord l'utilisateur est l'objet de savoir, mais alors qui est le sujet du savoir ? Est-ce qu'il y a un sujet du savoir ? Disons que c'est assez clair, quand on veut conduire les conduites, la prisons veut conduire les conduites d'une certaine manière, l'hôpital veut conduire les conduites d'une certaine manière, là ce que je trouve assez fascinant avec la montée en puissance des GAFAM c'est qu'on ne sait pas exactement à quelle conduite on veut arriver. Il n'y a pas vraiment de discipline, pas vraiment d'objectif dans tout ça. C'est plutôt on laisse les conduites se conduire et on essaie d'en tirer une valeur économique.

Et le profilage dans tout ça ? Est-ce que ce ne serait pas une sorte de conduite type ? Grâce au profilage on prédit les conduites et l'assemblage donnerait un ensemble de comportements type à avoir.
Oui mais c'est une conduite sans normes. Pour moi elle est là la distinction. C'est une conduite qui est normée par rien d'autre que la conduite des autres. A la fois c'est extrêmement dangereux car ça pousse à un conformisme très fort, et en même temps, l'acteur qui met en place le profilage, ne cherche pas à arriver à une norme, il n'essaie pas d'induire une norme. La norme c'est l'autre.

Comment est-ce que les GAFAM traitent les données personnelles ? Comment distinguent-ils les données pertinentes des non pertinentes ?
Je ne travaille pas chez eux donc ce n'est qu'une opinion, mais je pense qu'il y a plusieurs niveaux. Je pense que ce n'est pas le même type d'analyse en fonction de qui on est. Typiquement, si vous recherchez un restaurant sur Google Maps, si vous n'êtes connectés à rien d'autres, que c'est un ordinateur qui n'a pas de compte Google configuré, vous aurez déjà un premier ciblage en fonction de la ville depuis laquelle vous vous connectez, l'endroit dans cette ville, le terminal depuis lequel vous vous connectez, qui va déjà donner des informations sur vous. C'est l'aspect contextuel de la recherche qui est un moindre mal. Après je pense qu'on surestime les capacités de profilage et d'analyse de Google et même des GAFAM. Aujourd'hui si j'achète des chaussures, j'ai des pubs de chaussures pendant deux semaines mais ce n'est pas si impressionnant que ça. Ça peut le devenir et être très impressionnant et surtout, il peut y avoir des conséquences beaucoup plus graves.

Typiquement, Google stocke tous mes mails pour me vendre des chaussures, mais moi je n'ai pas envie qu'on analyse tous mes mails pour savoir si on va me proposer des chaussures rouges ou des chaussures bleues. Pour moi il y a une disproportion énorme aujourd'hui entre les données collectées et l'efficacité du dispositif de monétisation de ces données qui est mis en place. Après, comment ces données sont-elles analysées, je trouve que ce qui est plus intéressant c'est de voir quels services ils arrivent à obtenir en les agrégeant. Il n'y a pas mieux que Waze et Google Maps pour savoir si on va être en retard tout simplement parce que tout le monde fournit ses données à ces acteurs en temps réel. Pour des cas comme ça, je ne vois effectivement pas l'utilité de collecter la localisation de tous ces acteurs, mais on voit bien l'intérêt à ce moment-là de les analyser de manière globale.

Puisque, comme vous dites, les individus sont sensibilisés à ces questions, qu'est-ce qui justifie le fait qu'ils continuent à utiliser les GAFAM ? Est-ce parce qu'ils n'ont pas d'autre choix ou est-ce une forme d'irresponsabilité ?

Pour moi on fait peser sur eux des questions qu'on ne devrait pas faire peser sur eux. Typiquement, il y a un code de la route, qui fait que les gens n'ont pas à se préoccuper de déterminer la bonne vitesse quand ils conduisent. Ils savent qu'il y a une vitesse maximale. Il y a des règles qui font que lorsqu'on nous octroie un prêt bancaire, on doit attendre 11 jours avant de le renvoyer signé. Les gens agissent à l'impulsion et c'est normal, c'est un fonctionnement de base, qu'on a quand on est une personne et que ce n'est pas notre métier, notre spécialité etc. Je pense qu'aujourd'hui on est dans un univers peu régulé et moi je n'ai pas vraiment de reproches à faire aux personnes qui utilisent tous ces services. Elles répondent à leur pulsion d'un instant A, leur confort à un instant B. Je n'ai pas trop envie de parler d'irresponsabilité en fait et peut-être que j'ai beaucoup tendance à dédouaner les utilisateurs de ces services, mais ça ne me parait pas adéquat de faire peser sur eux la charge d'utiliser des sociétés qui ont une bonne gouvernance des données personnelles. Après, il y a l'aspect aussi que les alternatives ne sont pas légion, elles sont très largement en dessous des services qui sont fournis, et pour moi le fait de les utiliser c'est presque entièrement un acte de militantisme, et on ne peut pas demander à tous les gens d'être militants. C'est pour ça que je crois beaucoup plus, malgré les défauts du RGPD, à l'encadrement des pratiques par la loi, qu'au fait de faire peser sur les utilisateurs la charge de changer l'intégralité de leurs comportements. On peut faire de la sensibilisation, mais comment est-ce qu'on combat le mieux l'obésité des enfants ? Et bien en changeant les menus à la cantine, pas en disant aux gens « olala vous leur faites trop de produits sucrés ».

Donc le RGPD et le droit à la portabilité peuvent être des solutions ?

Pour moi la portabilité au niveau des individus n'a aucun intérêt. Je pense que ce qui changerait vraiment les choses, c'est si un jour on réussit à trouver des acteurs avec un modèle économique plus viable qu'est celui de la gratuité, d'un coup ils n'auront pas à construire toute la base de données et ils pourront importer les données existantes. Ça, ça peut vraiment changer les choses, et notamment en termes de compétition.

En revanche, est-ce que cela vous ennuie si on termine l'entretien plus tard car il va vraiment falloir que je file ?

Oui bien sûr, merci beaucoup !

Interview n°2

Tu as remis en question ma vision des relations entre les GAFAM et les théories de Foucault. Vois-tu plus de parallèles avec les théories de Deleuze ?

Je connais moins que Foucault donc c'est plus difficile de répondre. Pour moi, l'aspect d'autocontrôle est primordial. La quantification, la mesure, les petits contrôles de notre quotidien. Aujourd'hui, il est clair que c'est le pouvoir sans la norme : c'est le contrôle personnel sur une version améliorée de soi, on est dans l'optimisation permanente. Je suis totalement d'accord avec le concept de friction de Damasio, qui correspond à un moment de liberté où tu n'as pas ton smartphone pour faire le lien avec le monde, de manière autocentrée. Le smartphone est un monde sans friction. Le « collier électronique » de Deleuze cache une composante fondamentale du rapport à la technologie, à savoir qu'on le choisit. Il nous apporte beaucoup de confort dans la vie, mais tous les côtés négatifs … attends j'allais dire un truc avec lequel je ne suis pas d'accord... Le côté négatif, les externalités négatives : tu es localisé en permanence mais c'est pratique. Bon, pourrait-on imaginer une solution libre dont les données ne seraient pas diffusées ? Pour moi, non, car c'est un comportement qui me gêne. En effet, il y a une différence entre le pouvoir (ex : un GPS qui t'amène d'un point A et un point B sans avoir à réfléchir) et la puissance (capacité à s'orienter, et donc à refaire le chemin une 2ème fois sans GPS) chez Damasio, qu'il a lui-même pris de Spinoza : il est totalement opérant ici. Selon moi, il ne faut voir le monde de manière binaire pour ou contre les technologies : j'ai des amis qui sont puissants avec leur smartphone parce qu'ils l'utilisent à bon escient, pour améliorer leur travail dans le monde réel sans balancer trop de données. A l'inverse, moi je sais que j'ai du pouvoir avec mon smartphone, mais je n'en retire pas de puissance : Damasio, par exemple il n'a pas de téléphone, il n'a pas d'agenda, seul le fait de se rappeler d'un événement signifie qu'il valait la peine de s'en souvenir. Moi je note tous mes RDV, mais je n'ai pas la sensation de faire ça parce que ça me rend la vie plus facile : c'est juste parce que j'ai envie d'y aller, donc je ne veux pas oublier.

Tu dis que ce sont des outils qui nous rendent la vie plus facile, donc le mot « prison à ciel ouvert » serait trop violent ?

J'ai beaucoup adhéré à ces thèses, j'essaie de me rappeler pourquoi. Je pense que tu peux devenir assez prisonnier de toi-même. La dimension politique de l'outil mise de côté, j'ai réussi à avoir un rapport plus sain avec les nouvelles technologies. De quelle prison parle-t-on ? Si c'est prisonnier de ton propre confort je suis totalement d'accord. (…) Mais c'est compliqué (…) : si quelqu'un en qui j'ai confiance faisait la même chose, est-ce que je me sentirais aussi bien ? Mozilla voulait faire un smartphone qui ne te trace pas, qui ne te rende que des services. Apple le fait aussi : les seules infos qu'ils te prennent c'est pour te rendre la vie plus facile, et c'est chiffré. Fondamentalement y'a toujours un problème car je n'aime pas le « geek humain » que ça fait de nous. La prison à ciel ouvert c'est que quelqu'un veut te rendre prisonnier ; mais prisonnier de quoi ? Je ne sais pas…

Il dit que « la société disciplinaire vise à contrôler nos âmes » : est-ce excessif ? est-ce transposable aux GAFAM sachant qu'ils ont accès à notre intimité ?

Il y a en effet un lien car ça leur donne un « terrain de jeux ». Facebook avait fait scandale il y a quelques années parce qu'ils avaient fait une expérience pour voir s'ils pouvaient pousser les gens à voter. Ils avaient affiché comme contenu positif aux gens associé à l'idée du vote, et les gens étaient effectivement allés plus voter. Là où je trouve que « contrôler nos âmes » est excessif, c'est parce que le contrôle signifie toujours que tu veux faire ou pas faire des choses aux gens. Or, on a surestimé le côté « grands méchants » des GAFAM, dans la mesure où ils n'ont pas d'objectifs : ils sont d'ailleurs très a-politiques. Cependant il faut toujours envisager le pire : je n'ai pas envie qu'il y ait des armes de « massification de l'information » et de l'influence que tu peux avoir sur les gens (termes excessifs). Mais clairement, ce n'est pas la grande conspiration des GAFAM qu'on pourrait attendre. Cela dit, c'est un principe de précaution à avoir : on peut créer des instruments tellement puissants… En fait tu n'en sais rien : quand Sundar Pichai dit qu'il veut le bien de l'humanité, je veux bien, d'accord mais Google reste une entreprise quoi, et une entreprise ce n'est pas démocratique. A un moment, tu ne peux que compter sur le fait que ça ira dans ton sens. C'est ça le vrai risque. Avoir un très beau collier électronique c'est super mais le jour où quelqu'un veut mettre en place un projet politique de contrôle du collier, et bien je n'ai pas de pouvoir pour m'en débarrasser. On revient toujours au problème de la centralisation des données ; si un GAFAM veut contrôler mon âme il peut le faire très facilement.

Parlons un peu de la souveraineté des données : pourrait-on dire que les individus sont irresponsables ou négligents sur l'utilisation qui est faite de leurs données ?

C'est tout l'enjeu du *privacy paradox*. Pourquoi, alors que tout le monde sait qu'il ne faudrait pas fournir toutes ces informations en ligne, pourquoi est-ce qu'ils continuent à le faire ? Il y a les théories cognitives qui mettent en avant le sentiment d'addiction que produit Facebook par exemple sur le circuit de récompense du cerveau. Pour moi il y a surtout une dilution de la part de responsabilité. C'est comme quand tu votes : plus tu votes à contre-courant des gens et moins il y a de risques que tu le fasses parce que tu vas sur la pente la plus « paresseuse ». Cette paresse est renforcée par l'accumulation de côtés négatifs : si tu sais que tu ne tries pas tes déchets alors que ça a un impact sur l'écologie, tu peux te dire que « c'est vraiment de la paresse » : alors qu'avec les nouvelles technologies, tu te prives de récompense, de relations avec les autres, tu perds du temps… et il n'y a pas vraiment de monde désirable dans l'autre sens. En effet, on voit un monde dystopique dans les GAFAM : mais franchement, à part Damasio, personne ne présente un futur alternatif désirable. Personne ne dit à quel point c'est génial de plus avoir de smartphone. Mais l'humain réagit plus à la récompense qu'à une peur lointaine et diffuse de potentiels problèmes qui pourraient arriver. Ce mélange fait que rien ne te pousse à faire autrement, si tant est qu'il y a quelque chose d'intéressant à faire autrement. Mais c'est en train de changer : j'ai fait une table ronde à MiXit à Lyon sur les alternatives éthiques aux outils numériques. Notamment, un élément que je trouvais intéressant est le suivant. : on n'a jamais trouvé une définition commune de l'alternative éthique. Surtout, il ressort que c'est difficile de faire émerger une vision positive d'une alternative éthique. Il y a 20 ans, « manger bio » n'était pas sexy ; aujourd'hui ça signifie prendre

soin de son corps, de la nature, etc… Peut-être que dans 10 ans la nouvelle boboïtude sera de dire « je vis sans smartphone, sans Google ». Ça commence un peu : les centres de vacances numériques, les centres de désintoxication numérique… Mais ça commence à être glamour d'avoir une vision éthique du numérique.

Tu parles de l'importance de l'autonomie dans ton livre : comment tu imagines le faire ? Les utilisateurs ne voient pas forcément l'intérêt de se réapproprier leurs données.
La portabilité peut aider : les entreprises allaient s'en emparer. Mais je déchante un peu. En effet dans mon travail d'accompagnement à la mise en conformité de la RGPD, les entreprises en sont toujours à lister les données qu'elles récupèrent… La portabilité n'existe pas encore dans la tête des gens, il est peut-être trop tôt. Mais il y a une question : avant de contrôler ces données, c'est d'être capable de les confier à qui tu préfères. Typiquement, la portabilité peut me permettre de changer de tel logiciel à tel autre en un clin d'œil : mais je continue tout de même à donner mes data, et je n'en ai toujours pas le contrôle. Le contrôle est un terme vraiment polysémique. Oui, les alternatives libres restent des alternatives éthiques au sens fort : mais celles d'aujourd'hui ne font que proposer mieux que la concurrence, mais elles ne fonctionnent pas à l'idéologie. Par exemple, ce qui a fait bouger les gens de Twitter et Youtube à Mastodonte et PeerTube, c'est simplement parce que ce sont des systèmes d'instance avec des règles claires : si tu parles dans mon groupe, c'est parce que tu acceptes mes règles. Mastodonte et PeerTube fonctionnent parce que l'on se dit « ce n'est pas plus sécurisé, mais ça correspond à ce que je recherche sur un réseau social ». Là où Youtube refuse toute la monétisation des vidéos sexuelles, je peux décider l'inverse sur mon instance PeerTube. Pour moi, il y a toujours un tiers de confiance à un moment : soit tu dis que le tiers de confiance c'est toi, soit tu es en capacité de le choisir, et c'est ce dernier qui est le plus simple, mais pas le plus sécurisant pour un individu.

L'argument du « rien à cacher » revient systématiquement lorsque l'on parle de détention de données par les acteurs du numérique. Lors de tes recherches, tu as été confrontée à cela : comment l'expliquer ?
Pourquoi les gens pensent qu'ils n'ont rien à cacher ? Ils ne le voient qu'à l'échelle individuelle dans la situation actuelle : d'ailleurs, je pense que leur choix de n'avoir rien n'a cacher et d'accepter des modèles économiques basés sur la captation de données, ce sont des choix que les gens aimeraient ne pas faire. Ce n'est pas parce que le « blond blanc hétéro cisgenre » se dit qu'il n'a rien à cacher que les minorités ne se le disent pas, comme les homos par exemple. La deuxième explication, c'est qu'il y a une question de confort. Si tu commences à réfléchir aux alternatives qu'il faudrait avoir si tu avais des choses à cacher, d'un coup c'est trop : « c'est compliqué donc je n'ai rien à cacher ». Alors comment déconstruire ? 1. Tu peux leur dire « donnes moi tes mots de passe de comptes en ligne » : mais alors tu te rends compte que les gens n'ont rien à cacher à des gens qu'ils ne connaissent pas. 2. Tu peux leur demander « est-ce que tu as des rideaux à tes fenêtres ? est-ce que tu fermes la porte quand tu vas aux toilettes ?», pour moi c'est un bon argument car il souligne la distinction public/privé. 3. Le troisième argument est de dire que tu ne peux pas construire une société saine à partir du moment où tout le monde voit tout ce qu'il se passe. Ex : si tu apprends à chanter, et que tout le monde te regarde, tu aurais honte et surtout jamais

personne ne voudrait ensuite t'écouter au vu de tes cours. Ce qui est révélateur, c'est que lorsque j'installe la messagerie chiffrée Signal à mes amis, la première chose qu'ils font est de blaguer sur le terrorisme, comme s'ils ne pouvaient pas le faire sur des réseaux traditionnels. Il y a une fonction de catharsis dans le fait qu'il y ait des endroits secrets dans le numérique, où tu n'es pas regardé. Donc ils te répondent au début « j'ai peur de rien quant à mes données sur twitter » mais quand ils sont sur Signal, ils écrivent des choses qu'ils n'auraient jamais écrites auparavant. L'expérience consistait à demander aux gens, sur une page avec un logo de la NSA, dans quelle mesure ce logo les influençait. En comparant ces résultats, on remarquait que les gens qui disaient qu'ils ne changeaient pas de comportement quand ils étaient surveillés, avaient une plus grande propension à le changer. Il y a donc cette notion d'invisibilité de la surveillance. Et effectivement, Fabrice Rochelandet parle de *privacy by using* d'indicateurs pour rendre visible ton comportement et les données qui transitent. C'est pas mal ; quand tu le vois, ça permet de réaliser ce qui est en train de se passer et de ne pas l'oublier. Tu peux ajouter un plug-in sur internet qui te dit quand tu envoies des données : mais qui a envie de s'auto-infliger cela ? Une grande majorité de nos interactions sociales se sont construites autour de ces outils.

Y a-t-il encore des gens qui se croient anonymes en ligne ?
Je pense vraiment que personne ne s'imagine être anonyme en ligne, au vu de tous mes entretiens passés. 80% des gens se disent inquiets de leurs données personnelles ; ils savent donc globalement que leur utilisation n'est pas vertueuse. Mais, mêmes les comportements vertueux ne proviennent pas d'un bon sens, mais de l'évitement d'un désagrément : quand les individus installent des ad-blockers sur internet par exemple, c'est moins pour le traçage des données que pour le caractère intempestif des publicités. Comment rendre concret un désagrément de donner du data ? Peut-être que plutôt culpabiliser les gens sur le volume de données transmises, peut-être imaginer une lumière verte sur ton navigateur dès que tu n'es plus pisté en ligne, ça pourrait marcher. Il faut stopper la dystopie et mettre en avant l'aspect positif des outils alternatifs. Deuxième exemple ; mes connaissances qui ont supprimé Facebook ne l'ont pas fait pour leurs données, mais pour leur bien-être, car elles en avaient marre d'être sollicitées tout le temps.

As-tu d'autres idées sur l'avenir de la surveillance ?
De manière générale je ne suis pas très optimiste sur le repentir qui se réveille et qui dit « on en a marre d'être listés, on arrête les GAFAM ». Je prévois plutôt une adaptation des plateformes, qui vont proposer de plus en plus de solutions pour protéger la vie privée, car elles vont faire l'objet d'un *privacy washing*. Ça va être un futur élément de différenciation : quelle plateforme va proposer le plus de sécurité pour les données ? Le truc c'est que le prochain combat va être de faire prendre conscience aux gens que ce sont les méta données le problème, pas vraiment les données personnelles. Typiquement, Facebook peut dire, sans lire tes conversations, si tu sors avec la personne ou pas d'après le rythme de conversation : fréquence, durée, heures de connexion… Le problème de la surveillance sera déplacé des données au métadonnées, mais ce sera plus compliqué de faire prendre conscience aux individus.

Merci beaucoup !

Appendix 6 – Interview Transcript #4

Interviewer: Zuzanna Sonenberg
Interviewee: Jérémy AROLES, Assistant Professor in Organization Studies in the Business School of Durham University
Interview Setting: Interview conducted via Skype on June 26th, 2019, at 11:00 am CET, with the support of Apple MacBook recorder.

(Start of Interview)
(Presentation of the interviewer and the research topic, see Appendix 1 – Interview guide)

Pouvez-vous me parler un peu de vous ?
En ce qui concerne votre sujet, j'ai travaillé sur les théories de G. Deleuze au cours de mon doctorat. Aujourd'hui, je travaille surtout sur les nouvelles formes de travail et leur développement éthique.

Qu'est-ce que la surveillance des GAFAM vous évoque-t-elle ?
Je peux vous poser une question ? Vous pensez contacter ces entreprises ou vous vous focalisez plutôt sur le ressenti des individus face à ces intrusions ?

C'est un mémoire de fin d'étude de M2. M. de Vaujany m'a conseillé de faire une méthodologie de recherche : entretiens avec des spécialistes, puis faire un questionnaire à destination des gens « lambdas » pour récolter leurs usages, leur degré de sensibilisation…
C'est très intéressant. Je pense qu'en termes de variables importantes vous aurez l'âge et l'aspect générationnel. En travaillant à Manchester, j'enseignais « Globolization and the Digital Divide » : il y avait des sessions sur la *privacy*, les GAFAM, et en fait un très grand nombre d'étudiants ne semblaient pas intéressés par ces problématiques. Et un grand nombre répétait le slogan des services américains « If you got nothing to hide, so you should not be worried ». Pour en revenir à vos questions, la difficulté majeure face au monopole des GAFAM est le manque d'alternatives. Pour Deleuze, si on veut progresser dans le monde il faut une fenêtre de possibilités ; à partir du moment où vous la perdez, vous basculez dans le totalitarisme. Regardez *L'abécédère* de Deleuze, ce sera positif.

Peut-on parler de surveillance ? Ou peut-on parler de traçage ?
Ça renvoie à la dimension performative du langage. L'emploi des mots est important : quelles différences faites-vous ?

Je me suis aperçu après plusieurs entretiens que les gens faisaient la différence entre ces mots. La surveillance serait active tandis que le traçage serait passif.
Effectivement, la différence est en termes d'intention : suivre pas à pas la personne ou seulement avoir accès à un ensemble de données qui peuvent être mobilisée dans un contexte particulier. L'idée de tracer est plus insidieuse, une forme de contrôle beaucoup plus latente, plus invisible. La surveillance pourrait être visible, même si elle ne l'est pas forcément.

Deleuze s'inscrit plus ou moins dans le prolongement de Foucault, en passant d'une société disciplinaire à une société de contrôle. Comment est-ce que vous verriez la transposition de ces termes dans le cas des GAFAM ?
Connaissez-vous l'image du nomade développée par Deleuze et Guattari ? Il y a deux formes d'espaces ; striés (entièrement contrôlés, comme la ville) et lisses (moins sujets au contrôle capitaliste, comme l'océan). Le nomade habite ces espaces lisses qui échappe au contrôle du capitalisme, et il en a besoin pour vivre. Il y a un contraste entre la figure du nomade et le capitalisme (ou l'État en général) : ces différentes technologies qui sous-tendent le développement du contrôle ont permis une certaine forme d'émancipation. A travers les technologies, il est possible de conquérir de nouveaux espaces lisses. Mais le processus intéressant est qu'au fur et à mesure, les technologies ont été « incorporated » par l'État à travers différentes mesures de contrôle.
Donc pour essayer de revenir à votre question, si vous regardez le parallèle entre la figure du nomade et l'État, cela vous permet de dresser un bilan intéressant de l'évolution des développements technologiques et le rôle que ces derniers ont joué dans les systèmes de surveillance : en passant d'un rôle plus émancipatoire à une dimension de contrôle.

Dans cette figure il faut toujours qu'il y ait l'État ?
Oui, car le nomade est une figure dialogique. Il y a une opposition entre les deux espaces, et lui est toujours opposé à la figure de l'État : il essaye de « push the boundaries », alors que l'État a comme processus d'imposer graduellement une forme de contrôle. Le nomade ne peut exister sans l'État en quelque sorte.

Est-ce applicable tel quel dans mon cas ? Finalement, n'est-ce pas les GAFAM qui détiennent le contrôle ?
On peut voir l'opposition nomade/État comme une opposition nomade/capitalisme. L'État peut être remplacé par les grandes entreprises en général.

Donc le nomade peut-il être remplacé par le citoyen d'aujourd'hui ?
Oui tout à fait.

Deleuze développe le concept de collier électronique dans son *Post Scriptum sur les sociétés de contrôle*. Est-ce que vous voyez un lien avec les GAFAM ?
Il y aurait de quoi faire un parallèle. En Chine, ils font de la reconnaissance faciale : on peut y voir un parallèle car en tant que citoyen vous êtes notés positivement, négativement, avec des conséquences. Là, c'est un collier électronique qui pose une forme de contrôle beaucoup plus

individualisante, où l'on peut concrètement restreindre le mouvement de personnes. Mais si l'État chinois peut faire ça c'est par l'appui des grandes entreprises technologiques.

Donc vous reliez le concept de contrôle à celui de l'État. Les GAFAM ou les sociétés ne seraient que des intermédiaires ?
Pas forcément des intermédiaires. Je pense qu'ils ont beaucoup d'intérêts en commun. Il y a beaucoup d'accord bilatéraux en termes de législation, d'accès au marché, etc… Ce seraient des collaborateurs plutôt.

Dans mon sujet sur la surveillance de masse opérée par les GAFAM, dois-je intégrer l'aspect étatique ?
Pas nécessairement. Vous pouvez avoir 2/3 paragraphes de problématisation entre ces géants de l'internet et l'État. Mais ne vous embarquez pas sur ces thèmes en particulier.

Les GAFAM détiennent-ils un pouvoir ? Est-il disciplinaire ? Serait-ce une prison à ciel ouvert ?
Prison à ciel ouvert…c'est pas mal ça ! S'il y a un pouvoir… tout dépend de la valeur que l'on accorde aux données. La notion de contrôle est beaucoup plus difficile à aborder : si vous êtes un citoyen lambda, ces organisations n'exercent aucune forme de contrôle dans tous les cas, puisqu'elles n'auraient pas à leur disposition des données qui puissent être utilisées contre vous. Je ne sais pas si je réponds vraiment à votre question en fait.

Justement, vous parlez de définition du contrôle : laquelle serait-ce pour Deleuze ?
Je ne pourrai pas vous répondre. Deleuze a un peu tendance à inventer ses concepts et à les rendre fluctuants. Dans le cadre de votre projet, vous voyez le contrôle d'une perspective plus autoritaire/légale ? Ou en termes de *behavior* ? Pour moi ce sont deux niveaux différents. Je ne connais pas la définition précise du contrôle que Deleuze fait… on y reviendra à la fin de l'entretien si ça ne vous dérange pas.

Entendu. A votre avis les gens s'asservissent volontairement aux GAFAM, malgré les affaires récentes ?
Il y a bien une conscience que quelque chose ne va pas, mais pas une conscience concernant les implications. Il y a certainement un manque d'éducation concernant les conséquences directes. Encore une fois, il y a une forte dimension générationnelle : auparavant, les gens faisaient très attention à leur « privacy », « confidentiality » et ce que ça voulait dire vraiment. Si vous prenez une génération plus récente, c'est un concept qui va avoir une dimension différente. Clairement, il y a une évolution de définition de ces concepts.

Selon vous, comment s'organise ce contrôle derrière les nouveaux outils électroniques ? Comment les GAFAM nous contrôlent-ils ?
Je pense que c'est difficile à conceptualiser. Pour vous donner une anecdote, j'étais dans le RER, et il y avait deux femmes qui essayaient de réserver un billet de train. Les deux trouvaient deux

tarifs différents, pour la même recherche. Et elles ont commencé à parler de l'injustice liée aux algorithmes, mais ce qui me frappait, c'est qu'elles utilisaient l'article « it » or « they » pour parler de quelque chose qu'on ne peut pas vraiment nommer, quelque chose d'abstrait qui contrôlerait les attitudes dans le réel. On en revient à quelque chose d'invisible, quelque chose qui est très embedded dans l'environnement technologique, de sorte qu'il soit très difficile de distinguer les processus qui sous-tendent à cette situation.

Tout repose sur l'invisibilité ?
Oui clairement, l'absence de matérialité et le fait que ce soit invisible, une des conséquences directes est que du coup c'est difficile d'attribuer une responsabilité. C'est difficile d'accuser ce qui est problématique.

Mais alors du coup on ne voit pas le problème ou on refuse de le voir ?
Il y a un sentiment d'impuissance : on en revient à un manque d'alternative et de possibilités.

Que faire pour « réveiller les masses » ?
C'est une question que met en avant Shoshanna Zuboff : concrètement, qu'est-ce qu'on peut faire ? Est-ce qu'une action collective pourrait avoir un impact ? Ce serait à l'État d'imposer un cadre légal de contrôle, « consistent » et « across countries ». Mais qu'est-ce qu'un État peut faire face à des organisations supranationales ?

Que pensez-vous de la marchandisation des données personnelles qu'évoque S. Zuboff ?
Ce qui est assez intéressant, c'est de voir les différents textes qu'elle a publiés depuis plusieurs années. En fait, ses idées sont présentes depuis longtemps, mais il était plus difficile de voir les ramifications et les conséquences de ce qu'elle mettait en avant. Aujourd'hui, les gens sont plus alertés sur ces sujets donc ils seront certainement plus réceptifs à son ouvrage. Auparavant, ça semblait un peu « futuriste ».

Les GAFAM nous contrôlent-ils vraiment grâce aux données collectées ?
Oui : vos recherches sont recoupées avec vos précédentes recherches par exemple. C'est du marketing beaucoup plus targuété, une compréhension beaucoup plus fine des besoins des utilisateurs, des préférences des consommateurs. C'est un système beaucoup plus efficace.

En quoi cette collecte de données massive est-elle dérangeante voire dangereuse ?
C'est une bonne question, ça dépend de comment est-ce qu'on regarde les choses mais on peut dire que c'est quand même inquiétant la facilité avec laquelle il est possible de faire du *profiling* sur les gens. Juste ne regardant la façon dont vous utilisez internet sur une période d'un mois, on pourra faire un profil très détaillé de qui vous êtes, d'où vous venez, quelles sont vos ambitions, qu'est-ce qui est important pour vous et ainsi de suite. Encore une fois le manque d'alternatives… Il n'y pas tellement de façon de *uptelled* le système. C'est plus la dimension totalitaire de ces procédés qui est problématique.

Donc on n'a aucun autre choix ?
C'est ça.

Une fois qu'on a souscris à ces services on ne peut plus en sortir ?
Oui exactement.

Est-ce que selon vous, le profilage porte atteinte aux libertés des individus ?
So you know this principle that if you have nothing to hide you shouldn't worry about the fact that your data is collected, I think it is quite problematic because it is not so much about having something to hide on that, it is more about the fact as a principle we should be able to have a full control of anything that is personal. Voilà, c'est l'idée que ça devrait être un principe que d'avoir justement un contrôle sur toutes les choses qui nous sont personnelles. Le fait que j'achète ceci ou cela en ligne, ce n'est pas une information, un secret qui va avoir des conséquences négatives sur moi ou les autres, c'est plus dans la mesure où par principe cela ne devrait pas être révélé, ou plutôt par principe ce genre d'information ne devrait pas être détenu par des compagnies privées ni utilisé à des fins commerciales. Si on met trop en avant la notion de risque ou de danger, on a tendance à oublier que c'est fondamentalement un problème de principe en rapport à ces différentes compagnies.

Ce serait quoi pour vous la donnée personnelle ?
Toute information me concernant dont je n'ai pas conscience qu'elle est partagée. Toute donnée me concernant en tant qu'individu et en particulier les données pour lesquelles je n'ai pas conscience que des compagnies privées y ont accès.

Ce serait donc quelque chose qui ne s'apparente pas à un bien marchand qui pourrait être revendu ?
Oui ce sont des choses différentes bien qu'il soit possible de monétiser ses données.

Donc quand vous dites que par principe on devrait avoir le droit d'avoir le contrôle sur ce qui est personnel, donc ça voudrait dire que personne d'autre n'y a droit sauf si on donne notre consentement ?
Oui exactement, c'est une forme détournée du *Contrat Social* de Rousseau. Dans le *Contrat Social* on abandonne certaines libertés individuelles pour avoir certaines choses en retour (la sécurité, etc.), cela marchait très bien dans le contexte du XVIII° siècle, mais je pense que là on a justement une *breach* de ce Contrat Social. On donne accès à toutes ces données, toutes ces informations mais justement sans en avoir conscience et sans gagner quoique ce soit en retour.

Mais alors les services soi-disant gratuits, offerts par les GAFAM ne sont pas cette contrepartie ?
Le problème c'est que ce n'est vraiment pas explicite. A quel genre de service vous pensez ?

Je pense tout simplement à l'accès à l'information via Google, l'accès à Gmail ect.

C’est ça, mais je pense que la majorité des personnes ne réalisent pas la dimension transactionnelle de tout ça. Quand vous utilisez Google pour chercher quelque chose, vous ne réalisez pas forcément que vous passez une sorte de contrat avec Google. Je peux utiliser la plateforme, mais en contrepartie je donne des données personnelles. Mais cette transaction n’est vraiment pas explicite. Il est peut-être là le problème, c’est-à-dire que beaucoup de personnes pensent qu’on peut utiliser ces plateformes de façon innocente pour notre loisir ou bénéfice sans réaliser qu’il y a forcément un coût, alors qu’il y a toujours un coût à payer.

Mais alors le concept de « servitude volontaire » s’applique sans s’appliquer vu que les personnes ne réalisent pas qu’elles passent un contrat ?
C’est ça, exactement.

Je me permets de revenir à la question posée précédemment, qu’est-ce que société de contrôle veut dire et est-ce que c’est applicable aux GAFAM ?
Je pense qu’on peut voir la société de contrôle comme une forme de conditionnement invisible ou inconsciente.

Quelles seraient les évolutions possibles de la situation actuelle ?
Je doute que la situation change beaucoup pour deux raisons, la première est qu’il y a eu un certain nombre de scandales, et bien évidemment cela a mené à la publication d’articles critiques et ainsi de suite mais fondamentalement je ne pense pas que cela va changer l’attitude des gens. Le deuxième point est qu’on a toujours une sorte de fascination autour des technologies, des nouvelles technologies. Je pense que cette fascination masque tous les problèmes de contrôle, de sécurité, de *privacy*, de surveillance etc., qui sont connectées à l’émergence de ces technologies en question.

Vous parlez de fascination, mais pourquoi les gens ne remettent-ils rien en question ?
Je pense que c’est un sentiment d’impuissance. On vit dans une société très individualisante, où il est très difficile de mobiliser des formes d’actions collectives. Et même si ces formes peuvent être mobilisées, elles ne pourraient pas avoir l’ampleur nécessaire pour avoir un impact sur ce genre de compagnies.

Les GAFAM sont donc tout puissants ?
Dans le contexte présent, relativement oui.

Donc c’est un monopole, un pouvoir totalitaire ?
Oui, dit comme ça, ça n’a pas l’air très cool en effet.

Le terme « irresponsabilité » est-il trop fort pour parler des individus ?
C’est une histoire d’intention. Par irresponsabilité vous voulez dire que ce sont des gens qui n’en n’ont volontairement rien à faire ou c’est plus une passivité générale ? Je pense qu’on est plus dans l’ordre de la passivité générale que d’activement n’en n’avoir rien à faire.

Pourquoi l'argument du « nothing to hide » est si difficile à déconstruire ? Et vient si spontanément dans la bouche des gens ?

Je pense que ce qui est intéressant à observer c'est la manière dont ce genre de slogan a été approprié à la fois par des structures étatiques et des compagnies privées, ce qui est assez informatif de certaines déconnexions qu'il existe entre ces différents types d'identités. On va aussi se servir de cet argument pour dire : on opère ces systèmes de surveillance pour protéger la société. Vous, si vous ne faites rien de mal, il n'y a pas de soucis, mais potentiellement en surveillant les gens, on pourrait repérer des actes terroristes etc. C'est donc sous couvert de vouloir protéger la société. Une fois que vous faites cette connexion entre surveillance et protection de la société, vous êtes entièrement dans l'argument totalitariste, mais en même temps vous créez un argument qui est assez difficile à déconstruire, tout du moins dans les médias en tout cas. On va vous dire « en effet, on surveille vos activités en ligne, mais grâce à cela, nous avons pu repérer et éviter une attaque ou appréhender tel individu qui avait pour projet de faire ceci ou cela ». Dans ce cas-là, c'est dire que peut-être qu'au fond c'est justifié. C'est l'argument qui ressort à chaque fois qu'un acte terroriste est commis. Ce qui est intéressant de voir c'est que si l'État n'arrête pas à temps le terroriste, on va dire « mais comment ça se fait que cette personne n'ait pas été surveillée ? Comment se fait-il qu'on n'ait pas eu d'indication que cette personne allait commettre tel ou tel acte ? ». Cela dénote une certaine hypocrisie.

Merci beaucoup !

Appendix 7 – Interview Transcript #5

Interviewer: Zuzanna Sonenberg
Interviewee: Tristan NITOT, VP Advocacy, Qwant, former President of Mozilla Europe
Interview Setting: Interviews conducted via Skype on June 21st, 2019, at 2:00 pm CET with the support of Apple MacBook recorder.

(Start of Interview)
(Presentation of the interviewer and the research topic, see Appendix 1 – Interview guide)

Pourriez-vous me parler un peu de vous ?
Pour faire vite, moi je suis informaticien, je suis tombé dans le numérique quand j'étais petit, j'ai appris à programmer tout seul à 14 ans et je trouvais que l'informatique c'était génial. J'ai fait une école d'ingénieur plus pour valider mes acquis que pour apprendre véritablement quelque chose, et puis je n'y étais pas beaucoup parce que je travaillais pendant ce temps-là. En 1997, j'ai rejoint la société Netscape qui a popularisé le navigateur Web, j'ai fait la promotion du Web et des technologies pendant longtemps. Dès 1998, la société Netscape a initié le projet Mozilla, qui était l'ouverture du code source de son navigateur pour que des gens viennent l'aider à développer des futures versions du navigateur et ça a donné Firefox. Comme j'étais là au début et que j'étais basé en Europe alors que mes collègues étaient aux États-Unis, quand Netscape a abandonné le projet Mozilla, mes collègues américains ont monté la Mozilla Foundation et moi je voulais les aider en Europe et j'ai monté Monzilla Europe, ça c'était en 2003, c'était une association de loi 1901 où j'ai été président pendant 9 ans. Au bout d'un moment j'en ai eu un peu marre d'être sur le projet Mozilla, j'avais envie de changement, même si je suis toujours très fan du projet Mozilla j'avais envie de faire autre chose, et donc il y a 4 ans j'ai quitté Mozilla et j'ai passé 3 ans dans une start-up sur les données personnelles qui s'appelle Cozy Cloud. C'est là que j'ai pris Nina pour qu'elle vienne travailler avec nous. Et il y a un an j'ai quitté Cozy Cloud pour rejoindre Qwant.

Que faites-vous au sein de Qwant ?
Je suis VP Advocacy, Vice-Président Plaidoyer en français. Je remplace notre président sur les aspects de communication vers l'extérieur, de la prise de parole en général, notamment concernant les données des utilisateurs, pourquoi Qwant respecte la vie de ses utilisateurs, en quoi c'est essentiel, comment on s'y prend etc. Beaucoup de communication autour de la vie privée.

Justement, pourquoi Qwant serait mieux que Google en termes de respect des données ?
Parce qu'il est « amnésique ». Il a une bonne mémoire sur ce que l'on trouve sur le web, mais il ne se souvient de rien concernant les utilisateurs. Qwant ne sait pas qui vous êtes, il oublie votre

adresse IP, il ne la rapproche pas des termes de recherche que vous soumettez, et se contente de donner une réponse. Son business model ne repose pas sur la capture de données personnelles, à l'inverse de Google qui incite fortement à ouvrir un compte Gmail qui permet de vous relier à un historique de navigation. D'ailleurs, le vrai client de Google c'est l'annonceur publicitaire, qui est friand du ciblage de Google.

Vous avez co-écrit *Numérique : Reprendre le Contrôle* et écrit *Surveillance : les libertés au défi du numérique. Comprendre et agir*. Quelles étaient vos motivations en écrivant ces ouvrages ?
J'ai eu un besoin d'écrire *Surveillance,* car je constatais que le numérique, dont je suis fan, était en train de filer un mauvais coton, et personne ne comprend comment et pourquoi car il n'y a pas d'éducation au numérique. Ils ne comprennent pas le capitalisme de surveillance, et pensent qu'on leur fait un cadeau génial de la même manière que les Troyens ont cru qu'on leur offrait un cheval de Troie. C'était un cadeau hyper généreux, incroyable, mais qui cachaient des soldats qui ont détruit la ville. Là c'est exactement pareil. Pourquoi Google vous offre tant d'outils ? Pourquoi est-ce qu'il offre Google Analytics aux entreprises, ou encore Android à Samsung ? Tout ça, ce sont des chevaux de Troie destinés à capturer de la donnée personnelle. C'est dangereux parce que l'on ne sait pas de quoi demain est fait et que l'on a tous quelque chose à cacher. Ce qui disent qu'ils n'ont rien à cacher, et bien c'est triste d'entendre ça et puis c'est faux. Avez-vous la conférence TED de Glenn Greenwald ? Il a été contacté un jour par Edward Snowden, et a récupéré ses révélations. Suite à cela, il fait une conférence TED dans laquelle il explique pourquoi on a tous quelque chose à cacher. Quand vous vous observés, et donc jugés, regardés, d'une manière ou d'une autre, vous vous autocensurez. Vous vous interdisez des actes et des pensées. Cela met comme des barreaux dans la tête des gens. Des choses qu'ils auraient osé penser et exprimer, ils ne le font plus car se savent sous surveillance. C'est une problématique de liberté individuelle, d'autant plus que l'article 12 de la Déclaration des Droits de l'Homme proclame le droit à une correspondance privée. Or, si vous vous savez observé, vous n'innovez plus, car l'idée créative est dérangeante en ce qu'elle bouscule l'ordre établi.

Donc est-ce conscient ou non de la part des individus ?
Probablement pas. En fait, les gens ne réalisent que rarement qu'ils s'autocensurent. C'est plus de la peur non-avouée. Je viens de vous envoyer un graphique, cliquez dessus. Ce graphique est en deux parties gauche et droite avec une barre au milieu. La barre ce sont les révélations Snowden. A gauche, c'est l'audience des pages de Wikipédia relative au terrorisme : on voit que les gens visitent de plus en plus ces pages-ci. C'est bien qu'ils le fassent, ils ont le droit de le faire et c'est bien qu'ils le fassent, c'est légal. Puis, juin 2013 : révélations Snowden, les gens apprennent qu'ils sont sous surveillance par la NSA. Et là, on voit une baisse de 20% de l'audience et ensuite ça plonge. Conclusions : les gens n'osent plus aller sur les pages concernant le terrorisme depuis qu'ils savent qu'ils sont sous surveillance.

Ici, vous m'avez décrit une surveillance plutôt étatique. Cela s'applique-t-il aux GAFAM ?
Pas forcément. Les GAFAM sont souvent perçus comme bienveillants. Si vous regardez la réputation de Facebook, elle est exécrable, ils multiplient les bévues, et pourtant les gens utilisent

le site en se disant qu'ils ne prennent pas trop de risques. Le danger est aussi bien au niveau d'un individu qu'au niveau d'une société et du fonctionnement institutionnel : regardez le scandale Cambridge Analytica. Je ne suis pas fan de l'expression GAFAM puisqu'elle met dans le même sac des entreprises différentes : Google et Facebook ont des business model comparables (collecte de données pour attirer des annonceurs), alors qu'Apple vend du matériel cher et Amazon fait de la grande distribution ou louer des services cloud (même s'il a une tendance à aller vers le B2C et dans le data). Idem pour Microsoft. Certains sont de nouveaux entrants, comme l'entrée en bourse de Slack par exemple, dont le modèle se rapproche de celui de Google. Sur la vie privée, ce sont surtout les États qui aimeraient engendrer les données sur les citoyens ; mais ce sont des entreprises comme Google et Facebook qui rendent la chose économiquement et matériellement possible.
Entre l'élection et l'institution de Trump, des activistes américains décident de faire une grande manifestation de manière décentralisée. Ils créent un site web à cet effet : Trump demande au Departement of Justice de saisir tous les fichiers log (historiques des connexions) sur ce serveur-là, de manière à faire peur aux opposants qui s'étaient inscrits sur ce site.
Ce qui rend économiquement possible la surveillance de masse c'est la centralisation de nos données entre les mains de quelques géants, sinon ça couterait trop cher. Nous sommes les idiots utiles de Google et Facebook qui sont les idiots utiles des États : c'est à deux étages. Je montre souvent la photo de deux vaches dans un pré lors de mes conférences : l'une dit « je suis nourrie gratuitement », l'autre répond « oui et en plus on est logé gratuitement ». Les gens pensent qu'ils sont les clients de Google et de Facebook, c'est juste qu'ils bénéficient de services gratuits. Mais non, on n'est pas les clients de Google ni de Facebook, on est leur bétail. Tant qu'on a en tête qu'on est des clients on comprend tout de travers. Il y a d'un côté les utilisateurs et de l'autre les annonceurs. Dans le cadre des plateformes, celui qui donne du vrai argent, c'est l'annonceur publicitaire. Le vrai client du fermier, c'est la coopérative laitière, pas les vaches. La matière première c'est le lait, à revendre.
Les gens n'ont pas conscience des données personnelles qu'ils laissent. Ce n'est pas seulement les données d'âge/taille/statut marital, ce sont aussi quelles personnes sont amies, quelles sont les vidéos que je regarde, où est-ce que je like, où est-ce que je partage, combien de temps je passe, sur mobile ou ordinateur, à quelle fréquence… Tout ça c'est de la data. Mais les utilisateurs lambda ne le comprennent pas. Ils ne comprennent pas qu'ils sont en train de faire un échange data contre un service qui coûte peu cher. Les grandes lignes publiques de la comptabilité de Facebook montrent qu'il fournit un service pour moins de 3 euros par utilisateur et par an : c'est le coût du service Facebook en comptant très large. Service obtenu en pompant toutes nos données personnelles. Je n'ai pas calculé la marge de Facebook, mais juste pour vous donner une idée, chez Google, un utilisateur occidental rapporte entre 60 et 90 euros par an, ce sont des marges énormes. Ce sont des marges de l'ordre de 70%. Les comptes de ces sociétés cotées sont publics, on peut les retrouver sur Internet. Vous pouvez regarder combien ils gagnent, et ensuite vous faites vos rapports, vous divisez par le nombre d'utilisateurs.

Vous utilisez le terme de « surveillance », de « surveiller » lorsque vous parlez des États. Est-ce que vous pensez que ce terme est adapté aux GAFAM ?

Je ne sais vraiment pas. Ce n'est pas forcément Big Brother, c'est plutôt Big Mother. Ça peut être une surveillance avec un aspect de dépendance. Ce n'est pas un gardien de prison qui surveille des prisonniers ; on est librement prisonnier de quelque chose d'irremplaçable dans nos vies quotidiennes. On croit qu'il est impossible de s'en défaire, et on fait tout pour vous en dissuader. C'est une dépendance bienveillante car le service est utile, pratique, sympa… Big Mother vous donne des bonbons et vous restez.

Je vous posais cette question car dans mes entretiens, les gens faisaient la dichotomie entre surveiller et tracer. Quel est votre avis ? Y'a-t-il une différence ?
Tracer ça correspond, mais c'est surtout profiler qui correspond. L'objectif est de pomper la donnée, profiler l'utilisateur, et rendre accroc. Car à l'inverse, recruter de nouveaux utilisateurs coûte cher : annuellement, Google donne 9,5 milliards de dollars à Apple pour qu'il mette Google Search en navigateur par défaut dans l'iPhone et l'iPad, autant d'argent juste pour que Apple mette Google en navigateur par défaut. Ça fait cher la case à cocher. Donc c'est important qu'il y ait un barrage, que les gens ne puissent pas aller voir ailleurs.

Comment qualifieriez-vous le profilage fait par les GAFAM ?
Ils font du profilage actif, c'est la condition de leur survie, c'est leur Business Model. L'utilisateur reste sur une plateforme parce que c'est sympa ou pratique, parce qu'il y a du fun ou de l'utilité. A l'inverse, il doit fournir du contenu : Facebook sans le contenu des utilisateurs, ça n'a plus aucun intérêt. Le contenu ce sont les photos, les commentaires, les likes. On est relativement conscient de fournir du contenu. Au-dessus, c'est de la donnée personnelle. Et là, les gens n'en ont pas du tout conscience. Les gens n'ont pas conceptualisé ce qu'est la donnée. La donnée est invisible et en plus elle est dématérialisée, fournit via le wifi ou la 4G. Les gens qui n'ont pas été formés au numérique, leur dire qu'ils ont fourni de la donnée ça ne leur parle pas. Il y a un milliard de façons de pomper de la donnée personnelle avec toutes les applications etc. Facebook pompe de la donnée personnelle, lorsque vous installez son application elle vous dit : je veux lire votre GPS, votre carnet d'adresse, vos textos, je veux savoir qui vous appelez, je veux accéder à tous vos fichiers… 2 milliards de personnes ont cliqué sur le bouton « Accepter » sans lire les conditions d'utilisation, c'est un autre problème. Mais au moins c'était extrêmement clair. C'est un marché de dupes car c'est un échange mais les gens n'ont pas conscience du volume et de la valeur des informations qu'ils donnent. Je vous l'ai dit précédemment, les individus vendent leurs données à très bas prix (3 euros/pers/an), ils n'ont pas conscience que le service échangé vaut très peu cher. C'est comme durant la traite négrière : on donnait de la verroterie contre des personnes ou des terres. On profitait du fait que le type en face n'avait aucune idée de la valeur de ce qu'il vous donnait et de ce qu'il recevait en échange. Ici, c'est pareil : on donne des choses sans comprendre leur valeur.

Comment définiriez-vous la donnée ? En opposition avec le contenu ?
C'est subtil. Le contenu d'une certaine manière, ce sont des données. Mais il est fourni volontairement, sans forcément comprendre ce que vous faîtes. Facebook est propriétaire du contenu que vous mettez dessus : un jour, un homme a trouvé qu'un réseau de rencontre amoureuse était illustré par une photo de sa femme, dont le propriétaire était Facebook.

La donnée c'est ce qui n'est pas forcément visible, ce qui est capté à l'utilisateur sans qu'il le réalise : les données GPS par exemple. Lorsque la coordonnée géographique est communiquée à Google, je ne reçois pas de notification qui m'en informe.
Depuis peu, des applis indiquent lorsque telle ou telle application utilise vos données ; ce système donne de la visibilité au transfert de donnée à des tiers. On donne ainsi de la visibilité à de la donnée capturée par des tiers. C'est très récent.

Vous parlez du manque d'éducation des utilisateurs. Comment le décririez-vous ?
Il y a une très forte injonction de passage au numérique : par les pairs, les employeurs… et ce passage est socialement récompensé parce que l'on devient « *in* ». Surtout, il y a un certain pouvoir à parvenir à utiliser les applications, ça nous met en valeur vis-à-vis des autres.
En face, il n'y a aucune formation au numérique. Fondamentalement, les gens s'éduquent au numérique par un parent qui n'y connait souvent rien, et le premier achat de smartphone ne s'accompagne pas d'explications. L'éducation passe malheureusement aussi par les scandales, mais aussi par les publicités des applis elles-mêmes. Il y a vraiment un manque de recul de la part des utilisateurs : les GAFAM, pour eux, c'est flou.

Donc on serait plutôt dans de la sensibilisation indirecte que dans la formation proactive ?
Exactement. Les risques mais aussi les possibilités doivent être sus et connus ; moi personnellement je ne suis pas que dans la dissuasion. Mais il y a clairement un manque de sensibilisation et de structuration dans celle-là. Les scandales ne permettent pas de tout à fait comprendre les enjeux du problème : on ne se focalise que sur l'événement, et pas sur les problématiques qu'il soulève.

Que pensez-vous des théories de M. Foucault ?
Ma pensée n'est pas aussi profonde, mais je pense qu'il y a une structuration invasive des nouvelles technologies. J'aime me connecter à Wikipédia, mais le temps passé sur les réseaux sociaux est beaucoup trop grand. Quand je vois les selfies, le scrolling sur Instagram, etc… je me dis que l'humanité mérite mieux que ça.

Donc vous pencheriez plus du côté de la théorie du collier électronique de Deleuze ?
Oui, mais il y a surtout un questionnement autour de l'économie de l'attention qui se transforme en économie de l'addiction. Nous sommes cramponnés à nos colliers. Avez-vous lu l'article sur l'Everest ? Des gens meurent de froid en-dessous du sommet, en attendant que ceux qui sont dessus prennent leur selfie. C'est dramatique. La culture Instagram est ce qu'il y a de pire pour moi.

Quelles seraient les solutions à cette situation ?
De l'éducation et du ralentissement. La période actuelle est une période de transition : la société va avoir les moyens de prendre du recul, d'éduquer… Le numérique a avancé très rapidement, mais la société a suivi tant bien que mal. La tendance va s'inverser, on va lever le pied.

Merci beaucoup !

Appendix 8 – Online questionnaire

Part 1 : Profil de l'enquêté

1. Êtes-vous : Femme / Homme

2. Quel âge avez-vous ? 18-24 ans / 25-34 ans / 35-44 ans / 45-54 ans / 55-65 ans

3. Quelle est votre catégorie socio-professionnelle : Agriculteurs / Artisans, commerçants, chefs d'entreprises / Cadres et professions intellectuelles supérieures / Professions intermédiaires / Employés (qualifié/non qualifié) / Ouvrier (qualifié/non qualifié) / Retraité / Sans activité professionnelle (étudiant/chômeur) / Autre

4. Quel est votre niveau d'étude actuel ? Bac / Bac+2 / Bac+3 / Bac +4 / Bac+5 / Doctorat

Part 2 : Navigation en ligne & utilisation des services numériques

1. A quelle fréquence utilisez-vous les services offerts par Google ? Plusieurs fois par jour / Plusieurs fois par semaine / Plusieurs fois par mois / Rarement / Jamais

- Google Search (barre de recherche)
- Gmail
- Google Drive
- Google Maps

2. A quelle fréquence utilisez-vous les services offerts par Facebook ? Plusieurs fois par jour / Plusieurs fois par semaine / Plusieurs fois par mois / Rarement / Jamais

- Facebook
- Messenger
- Instagram
- Whatsapp
- Snapchat

3. A quelle fréquence utilisez-vous les services d'Amazone ? Plusieurs fois par jour / Plusieurs fois par semaine / Plusieurs fois par mois / Rarement / Jamais

4. A quelle fréquence utilisez-vous les services d'Apple ? Plusieurs fois par jour / Plusieurs fois par semaine / Plusieurs fois par mois / Rarement / Jamais

5. A quelle fréquence utilisez-vous les services de Microsoft ? Plusieurs fois par jour / Plusieurs fois par semaine / Plusieurs fois par mois / Rarement / Jamais

6. Selon vous, ces services sont-ils indispensables à votre vie quotidienne ? Oui / Non

7. Ces services sont-ils irremplaçables ? Oui / Non

8. S'ils devenaient payants, seriez-vous prêt à verser quelques euros par an pour continuer d'en bénéficier ? Oui / Non

Part 3 : Possession & utilisation d'objets connectés

1. Possédez-vous un smartphone ? Oui / Non

2. Quelle(s) utilité(s) faites-vous de votre smartphone ?

- Téléphone / SMS
- Multimédia (Musique, Vidéos, Photos)
- Emails
- Internet mobile
- Réseaux sociaux
- Applications
- Jeux
- Achats via mobile
- Paiement
- Navigation GPS

3. Gardez-vous votre smartphone toujours près de vous ? Oui / Non

4. A quelle fréquence utilisez-vous votre smartphone ? Plusieurs fois par heure / Plusieurs fois par jour / Au moins une fois par jour / Plusieurs fois par semaine / Plus occasionnellement

5. Selon vous, votre Smartphone est-il un outil pouvant provoquer des effets néfastes (santé, sécurité (utilisation au volant), liberté (addiction)) ? Oui / Non / Je ne sais pas

6. Détenez-vous une montre connectée ? Oui / Non

7. Quelle(s) utilité(s) faites-vous de votre montre connectée ?

- Téléphone / SMS
- Multimédia
- Emails
- Internet
- Applications
- Jeux
- Réseaux sociaux

- Santé
- Activités sportives
- Paiement
- Navigation GPS

8. A quelle fréquence utilisez-vous votre montre connectée ? Plusieurs fois par heure / Plusieurs fois par jour / Au moins une fois par jour / Plusieurs fois par semaine / Plus occasionnellement

9. Selon vous, votre montre connectée est-elle un outil pouvant provoquer des effets néfastes (santé, sécurité, liberté (addiction)) ? Oui / Non / Je ne sais pas

Part 4 : Degré de confiance des utilisateurs

1. Faites-vous confiance aux GAFAM ? Échelle de 1 à 10

2. Avez-vous des degrés de confiance différents en fonction des GAFAM ? Oui / Non

3. Si oui, précisez le degré : Échelle de 1 à 10

- Google
- Facebook
- Amazone
- Apple
- Microsoft

4. Faites-vous confiance aux réseaux sociaux ? Échelle de 1 à 10

5. Faites-vous confiance aux objets connectés ? Échelle de 1 à 10

6. Lorsqu'il s'agit de partager des informations intimes, lequel de ces outils est selon vous le plus adapté et sécurisé ? Classez les assertions suivantes dans l'ordre croissant, échelle de 1 à 5 (1 le moins sécurisé ; 5 le plus sécurisé)

- Réseaux sociaux
- Messagerie instantanée
- E-mail
- SMS
- Appel téléphonique

Part 5 : Données personnelles & protection de la vie privée

1. Selon vous, détenez-vous le contrôle de vos données personnelles sur Internet ? Entièrement / Moyennement / Peu / Pas du tout

2. Selon vous, protégez-vous suffisamment vos données personnelles en ligne ? Oui / Non

3. Donnez-vous l'accord aux pages web d'enregistrer vos données personnelles pour pré-remplir des documents en ligne ? Oui / Non

4. Lisez-vous les conditions générales d'utilisation des sites internet et services en ligne avant de les accepter ? Systématiquement / souvent / de temps en temps / rarement / jamais

5. Contrôlez-vous le statut des cookies lorsque vous naviguez sur le web ? Systématiquement / souvent / de temps en temps / rarement / jamais

6. Vous arrive-t-il de dissimuler votre identité en ligne (par exemple utiliser une fausse identité pour accéder à un site internet) ? Oui / Non

7. Pour chaque proposition, indiquez le niveau de sensibilité de l'information : Échelle de 1 à 10 (1 pas sensible ; 10 très sensible)

- Localisation
- Habitudes d'achats en ligne
- Historique d'achats en ligne
- Historique des sites internet visités
- Boîte mail
- Adresse du domicile
- Numéro de sécurité sociale
- Numéro de carte bancaire
- Post sur les réseaux sociaux
- Numéro de téléphone
- Physiologie (âge, sexe, taille, poids)
- Orientation sexuelle
- Chats en ligne

8. Êtes-vous favorable à ce que les GAFAM puissent exploiter vos données personnelles pour vous offrir des services personnalisés ? Oui / Non / Je ne sais pas

9. Êtes-vous favorable à ce que les GAFAM puissent exploiter vos données personnelles pour vous offrir des réductions ? Oui / Non / Je ne sais pas

10. Quel est, selon vous, le degré d'intrusion des GAFAM dans votre vie privée ? Très bas / Bas / Modéré / Élevé / Très élevé / Excessif

11. A quelle fréquence abordez-vous le sujet de l'utilisation de vos données avec d'autres personnes ? Au moins une fois par jour / Plusieurs fois par semaine / Plusieurs fois par mois / Rarement / Jamais

12. Quel(s) sujet(s) ces discussions concernent-elles ? Question ouverte

Part 6 : Autres services numériques

1. Connaissez-vous des applications ou logiciels neutres vis-à-vis de la collecte de vos données personnelles ? Oui / Non

2. Connaissez-vous les services suivants ? Oui / Non

- Qwant
- Lilo
- Startpage
- Mozilla Firefox
- Brave
- Whaller
- Linux
- Eelo

3. Si oui, évaluez leur degré de substitution aux GAFAM : échelle de 0 à 10 (0=pas du tout substituable ; 10 = totalement substituable)

4. Connaissez-vous les logiciels libres (par exemple Framasoft) ? Oui / Non)

5. Si oui, évaluez leur degré de substitution aux GAFAM : échelle de 0 à 10 (0=pas du tout substituable ; 10 = totalement substituable)

Part 7 : Votre ressenti vis-à-vis des GAFAM

1. Quel impact les nouvelles technologies ont-elles sur votre vie privée ? Très positif / Positif / Neutre / Négatif / Très négatif

2. Quel est l'impact des services offerts par les GAFAM sur votre vie quotidienne ? Très positif / Positif / Neutre / Négatif / Très négatif

3. Les GAFAM ont-ils une influence sur la société actuelle ? Oui / Non / Je ne sais pas

4. Selon vous, les GAFAM ont-ils des concurrents ? Oui / Non / Je ne sais pas

5. Les activités des GAFAM devraient-elles être davantage contrôlées ? Oui / Non / Je ne sais pas

Part 8 : Marchandisation des données

1. Selon vous, les données personnelles sont-elles un bien marchand comme un autre ? Oui / Non / Je ne sais pas

2. Selon vous, les données personnelles ont-elles une valeur pécuniaire ? Oui / Non / Je ne sais pas

3. Êtes-vous favorable au don de vos données personnelles aux entreprises numériques afin de bénéficier de services gratuits ? Oui / Non / Je ne sais pas

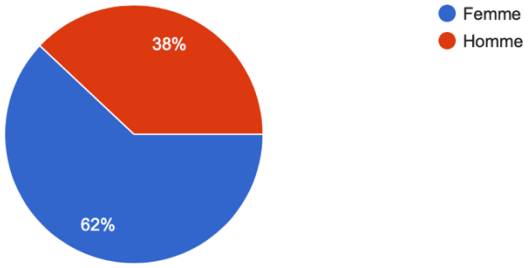
4. Que pensez-vous de l'assertion suivante : « Si c'est gratuit, c'est que c'est vous le produit ? » Echelle de 0 (pas d'accord) à 10 (tout à fait d'accord)

Appendix 9 – Results of the online questionnaire

Part 1 : Profil de l'enquêté

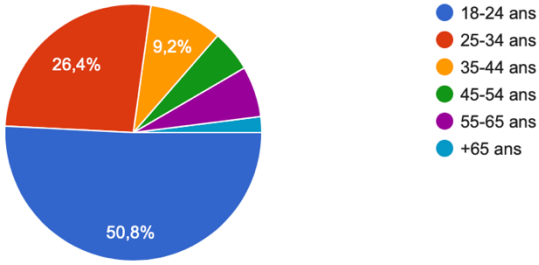
Êtes-vous

250 réponses



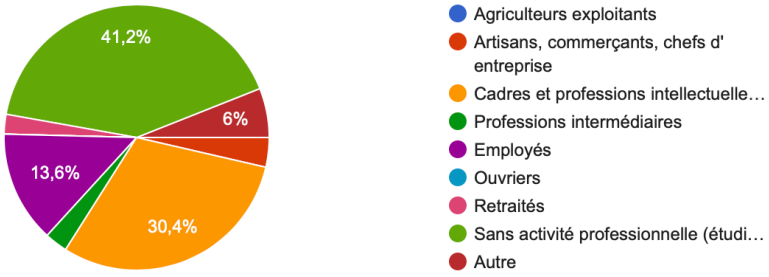
Quel âge avez-vous ?

250 réponses



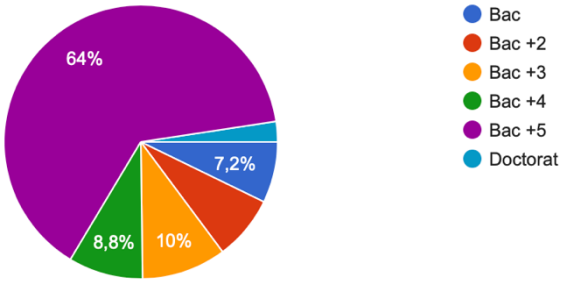
Quelle est votre catégorie socio-professionnelle

250 réponses



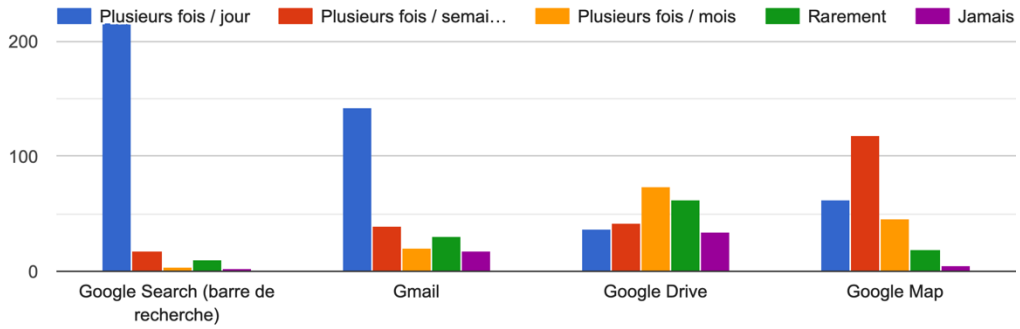
Quel est votre niveau d'études actuel ?

250 réponses

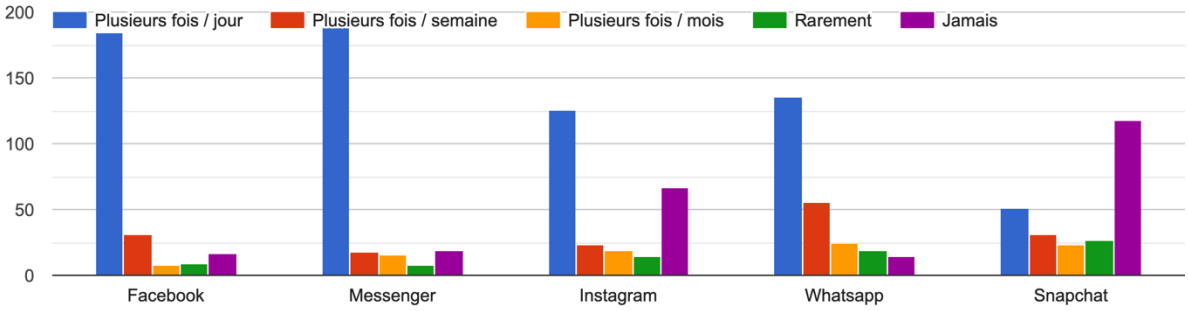


Part 2 : Navigation en ligne & utilisation des services numériques

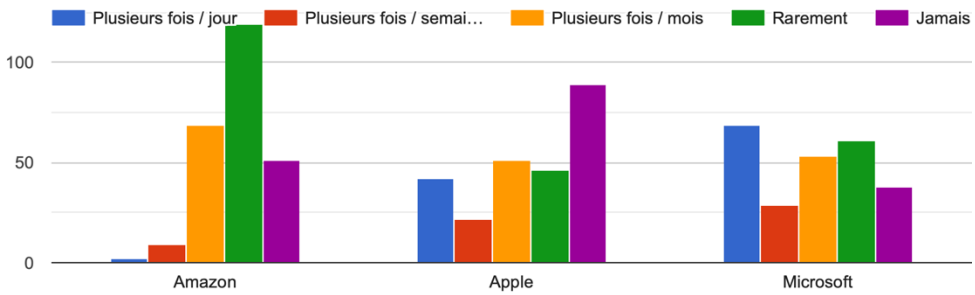
A quelle fréquence utilisez-vous les services offerts par Google ?



A quelle fréquence utilisez-vous les services offerts par Facebook ?

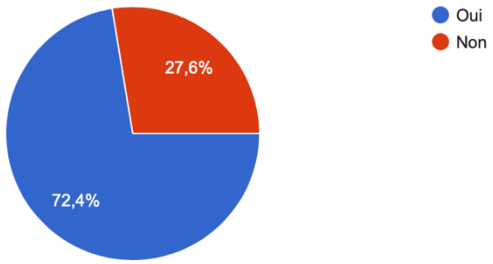


A quelle fréquence utilisez-vous les services de... ?



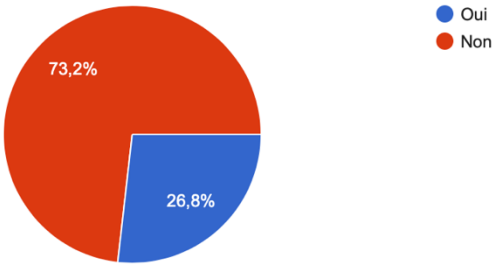
Selon vous, ces services sont-ils indispensables à votre vie quotidienne ?

250 réponses



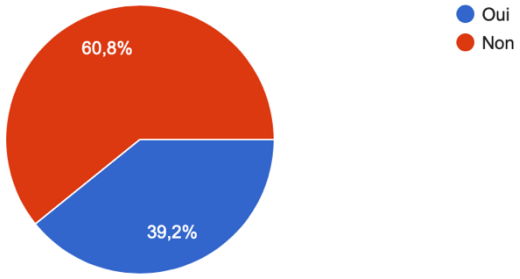
Ces services sont-ils irremplaçables ?

250 réponses



S'ils devenaient payants, seriez-vous prêt à verser quelques euros par an pour continuer à en bénéficier ?

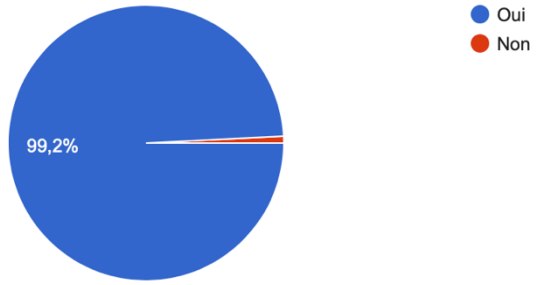
250 réponses



Part 3 : Possession & utilisation d'objets connectés

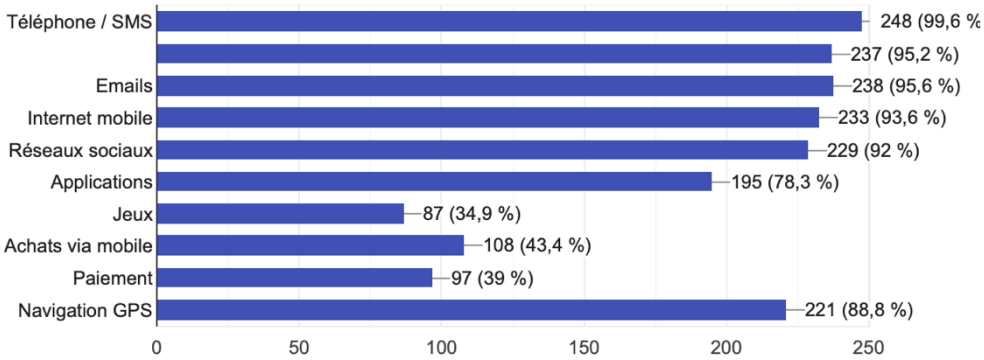
Possédez-vous un Smartphone ?

250 réponses



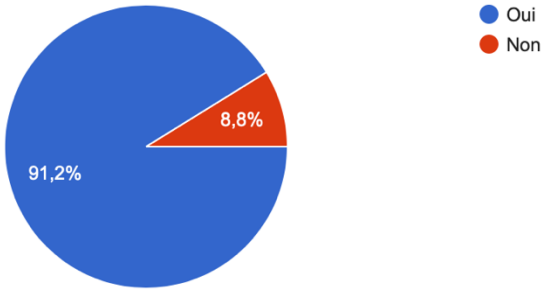
Quelle(s) utilité(s) faites-vous de votre Smartphone ?

249 réponses



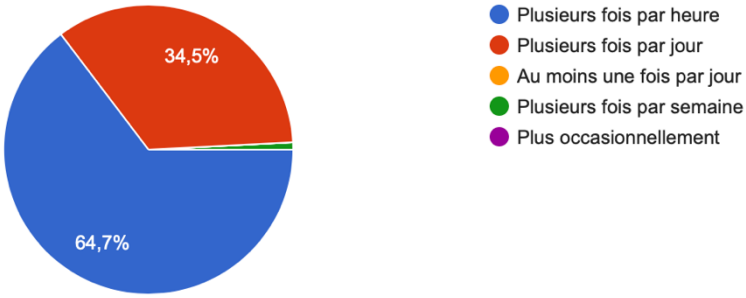
Gardez-vous votre Smartphone toujours près de vous ?

250 réponses



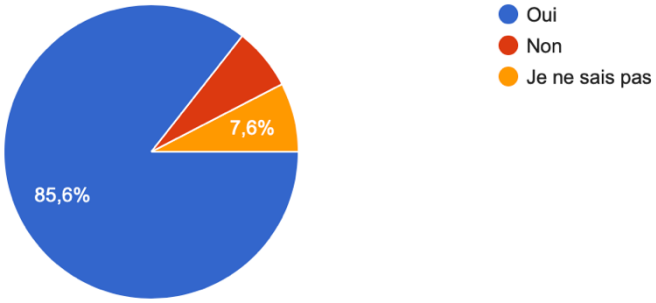
A quelle fréquence utilisez-vous votre Smartphone ?

249 réponses



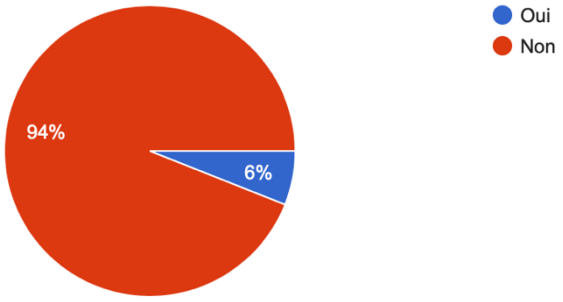
Selon vous, votre Smartphone est-il un outil pouvant provoquer des effets néfastes ?

250 réponses



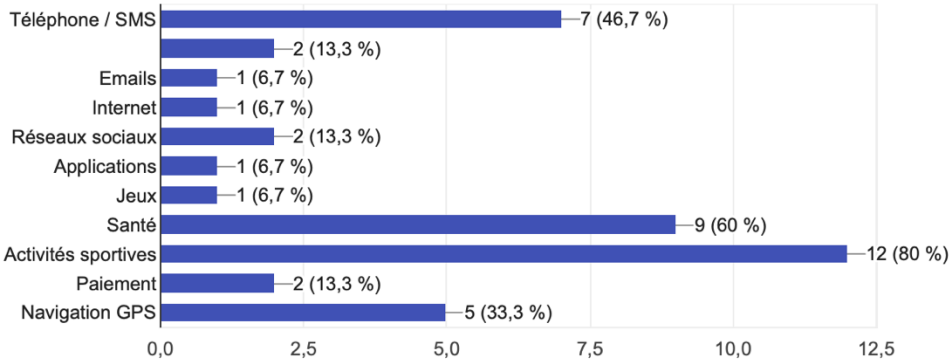
Détenez-vous une montre connectée ?

250 réponses



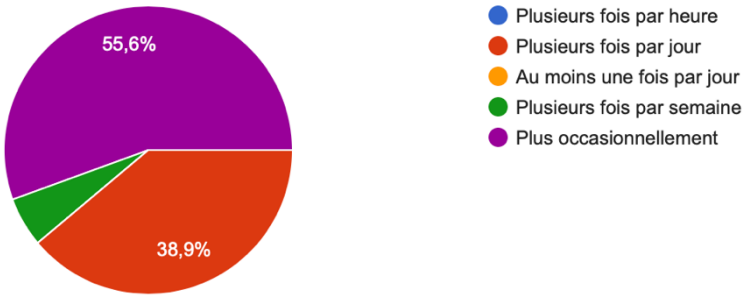
Quelle(s) utilité(s) faites-vous de votre montre connectée ?

15 réponses



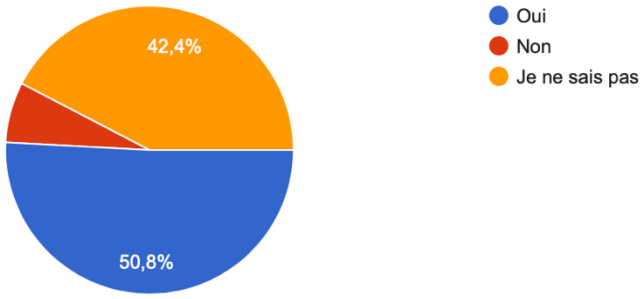
A quelle fréquence utilisez-vous votre montre connectée ?

18 réponses



Selon vous, votre montre connectée est-elle un outil pouvant provoquer des effets néfastes ?

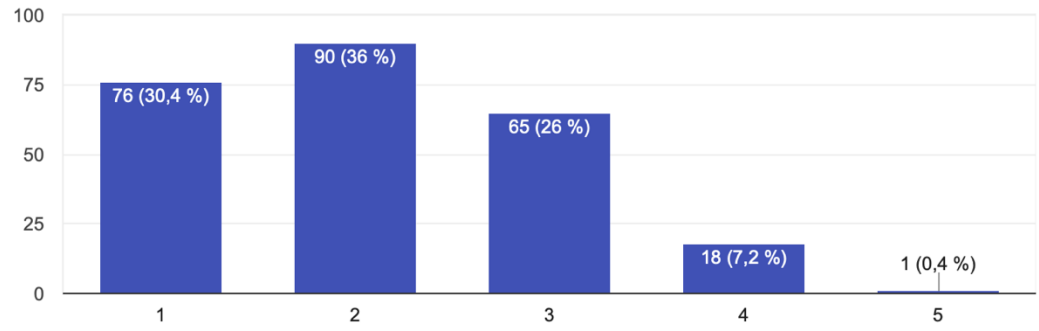
59 réponses



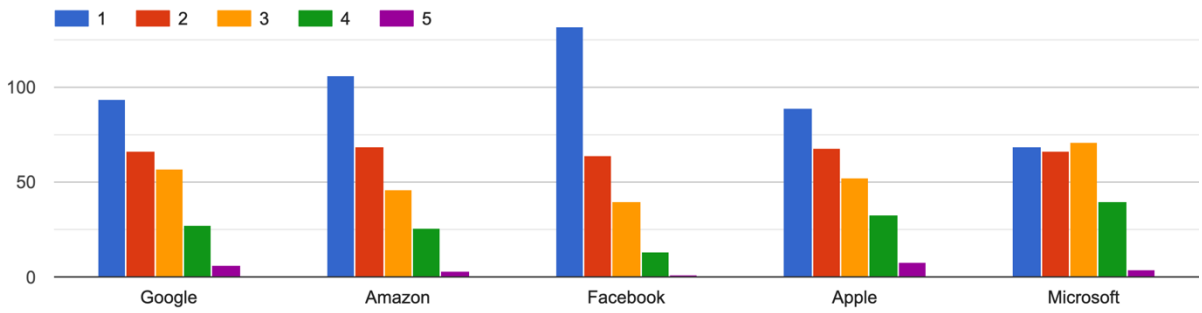
Part 4 : Degré de confiance des utilisateurs

Faites-vous confiance aux GAFAM ?

250 réponses

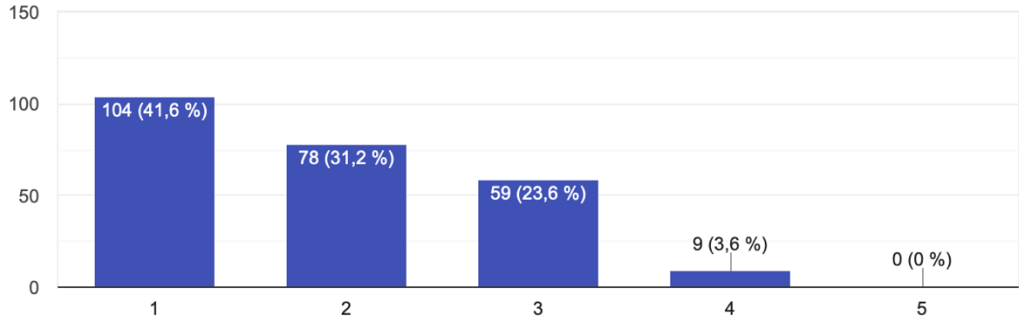


Evaluez votre confiance pour chacun des GAFAM... (Ordre croissant : 1 = pas confiance, 5 = confiance)



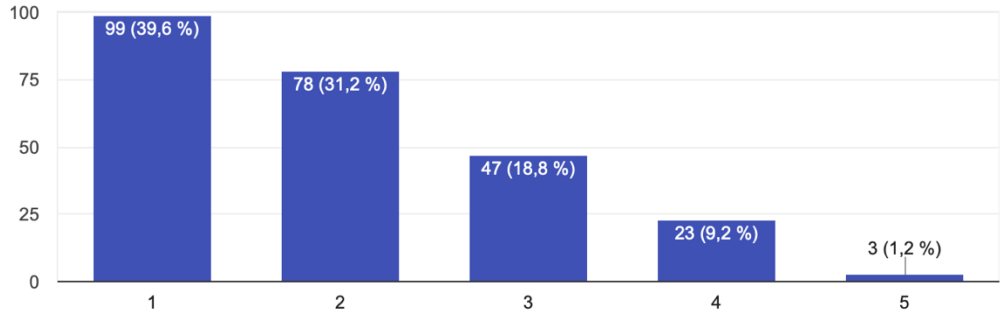
Faites-vous confiance aux réseaux sociaux ?

250 réponses

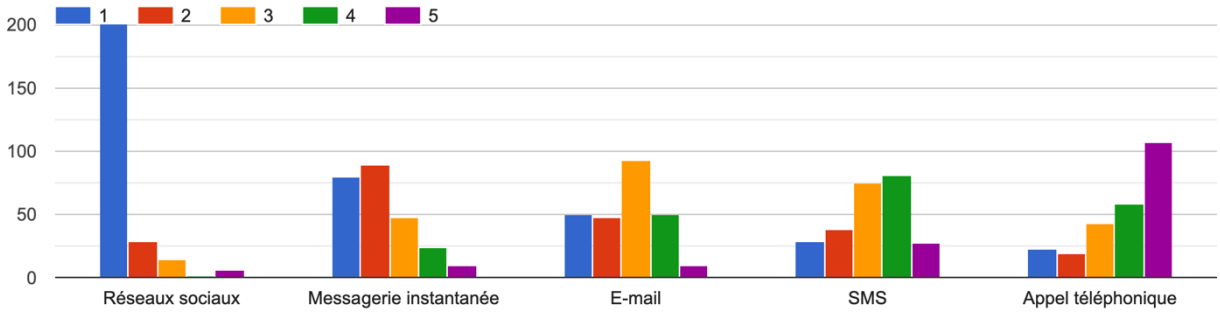


Faites-vous confiance aux objets connectés ?

250 réponses



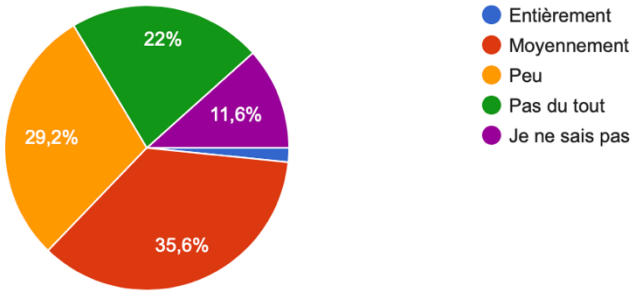
Lorsqu'il s'agit de partager des informations intimes, lequel de ces outils est selon vous le plus adapté et sécurisé ? (Ordre croissant : 1= le moins ; 5 = le plus)



Part 5 : Données personnelles & protection de la vie privée

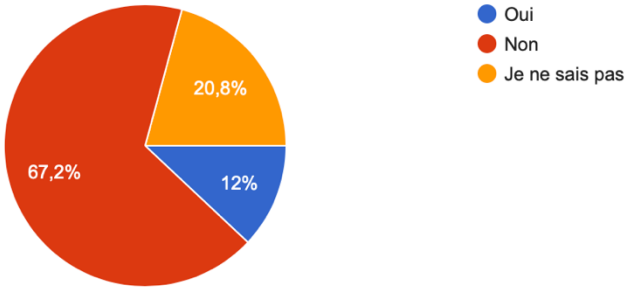
Détenez-vous le contrôle de vos données personnelles sur Internet ?

250 réponses



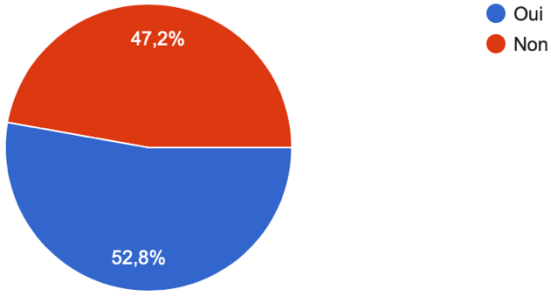
Selon vous, protégez-vous suffisamment vos données personnelles en ligne ?

250 réponses



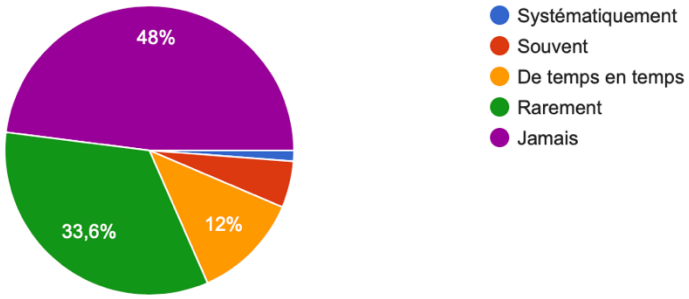
Donnez-vous l'accord aux pages web d'enregistrer vos données personnelles pour pré-remplir des documents en ligne ?

250 réponses



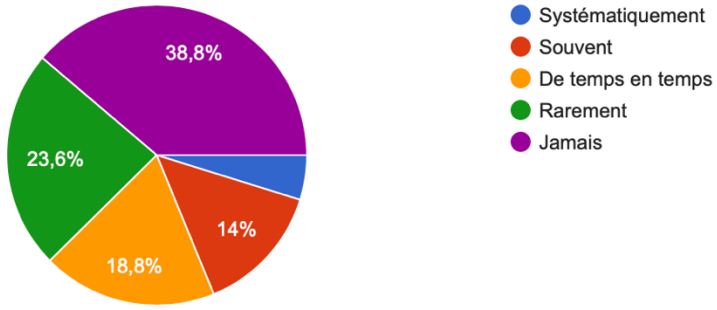
Lisez-vous les conditions générales d'utilisation des sites internet et services en ligne avant de les accepter ?

250 réponses



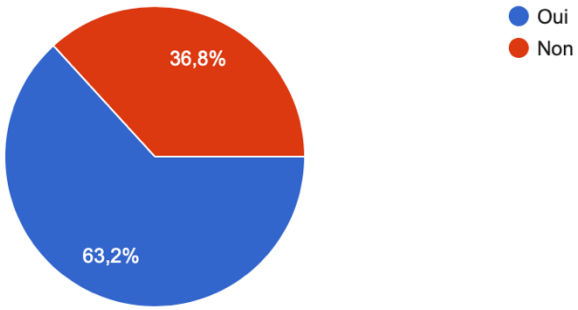
Contrôlez-vous le statut des cookies lorsque vous naviguez sur le web ?

250 réponses

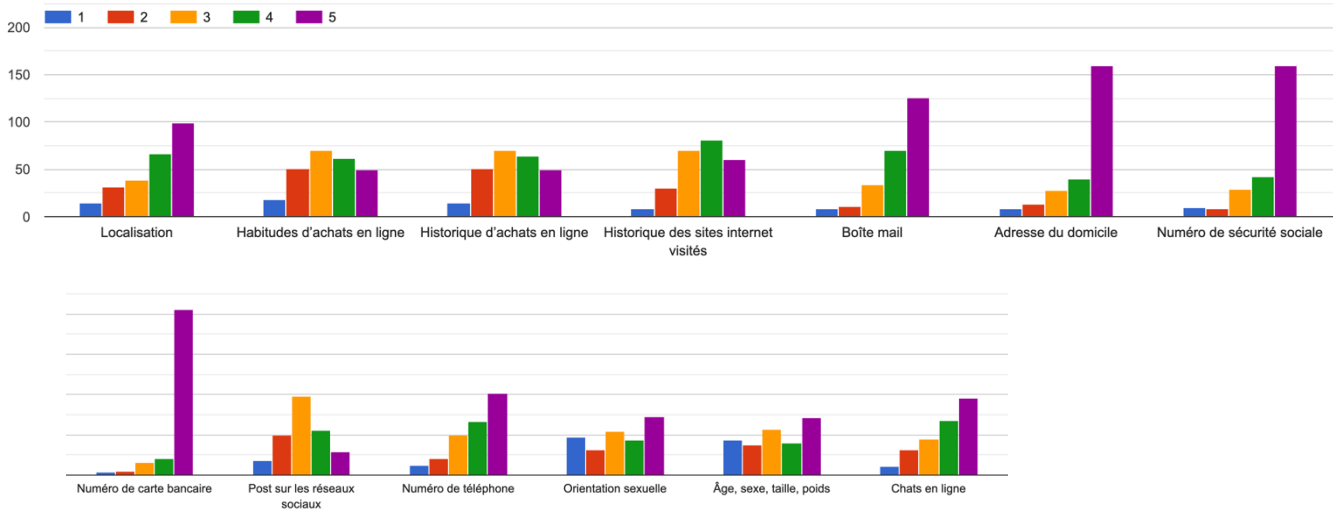


Vous arrive-t-il de dissimuler votre identité en ligne (par exemple remplir un questionnaire aléatoirement pour accéder à un site internet) ?

250 réponses

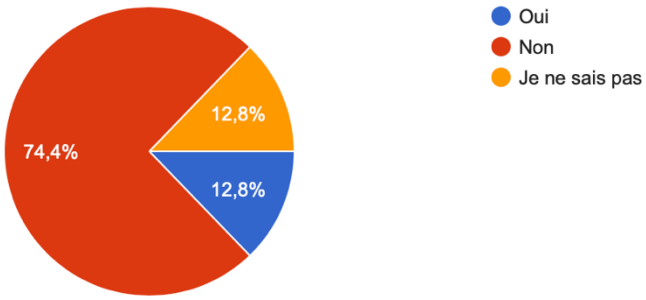


Pour chaque proposition, indiquez le niveau de sensibilité de l'information (Ordre croissant : 1 = pas sensible ; 5 = très sensible)



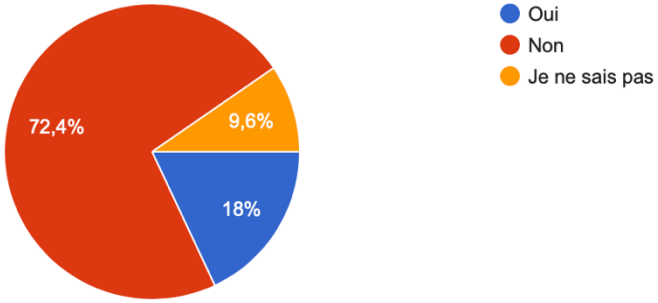
Êtes-vous favorable à ce que les GAFAM puissent exploiter vos données personnelles pour vous offrir des services personnalisés?

250 réponses



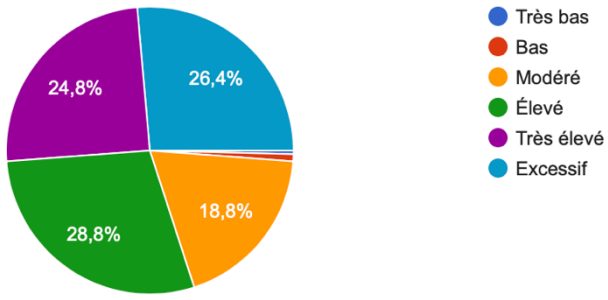
Êtes-vous favorable à ce que les GAFAM puissent exploiter vos données personnelles pour vous offrir des réductions ?

250 réponses



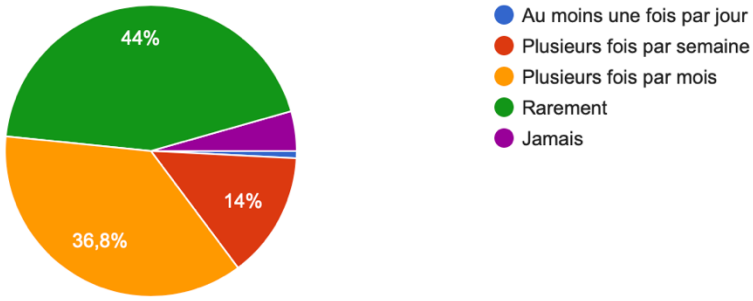
Quel est selon vous le degré d'intrusion des GAFAM dans votre vie privée ?

250 réponses



A quelle fréquence abordez-vous le sujet de l'utilisation de vos données personnelles avec d'autres personnes ?

250 réponses



Quel(s) sujet(s) ces discussions sur les données personnelles concernent-elles ?

250 réponses

Selection of the most interesting answers:

La confidentialité et l'intrusion dans la vie privée
Souvent, la peur de l'intrusion excessive est abordée, par exemple la "mise sur écoute" de nos propos, lorsqu'une discussion a lieu et que suite à celle-ci des suggestions nous sont faites lorsque l'on se connecte sur les réseaux sociaux
La place de ce genre d'entreprise sur nos vies, le futur de l'information
Piratage CB
Flou autour de la récupération
Cookies et publicités intempestives

La protection de celles ci
Données collectées à notre insu
Les données de santé
La conservation des données envoyées et publiées sur internet
RGPD, publicité
Publicités personnalisées, utilisation et vente des données
Le flicage
Sécurité des données / revente des données
La capacité des réseaux sociaux à proposer du contenu qui nous concerne/plait sans nous avoir au préalable demandé ce que l'on aimait. La sensibilité autour de la communication des données de carte bancaire en ligne. Les peurs d'usurpation d'identité...
Big brother is watching you
A qui appartiennent les données (niveau étatique)
Retargeting
L'influence des GAFAM sur nos opinions politiques
WeChat
La non-maîtrise de ces données par les utilisateurs
Protéger ses données, l'importance que la France puisse les protéger pour des citoyens, les contraintes à imposer en la matière aux entreprises
L'utilisation de ces données
Publicité ciblée, tracking
La RGPD
La protection des données
Les réseaux sociaux
L'insécurité
Protection de la vie privée
L'exploitation de mes données personnelles et leur monétisation
L'absence de contrôle de ses données et surtout la manne financière qu'elles constituent
Intimité, militantisme, ...
Liberté et atteinte à la vie privée, publicité omniprésente et de plus en plus ciblée...
Sur le fait de savoir si celles - ci sont réellement protégées et comment améliorer cette protection
Intrusion
Projection des données, pistage des infos, pubs ciblées
Publicités personnalisées, localisation (+++ Google)
Vie privée et neutralité du net
L'utilisation par les réseaux sociaux de données personnelles, le règlement européens sur la protection des données personnelles, l'utilisation des images personnelles
Utilisation, vente, vol d’identité
Localisation + connaissance trop importante des utilisateurs
La sécurité et le droit à la vie privée
Cyber sécurité, fraude et vols de données bancaires, utilisation des données par les GAFAM.
Vie privée, rapport de force entre États et GAFAM, confiance et consentement du consommateur
Droit, RGPD, utilisation abusive
Publicités en ligne, localisation automatique
Recommandation d'usage de VPN / Brave / Qwant.
Identité virtuelle
Vie privée + Big Brother is watching you

Vie privée, commercialisation des données, exploitation hors Europe
Atteinte à la vie privée, vol et recèle d'informations privée
Les libertés sur internet, la neutralité du web
Intrusion dans la vie privée et exploitation commerciale abusive
Aujourd'hui j'ai vaguement pensé que je partirais bien au Japon et j'ai eu quelques heures après une pub pour un voyage au Japon et sérieux c'est creepy
Le fait qu'il soit souvent impossible de ne pas transmettre de données personnelles, les spams sur email perso
Publicités ciblées, achats de billets de transport, appels intempestifs…
Écoute des conversations par l'iPhone qui cible les achats par la suite
Traçabilité des opinions exprimées, exploitation des données par les régimes autoritaires (not. cas de la Syrie), traçabilité de l'adresse IP, exploitation/accès au micro (pubs sponsorisées en lien avec des discussions uniquement orales ??!), vente des données mettant en danger les utilisateurs
La possible écoute des conversations par le micro mis par défaut sur Google ; les coïncidences de pub qui arrivent sur des comptes reliés entre eux (recherche Google vs pub Instagram par exemple) etc.
Orientation des achats, écoute des conversations par les appareils connectés, orientation / ciblage des publicités
Les publicités ciblées en fonction de notre navigation, le fait que nous ayons tout donné sur les RS lorsque nous étions plus jeunes et que l'emprunte numérique est donc difficile à gérer
Principalement l'utilisation de nos données pour du ciblage publicitaire
Le contrôle des données
Adresse, âge, sexe...
Surtout les réseaux sociaux et en particulier ce qui concerne le ciblage publicitaire
Messenger nous écoute par nos smartphones, on nous observe avec les camera frontale. SAMSUNG aussi sont à fond
Le profit de ces firmes
Photos et habitude de consommation
Protection des données, qu'est-ce qui doit être posté en ligne vs ce qui ne doit pas l'être
Protection et utilisation de nos données.
IA
GDPR, confidentialité des données
Publications et messages sur réseaux sociaux. Protection de la vie privée
L'exploitation de mes datas en tant que ressource, matière première pour laquelle je n'ai aucune rémunération alors que sans moi ces data n'existeraient pas.
Surveillance généralisée, utilisation des données à des fins commerciales, évasion fiscale, tout ce qui peut être lié au shaming, usage d'internet et des réseaux sociaux par adolescents et personnes âgées
L'utilisation de données sensibles détournées. Numéro de CB par exemple
Publicités ciblées après une conversation sur un produit
Piratage bancaire
Les mots de passe, les pubs ciblées
Coordonnés bancaires, achats, préférences, pubs
À quel point nos données personnelles sont utilisées, dans quel but, à quel point notre vie privée est touchée/scrutée
Le fait de savoir les données collectées de près ou de loin par les GAFAS et autres entités numériques / Le manque de transparence sur l'utilisation des données personnelles / Le contrôle relatif de nos données personnelles sur internet / le manque de confidentialité dans certaines

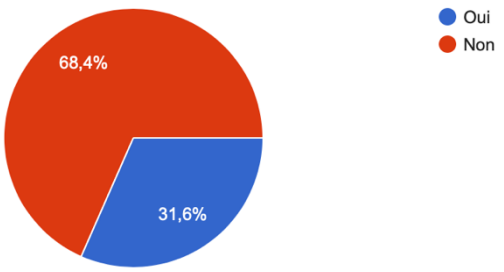
applications type FB, WhatsApp etc. et la recherche constante d'outils annexes pour conserver cette confidentialité (Telegram etc).
Sur les achats en ligne
Vie privée harcèlement
L'avenir et les moyens de contrôle
Mobile, internet, risque, protection
Le manque de contrôle sur nos propres données et le peu de visibilité sur ce à quoi ont accès les GAFAM, s'ils revendent nos données, à qui, etc.
L'absence de vie privée et l'accès à toute information personnelle
La désinformation, l'espionnage, le tracking, le ciblage des publicités, le recueillement des données
La question de savoir s'ils peuvent activer notre micro
Parfois on pense à quelque chose et on le voit apparaître dans des posts sponsorisés sur Facebook...
Dérives totalitaires, qu'elles soient privées ou publiques.
L'intrusion via les micros et les caméras
L'intrusion des GAFAM dans notre liberté d'achat
Protection de ces données
Objets connectés (type Google Home) qui pourraient écouter des informations sensibles, pubs personnalisées sur des sujets très précis alors que le sujet n'a été abordé qu'à l'oral...
Le « pistage » systématique et l'absence de l'anonymat
La publicité
Sécurité / Intrusion dans la vie privée
Utilisation des données sensibles
Les GAFAM et les gouvernements
Achats, vie privée, loisirs
L'utilisation à des fins politiques
Les contenus et pubs personnalisées sur les réseaux, la simplification des parcours d'achats ou d'onboarding clients à l'aide des données enregistrées un peu partout
Exposition des enfants sur les RS / recherche Google
Le contrôle de nos informations sur notre vie privée
Intrusion vie privée, dérives démocratiques
Leurs utilisations et la captation trop grande de données
Publicités liées à des sites visités
A quel point ces services ne sont en réalité pas gratuits
A quel point les GAFAM peuvent être intrusifs dans notre vie de tous les jours
Protection vie privée, usurpation d'identité
J'ai remarqué et plus d'une fois que lorsque je parle de vive voix avec un ami d'un sujet, j'ai systématiquement une pub sur Instagram ou Facebook concernant cet objet dont nous venons de parler alors que je n'ai JAMAIS fait de recherche là-dessus. Déjà arrivé également avec les conv Messenger
Paiements en ligne, vie privée déballée sur les réseaux sociaux
Comment mieux se protéger
Business issue de ces données
RGPD
Vie privée
Lorsque je reçois des notifications push sur quelque chose dont j'ai parlé à l'oral avec quelqu'un quelques jours auparavant (ce qui m'arrive souvent)

Lorsque, avec un groupe d'amis, nous sommes passés de Messenger à Signal / Telegram pour plus de sécurité/anonymité
Exposition sur les réseaux sociaux, récolte automatique (ou sans connaissance) des données sur nos appareils
Photos postées sur Facebook
Achats en ligne / coordonnées bancaires / sites suffisamment sécurisés ?
Vie privée / protection
Relation client dans le cadre professionnel, accès à l'identité en cas d'agression, vie privée
Sécurité
Vie privée / Identifiants
Addiction, au smartphone, veiller à moins utiliser son téléphone, les dangers de l'utilisation des données, le futur
Utilisation de Google ou de Qwant, ...
Toujours sur la peur / le fait d'avoir marre que nos téléphones et ordinateurs "nous écoutent", "nous lisent"...
Espionnage et renseignement
Que reste-t-il de la vie privée ?
Publicité personnalisé
Sécurité
Achats
La sélection des publicités par rapport à l'individu et ses habitudes
Sécurité de l'information, sécurité des SI
Utilisation des différents outils connectés
Utilisation des caméras des téléphones portables sans notre accord
Personnel = privé = intimité = foutez nous la paix
Utilisation à des fins commerciales, utilisation à des fins politiques, le risque de "fuites" de données
Les opérations de désinformation, les business model s'appuyant sur la gratuité (publicité)
Cyber-sécurité, protection vie privée
Suivi et stockage des données
La confidentialité Le contrôle de la vie personnelle
Réseaux sociaux, applications, utilisation des données
Confidentialité
Protection des données / publicités posts cibles / utilisation abusive des données / moyens de contourner cette utilisation / canaux de communication web alternatifs
La protection et l'utilisation des données
L'intrusion dans la vie privée
Paiement en ligne
La confidentialité, les cookies, les cyberattaques

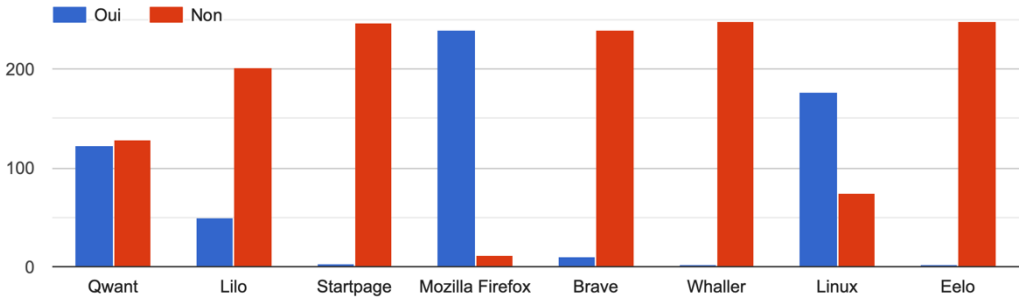
Part 6 : Autres services numériques

Connaissez-vous des applications ou logiciels neutres vis-à-vis de la collecte des données personnelles ?

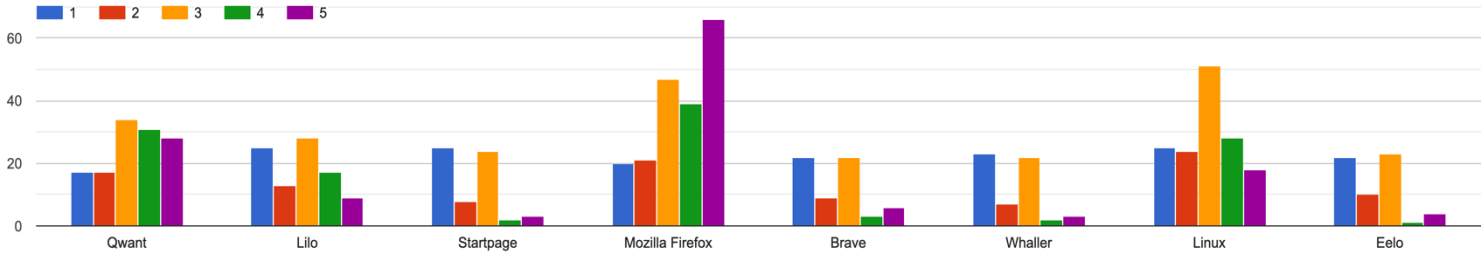
250 réponses



Connaissez-vous les services suivants ?

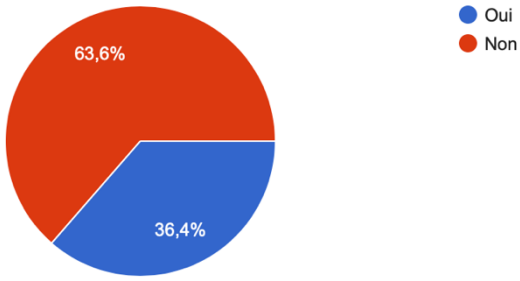


Si oui, évaluez leur degré de substitution aux GAFAM (Ordre croissant : 1 = pas du tout substituable ; 5 = totalement substituable)



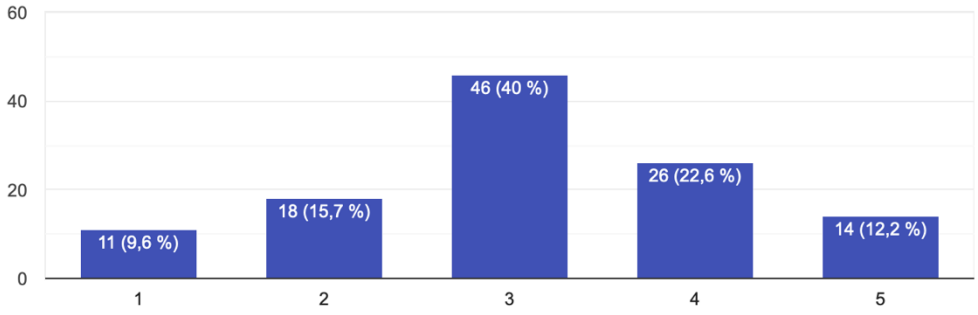
Connaissez-vous des logiciels libres ?

250 réponses



Si oui, évaluez leur degré de substitution aux GAFAM

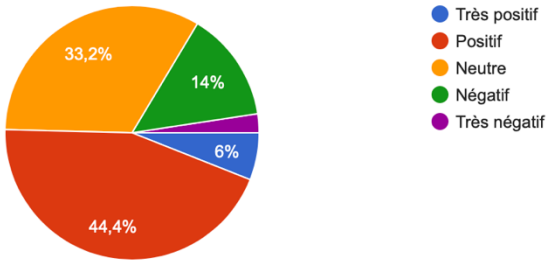
250 réponses



Part 7 : Votre ressenti vis-à-vis des GAFAM

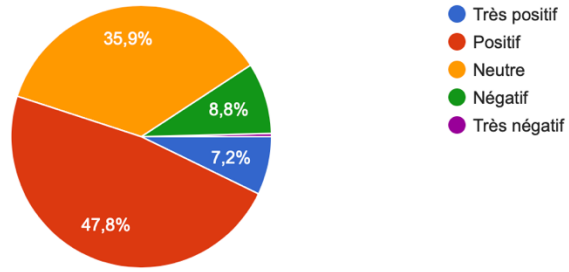
Quel impact les nouvelles technologies ont-elles sur votre vie privée ?

250 réponses



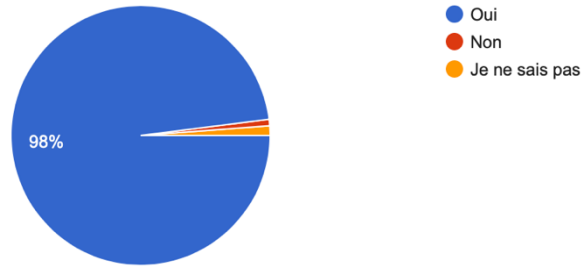
Quel est l'impact des services offerts par les GAFAM sur votre vie quotidienne ?

250 réponses



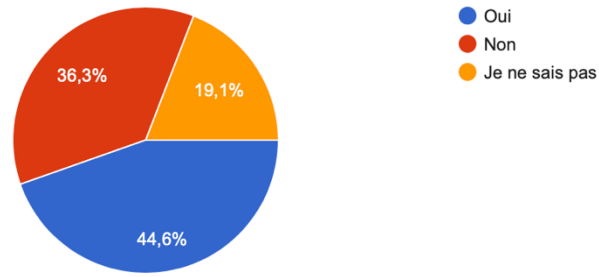
Les GAFAM ont-ils une influence sur la société actuelle ?

250 réponses



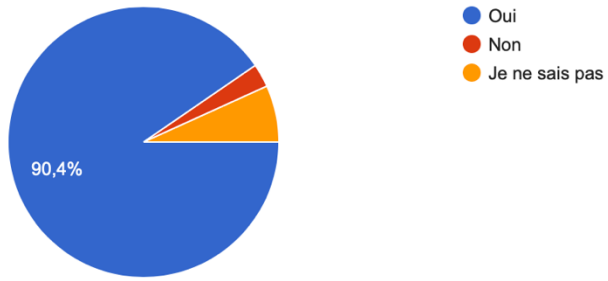
Selon vous, les GAFAM ont-ils des concurrents ?

250 réponses



Les activités des GAFAM devraient-elles être davantage contrôlées ?

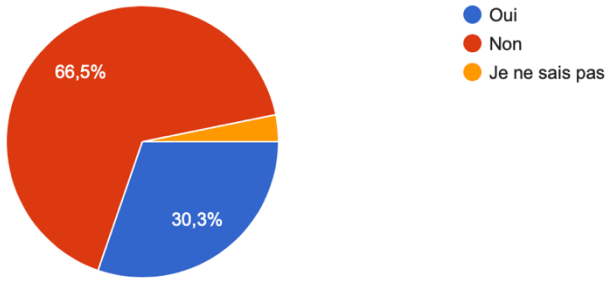
250 réponses



Part 8 : Marchandisation des données

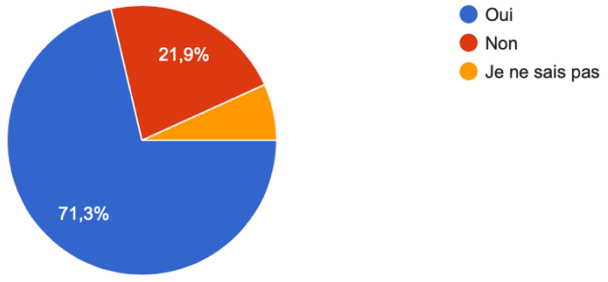
Selon vous, les données personnelles sont-elles un bien marchand comme un autre ?

250 réponses



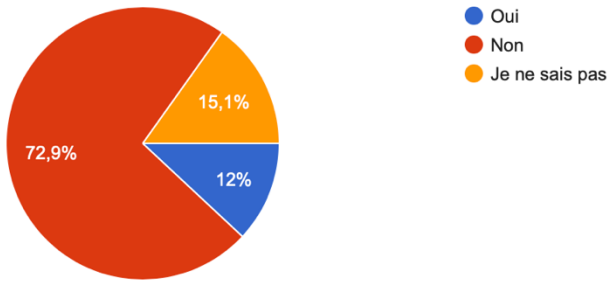
Selon vous, les données personnelles ont-elles une valeur pécuniaire ?

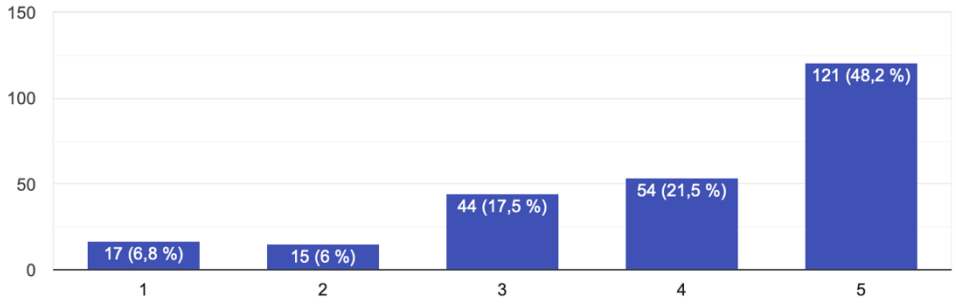
250 réponses



Êtes-vous favorable au don de vos données personnelles aux entreprises numériques afin de bénéficier de services gratuits ?

250 réponses



Que pensez-vous de l'assertion suivante : « Si c'est gratuit, c'est que c'est vous le produit » ?

250 réponses